An Economic Approach to Evaluating the Impact of AML/CFT Regulations

Caitlin M. McGough

Connel Fullenkamp, Faculty Advisor

Duke University
Durham, North Carolina
2016

Acknowledgements

I'd like to take this space to thank everyone who has supported me throughout this process. First and foremost, I would like to thank Professor Connel Fullenkamp for his faith in me to pursue this project and the patient guidance he provided along the way. Next, I am extraordinarily indebted to the experts I interviewed, who went above and beyond my expectations with their time and generosity, as well as to all of those who helped me make the initial connections (in one case, there were no fewer than four degrees of separation). Lastly, I would like to thank my friends and family for supporting me, especially my mother, who never fails to answer the call of duty when proofreading is required.

Abstract

This paper addresses the unintended consequences of AML/CFT regulations, seeking to provide an economic analysis of the drivers of de-risking and the broader consequences for the goal of financial integrity. Looking at qualitative data, this paper (1) concludes the problem of de-risking warrants a reconsideration of the enforcement approach and (2) recommends reorienting the banks' payoff matrix by reducing the cost of compliance and regulatory risk associated with providing financial services to high-risk, low-profit customers. This paper culminates with the recommendation to consider tolerating "honest mistakes" on the part of financial institutions in order to achieve the goals of integrity and inclusion in the international financial system.

Keywords: De-Risking, Financial Inclusion, Money Laundering, Terrorism Financing

Acronyms

AML/CFT: Anti-Money Laundering and Countering the Financing of Terrorism

BSA: Bank Secrecy Act of 1970

CDD: Customer Due Diligence

FATF: Financial Action Task Force

FinCEN: Financial Crimes Enforcement Network, U.S. Treasury Department

FININT: Financial Intelligence

ISIL: Islamic State in Iraq and the Levant (Syria)

KYC: Know Your Customer

KYCC: Know Your Customer's Customer

MSB: Money Service Business

MTO: Money-Transfer Operator

OFAC: Office of Foreign Assets Control, U.S. Treasury Department

RBA: Risk-Based Approach

SARs: Suspicious Activity Reports

I. Introduction

In the aftermath of 9/11, anti-money laundering and countering the financing of terrorism (AML/CFT) regulations were made more rigorous to counter illicit actors' use of the international financial system. Changes to the existing regime were based on the principles of financial transparency, information sharing, and customer due diligence. Governments began "requiring financial institutions to apply strict compliance standards and programs," and "viewed and treated [the banks] as the guardians of the integrity of the financial system" (Zarate). These enhanced AML/CFT regulations have resulted in consequences for a diverse range of constituencies. Formal financial institutions concerned about compliance obligations, migrant workers sending remittances home to relatives, and law enforcement agencies working against organized criminal actors have all observed the impact of these regulations. There is a clear sense among the different constituencies that they are being impacted by regulations, but there is little research that takes a comprehensive look at the full range consequences for these disparate groups.

The unintended consequences of AML/CFT regulations may broadly be characterized as "de-risking." The Financial Action Task Force (FATF), the international standard-setting body for AML/CFT practices, defines de-risking as terminating relationships with clients or categories of clients "to avoid, rather than manage, risk in line with the FATF's risk-based approach" (FATF 2014). De-risking typically occurs in high-risk, low-profit circumstances, making it difficult for customers in these categories to access the regulated financial system. In this way, de-risking has a negative impact on "financial inclusion", defined by the FATF as "providing access to safe, convenient, and affordable financial services to disadvantaged and other vulnerable groups who have been… excluded from the formal financial sector" (FATF 2013).

Because this is a policy problem related to the financial sector, development in impoverished regions, and national security, de-risking and its consequences for financial inclusion have been the topics of many government reports and think tank projects. What is lacking, however, is a comprehensive assessment of the consequences of de-risking for all constituencies involved, and recommendations for how to implement a proportionate, risk-based approach to enforcement.

The purpose of this paper is to fill these gaps and tell the whole story of AML/CFT regulations and financial inclusion as it relates to banks, money service businesses, and the national security apparatus. This paper seeks to apply economic analysis to qualitative data. Though it would be useful to run regressions of remittance flows or conduct an experiment on the factors driving de-risking, the data to support these endeavors simply does not exist. The very nature of this problem is that financial services are being pushed out of the regulated system, and visibility into transactions happening underground is difficult. Instead of a quantitative analysis, this paper uses information that is readily available in regulator reports, media anecdotes, and think tank products, to make economic arguments about why de-risking is happening, what de-risking means for the international financial system, and how the consequences are counterproductive to the goals of financial integrity. These findings culminate in a series of recommendations rooted in refining the regulatory approach to AML/CFT risk in order to curb the trend of de-risking while preserving the integrity of the financial system.

The primary materials consulted for this project were publications from the FATF and U.S. regulators, as well as research produced by the World Bank, the IMF, and a variety of think tanks. Additionally, the perspective of practitioners provided invaluable insight into the issues surrounding AML/CFT regulations. Juan Zarate, the former Assistant Secretary of the Treasury for Terrorist Financing and Financial Crimes**,** produced an authoritative text on the subject called

Treasury's War, which provides detailed coverage of the campaign waged by the U.S. government against terrorist organizations in the years following 9/11. Lastly, in order to fill the information gaps between different constituencies, extensive interviews were conducted with individuals in the Treasury Department, the State Department, and Deloitte Consulting LLP.[1]

The enhanced AML/CFT regime has incentivized banks to de-risk from certain industries, raising barriers to financial services and reducing financial inclusion on the periphery of the regulatory umbrella. In turn, this trend has disrupted the flow of remittances to developing regions and decreased visibility into transactions. This paper demonstrates how these consequences of AML/CFT regulations are counterproductive to the primary goal of financial integrity and makes recommendations on how to adopt a proportionate, risk-based approach to enforcement.

First, this paper provides background information on AML/CFT regulations and the increasing concerns surrounding de-risking and financial inclusion. Next, this paper uses economic analysis to evaluate the impact of AML/CFT regulations on banks' compliance practices, remittance services' access to formal bank accounts, and the national security apparatus's visibility into the financial system. Finally, this paper concludes with recommendations to reduce the impact of de-risking by refining the regulatory approach to AML/CFT risk.

II. Background

The purpose of AML/CFT regulations is to prevent bad actors from operating in the international financial system. Juan Zarate's *Treasury War* goes to great lengths to describe the

---

[1] These practitioners were generous with their time and expertise, and in return I assured their contributions would remain anonymous. Their contributions are cited as "Interview 1", "Interview 2", and so on. Details about their positions and agency-affiliations are included at the end of the paper, prior to the works cited page.

preventive paradigm constructed to counter illicit activity in the financial system. Traditionally, regulations emphasized preventing illicit funds from entering the formal financial system through money laundering. After 9/11, the threat of "reverse money laundering," legitimate funds destined for terrorist purposes, became a priority for regulators (Zarate 2013). Regulations therefore comprise a "living regime that continues to evolve based on the threats [to the financial system]" (Interview 2). Through his experiences, Zarate found that while regulations themselves evolve, the approach has been consistently rooted in leveraging the self-interest of financial institutions seeking to minimize the risk of illicit transactions that could bring high regulatory and reputational costs.

Official publications from the FATF and U.S. regulatory agencies provide a working knowledge of AML/CFT risk management principles and specific challenges encountered in the realm of these regulations. The FATF's "Recommendations" emphasize Know Your Customer (KYC) principles and that banks should take a risk-based approach to customer due diligence practices in order to satisfy KYC obligations (FATF 2012). This means that the degree to which a bank conducts customer due diligence – for example, identity verification and transactional scrutiny – depends on the AML/CFT risk category of the client. Indicators to assign AML/CFT risk might include geographic location and the type of service being offered.

Designed with the complementary goals of financial integrity and countering illicit actors, the AML/CFT regulatory regime has both defensive and offensive characteristics. Defensive measures are rooted in Know Your Customer (KYC) principles and transaction monitoring. To satisfy Know Your Customer Principles, the Bank Secrecy Act of 1970 mandated banks perform Customer Due Diligence (CDD) procedures and submit Suspicious Activity Reports (SARs) to the U.S. Treasury Department (Bank Secrecy Act 1970). The USA PATRIOT

Act expanded this regulatory umbrella to non-bank financial institutions, such as remittance companies, and required enhanced scrutiny of customers and transactions using the FATF's recommended risk-based approach (USA PATRIOT Act 2001).

The Treasury Department's offensive tools for countering illicit actors rely on robust compliance with these defensive requirements in the financial system. Treasury's Office of Foreign Assets Control (OFAC) uses its powerful sanctioning and designating authorities to counter illicit financial activity. OFAC compiles sanctions packages, which expressly prohibit any business activities with sanctioned entities, after building a case that meets a legal threshold (Interview 1). In contrast to this legal threshold, Section 311 of the PATRIOT Act empowers Treasury to identify institutions and individuals as a high AML/CFT risk without any requirement to prove malicious intent or criminal culpability. Section 311 designation effectively blacklists entities without a criminal conviction; *The Economist* has likened it to a "sledgehammer" ("American Regulators" 2016). Both instruments – sanctions and Section 311 designation – anchor on the customer due diligence and transaction monitoring conducted by financial institutions. These measures impact actors across the globe due to the U.S. dollar's dominance in international trade. With New York as the core financial hub for dollar-clearing transactions, U.S. agencies may claim regulatory authority over these transfers. Additionally, the effectiveness of these measures "relies on a global financial, regulatory, and diplomatic ecosystem that rejects rogue financial behavior" (Zarate 2013). Given the scope and severity of these measures, it is not difficult to conclude that they might have a negative impact on financial markets.

A variety of constituencies are concerned with de-risking and have sought to understand what is happening and what the consequences might be. The World Bank recently surveyed financial institutions, money service businesses, and government regulators to gain insight into de-risking, concluding, “de-risking is happening, though it hits specific countries, regions, and financial services in varying degrees” (World Bank Survey 2015). The World Bank found no systematic evidence that de-risking is happening on a large scale, but high-risk regions and markets are being impacted (Interview 2). One industry in particular is money transfer operators (MTOs), more broadly known as money service businesses (MSBs).[2] Zarate observed the potential consequences of this trend: “[De-risking] raises concerns that less credible or scrupulous financial actors will step in to fill the vacuum. For authorities, this would entail a potential loss of visibility… for banks, it would mean even greater pressure to abandon certain segments of the population of regions of the world” (Zarate 2013).

Driven by a combination of business factors and regulatory risk, de-risking disproportionately impacts low-profit industries on the periphery of the formal financial system, such as money service businesses. The World Bank survey of 82 MSBs found that more than half lost correspondent accounts in 2014, and over 69 percent of banks surveyed responded that MSBs and other remittance companies were the most impacted by de-risking (World Bank Survey 2015). For a broad exploration of the drivers of de-risking and the counterproductive implications, Tracey Durney’s study “Understanding Bank De-Risking and its Effects on Financial Inclusion” for the Global Center on Cooperative Security, a think tank, provides an excellent analysis. The study examines incentives and constraints of regulators, banks, and customers to arrive at its conclusions. The primary finding of the study is that de-risking actually contributes to an increased AML/CFT risk by pushing high-risk clients to smaller, or less regulated financial institutions that lack AML/CFT capacity (Durney 2015). In Section III, this

[2] This paper will refer to these remittance companies as MTOs, as it describes their primary service of transferring cash payments.

paper will examine these issues in greater detail and add evidence to Durney's conclusions with economic analysis. Additionally, the Recommendations provided in Section IV will go further than Durney's analysis and take lengths to describe an enforcement approach to resolve the unintended consequences.

Remarks from key U.S. regulators have put the spotlight on AML/CFT regulations and financial inclusion. Thomas Curry, Comptroller of the Currency, admitted in a speech, "Decisions to terminate relationships can have regrettable consequences… Transactions that would have taken place legally and transparently may be driven underground (Curry 2016). Treasury Secretary Jacob Lew spoke of the potential long-term impact of de-risking, "Financial transactions may begin to move outside of the United States entirely – which could threaten the central role of the U.S. financial system globally, not to mention the effectiveness of our sanctions in the future" (Lew 2016). This paper will expand on this question in the Section III during the discussion of the national security apparatus.

The evolution of AML/CFT regulations is undeniably rooted in a need to prevent illicit activity in the international financial system. Reflecting on the literature and existing information, there are two key takeaways. First, the enhanced regulatory regime has in many ways been largely effective in isolating and targeting rogue actors. Secondly, because regulations are pushing customers out of the formal financial system, the impact on financial inclusion is increasingly a cause of concern for banks, remittance services, and law enforcement.

III. Counterproductive Consequences: Banks, MTOs, and National Security

A. The Banks

In response to the new AML/CFT regime, financial institutions have increased compliance costs, reevaluated internal controls and practices, and in some cases, ended relationships with customers when the risks of enforcement action does not outweigh potential profits. The following section will explore how banks have altered their operations, processed signals from regulators, and reevaluated their correspondent relationships in response to AML/CFT regulations.

Enhanced AML/CFT regulatory rules and principles adopted after 9/11 were designed to leverage the “risk-based compliance calculus of financial institutions” in order to prevent illicit actors from exploiting the international financial system (Zarate 2013). As a result, financial institutions adopted more rigorous customer due diligence practices, incurring greater compliance costs to avoid the reputational and litigation costs associated with unwittingly providing financial services to criminal entities. According to the 2014 KPMG Global Anti-Money Laundering Survey, 78 percent of top global banks reported increases in the total investment in AML compliance. In the three-year period from 2011 to 2014, 22 percent of those who reported increases in AML compliance spending indicated an increase of 50 percent (KPMG 2014). Western Union, a provider of money-transfer services, spends $200 million annually searching for “suspicious activity,” while JP Morgan Chase & Co. has 9,000 employees working on AML compliance issues (Barry 2016).

The Wolfsberg Group, an association of 11 global banks, has developed industry standards for Know Your Customer (KYC), AML, and CFT policies. The Wolfsberg Standards on AML and correspondent banking policies provide useful insight into the variables banks assess in risk models for correspondent relationships. The primary risk indicators include geography, the AML control program of a client’s affiliates, the ownership and management structure, and the types of products and services the client offers. To further reduce legal liability, financial institutions file Suspicious Activity Reports (SARs) wherever their internal

AML/CFT controls identify risk, as required by the Bank Secrecy Act (Interview 1). Since the PATRIOT Act, financial institutions have filed over 17 million (SARs),(Barry 2016) averaging 55,000 per day from 800,000 financial institutions and 500,000 individual foreign bank account holders (Shasky Calvery 2015).

It is reasonable to conclude that these increased compliance costs are necessary, given the threats to the integrity of the financial system. However, the cost of AML/CFT compliance goes beyond increased operational costs for banks, and regulations should be evaluated in the context of the full cost to the society. De-risking is an unintended consequence in itself, but it also has broader ramifications on the financial industry. The remainder of this section will assess the drivers of de-risking, the decision to de-risk in the context of an uncertain regulatory environment, and how the information externalities associated with de-risking will make it more difficult to push marginalized clients back into the formally regulated financial system.

The decision of financial institutions to de-risk is driven by a combination of regulatory risk and business concerns, particularly low profitability in markets such as remittance services. While some have contested that banks de-risk from developing regions indiscriminately, anecdotal and survey evidence supports that financial institutions evaluate customers using a risk-based approach on a case-by-case basis, which is consistent with international AML/CFT principles (Interview 1). The World Bank uses two categories to assess the drivers of de-risking: business factors and regulatory risk factors (World Bank Survey 2015). These categories are clearly related, as regulatory costs factor into potential profits. One Treasury official concluded that de-risking is not rooted in blanket avoidance of AML/CFT risk, but rather is a result of a "customer by customer" approach evaluated in terms of the whole spectrum of "potential profits and compliance costs" (Interview 1). A World Bank Survey of banks produced similar findings;

the most cited reasons for closing the accounts of money-transfer operators were profitability, pressure from other actors (correspondents or law enforcement), lack of confidence in client's AML/CFT controls, and reputational risk (World Bank Survey 2015). Exiting from a money market due to new regulations has happened elsewhere. Because of the high volume of transactions and the low profits associated with transfers, even a small tightening in regulations may be enough to push dealers out of the market.

In addition to the understood compliance obligations under current regulations, banks are operating in an uncertain regulatory environment. International standards anchor on a risk-based approach to customer due diligence practices, providing financial institutions with flexibility in implementing their own AML/CFT controls (FATF). This is effective in some ways, especially considering the range of types of financial institutions and areas in which they operate, but flexibility also leads to ambiguity for banks with regard to how to implement regulatory principles. Enforcement actions and large fines compound the regulatory ambiguity, contributing to an extremely risk-averse environment from the perspective of financial institutions (Durney 2015). To better understand how banks are processing enforcement signals, it is useful to work through a simple game theory analysis of banks considering an MTO customer and regulators.

Beginning with incentives of banks and regulators, it is clear that in the case of a low-profit, high-volume sector like money transfers, regulators are setting financial institutions up to de-risk from certain customers and industries. Financial institutions prefer to avoid enforcement action due to reputational and litigation costs. Financial institutions also prefer higher profits, and remittances are naturally a low-profit, cash-transfer industry. Regulators prefer financial integrity: "We want to cut off illicit actors because we want to protect the integrity [of the financial system]" (Interview 1). Additionally, in the wake of the 2008 financial crisis, regulators prefer to be perceived as “holding institutions accountable for misconduct” (Durney 2015). Lastly, regulators prefer enforcement actions that result in large fines to deter violations, consistent with the rule of law principles. This payoff matrix accounts for these incentives, compliance costs, and low remittance profits:

Regulators

		Enforcement Action (p)	No Enforcement Action (1-p)
The Bank	Service	Π-C-F, I+F-k	Π-C, I
	No Service	0, E(I)	0, E(I)

Figure 1: Providing Services to an MTO

In this diagram, the bank has the option to provide services to an MTO, and the regulators have the option of bringing an enforcement action should the bank be in violation of AML/CFT regulations. Regulators receive a benefit of **I** from the integrity of the inclusive system and pay the cost **k** when bringing an enforcement action. In the case of no service to the MTO, regulators receive a payoff **E(I)** from the perception of integrity in the financial system, where $E(I) < I$ because a less inclusive regulated system translates into less integrity derived from that regulated system. Arguments elsewhere in this paper support that the benefits of financial integrity diminish for regulators, and society writ large, as financial inclusion is negatively impacted.

Because the customer is an MTO, profit **π** is low, and the cost of compliance **C** is high, due to the large volume of transactions to be monitored. The fine **F** is at the discretion of the regulators, and financial institutions perceive that in the case of an enforcement action, F will be high. This leaves the probability **p** of an enforcement action. Defining a specific function for p is beyond the scope of this paper, but taking a closer look at the factors motivating the probability of enforcement sheds further light on the drivers of de-risking.

Financial institutions perceive that in the case of a violation, the probability **p** that an enforcement action will be brought is high. The probability of enforcement is therefore a function of the probability of a bank making a mistake, and the probability of a regulator detecting that mistake. Recent cases of money laundering revelations provide indirect evidence that the probability of FinCEN detecting a mistake is high when a target or an industry is on their radar as an AML/CFT concern. Furthermore, financial institutions perceive that a probability of making a mistake is high. And given the volume of cash transfers, (the World Bank estimates that in 2014, immigrants in the U.S. sent about $54 billion abroad), even with robust AML/CFT policies, it is likely a bank will not detect every suspicious transaction. This leaves banks with a low, and possibly negative, expected value of providing services to MTOs:

$$\mathbf{EV = p(\pi\text{-}C\text{-}F) + (1\text{-}p)\ (\pi\text{-}C)}$$

This purpose of this simple exercise is to take a closer look at the payoff matrix financial institutions are facing in these de-risking decisions. The key takeaway is that the probability of enforcement is complex, and the current regulatory environment is setting up de-risking to be the rational option for banks. Indeed, one State Department official observed that in this situation, “There are many, many disincentives [for banks]” (Interview 2). The high probability of enforcement and the expectation of a costly enforcement fine motivate the banks to de-risk. This analysis will form the foundation of the recommendations in Section IV.

Examples of recent enforcement actions reinforce the banks’ perception of a high probability of enforcement and a costly enforcement fine. Each enforcement action brought serves as a signal from regulators about future enforcement. In 2012, HSBC paid a then-record

$1.9 billion fine after failing to conduct basic CDD on accounts in high-risk regions. HSBC was found to have drug cartel money laundering issues in Mexico, as well as violating sanctions by doing business in Iran, Libya, Sudan, Burma, and Cuba (Viswanatha 2012). Also in 2012, Standard Chartered was fined $340 million after being accused of scheming with Iran to hide billions of dollars of transactions to evade sanctions. Two years later, Standard Chartered paid another $300 million after not disclosing the full extent of those transactions to authorities (Rushe 2014). In 2014, BNP Paribas pled guilty to processing over $8.8 billion through the financial system in violation of sanctions against entities in Sudan, Iran, and Cuba and paid a record $9 billion fine (“BNP Paribas” 2014). These signals cause banks to continue to revise up their estimates for the probability of enforcement action and the cost of the fine.

Though the above analysis is simple and straightforward, it serves to illustrate the regulatory environment in which banks are operating and the conclusions they are reaching based on regulators’ actions. As one observer notes, “It is clear that the climate for those working in AML/CFT… is becoming unceasingly hostile and unforgiving. In cases that range from egregious failings to lesser administrative misdemeanors, the approach of the regulator has been consistently severe” (Parry 2014). The analysis shows that banks have concluded that regulators are seeking to tighten AML/CFT enforcement, which is supported by anecdotal evidence from interviews (Interview 4). Further, this analysis identifies the primary driver of de-risking: the high price of regulatory risk and compliance in a low-profit industry. This issue will be revisited in the Recommendations, which will seek to adjust the price of regulatory risk to mitigate the scope and impact of de-risking.

The central regulatory problem for financial institutions considering de-risking is uncertainty over their “Know Your Customer’s Customer” compliance obligations. The extent to which banks are held liable for their customer's customers is unclear. This uncertainty is a result of conflicting statements from different regulators and AML/CFT standard setting bodies. According to Section 311 of the PATRIOT Act, when Treasury designates a jurisdiction, financial institution, or class of transaction as a primary money-laundering concern, the Secretary may require domestic institutions with correspondent relationships to identify each customer of this customer. The statute also mandates enhanced customer due diligence for correspondent accounts and private banks affiliated with a domestic financial institutions' own correspondent (USA PATRIOT Act 2001). This means that a U.S. bank is liable for its Saudi correspondent bank's Libyan customers (Interview 1). This is directly contradictory to the FATF's statement that banks are not expected to know their customers' customers, as well as FinCEN's statement that banks need not know every MTO customer to comply with regulations (FinCEN Statement 2014). In a risk-averse environment in which there is uncertainty about the extent of a bank's liability for its customers' customers, banks will cover all their bases, and de-risking from marginalized customers may be the best option in high-risk, low-profit situations (Interview 2). "It is not reasonable to expect that banks… will expose themselves to severe penalties and reputation risk… for the relatively small financial benefit associated with remittances to high risk countries, especially when they have very little control over the quality of compliance for which they are being held accountable" (Makin 2014).

The regulatory drivers for de-risking are often rooted in a lack of visibility about a customer's, or a customer's customer's, account. De-risking from a customer exacerbates this information shortage, resulting in an information externality that may create a perpetual negative feedback loop for financial institutions. As de-risking becomes more prevalent in high-risk areas, "[Banks] are losing a broader visibility into that banking context and into that financial context" (Interview 3).

The example of information externalities in the mortgage markets provides a useful analogy to what could happen for customers in high-risk areas as a result of de-risking. In mortgage markets, lenders need information about borrowers and their collateral in order to evaluate risk. Leonard Nakamura, a senior economist at the Philadelphia Fed, found that evaluating one customer's collateral gives information on another customer's collateral, for example, the value of housing in a particular neighborhood. "An information externality can cause a slowdown in lending activity to be self-perpetuating because the slowdown results in a shortage of information available to lenders," which makes mortgage markets difficult to start (Nakamura 1993).

De-risking may similarly result in information externalities that exacerbate the lack of visibility in these markets. Evaluating the AML/CFT risk of one account may give insight into the AML/CFT risk posed by another customer. Consider that a bank's correspondent relationships and customers form nodes in a financial network. The more nodes, the more visibility into transactions between the nodes, and the richer the data set. Greater visibility into a higher volume of transactions leaves it easier to identify suspicious activities (Interview 3). In thinking about a bank's AML/CFT threat model, what would the consequence be of losing one node in the network? A historical example provides some insight. An international bank was growing increasingly concerned about its correspondent bank in Estonia failing to conduct proper due diligence. The suspicious payments, however, were not coming from the correspondent in Estonia, but the correspondent's correspondent based in Denmark. When the international bank discovered the problem, it immediately exited the relationship. This left the international bank blind to the transactions of the illicit actor throughout the course of its money laundering investigation, which could have proved useful in reevaluating the full range of its AML/CFT risk with correspondent banks transacting with each other in this financial network (Interview 4).

These information externalities have the potential to create a negative feedback loop that perpetuates the trend of de-risking. If banks continue to de-risk from high-risk markets, they will lose insight that enables them to assess a customer's AML/CFT risk. As seen in the mortgage market example, this will make markets more difficult to start. Banks will continue to de-risk from certain markets, decreasing visibility into those customers, and increasing the barriers to financial inclusion in the future.

After examining the drivers of de-risking, this section concluded that banks make the decision to de-risk from high-risk, low-profit customers due to the high price of risk and regulatory compliance. Next, this section assessed the regulatory uncertainty concerning inconsistent interpretations of a bank's Know Your Customer's Customer obligations. Finally, this section explored the information externalities that result from de-risking, which further exacerbate the issues of visibility into a bank's customers and customer's customers. The next section will address the impact of de-risking for MTO's, development, and the goal financial integrity.

B. MTOs: Inclusion & Development

As discussed in the previous sections, de-risking, driven by business factors and regulatory risk, disproportionately impacts low-profit, high-risk industries. The perception that MTOs are a high ML/TF risk is well founded. MTOs operate through cash settlements across jurisdictions with poor governance and little oversight from regulators (FATF 2013b). Banks' risk management indicators place MTOs in most high-risk categories, particularly for geography, business services offered (cash transfers), and the AML controls of affiliates (Wolfsberg Group 2014). Banks have little visibility into the sequence of transfers once the money has left the MTO's account, making it difficult to comply with CDD obligations. Additionally, according to the current interpretation of regulations, AML/CFT liability resides with the bank managing the MTOs' funds (Makin 2014). The lack of visibility into the end beneficiary of a transaction makes jurisdiction-specific regulation of MTOs essential for banks to tolerate their correspondents' risk. However, governments often lack the resources and institutions necessary to perform sufficient supervision of the industry, and MTOs operate in some of the least governed regions in the world. In short, "Banks have very little control over the quality of compliance for which they are being held accountable in the recipient markets" (Makin 2014).

In addition to the high objective regulatory risks, MTOs have demonstrated their vulnerability to exploitation by illicit actors in the past, which reinforces the banks' perception that they are high-risk customers. After 9/11, revelations about the extent of al Qaeda's funding through remittances became clear. According to the 2005 U.S. Money Laundering Assessment, FBI field offices consistently identified MTOs as the third-most utilized money laundering method, and specifically cited money remitters as a threat (Treasury 2005). Al Barakaat, an international remittance system founded in Somalia in, was designated by Treasury as a primary money laundering concern. Though Al Barakaat's customers were mostly unwitting Somali expatriates remitting money to relatives, Treasury assessed that the head of the company had diverted 10 percent of global revenues to al Qaeda (Zarate 2013). This trade off – a lifeline to Somalis versus an established AML/CFT concern – is exemplary of the regulators' approach to financial integrity since 9/11. Regulators have tended to prioritize AML/CFT above all other regulatory objectives, leading observers to call it the "primary" or "exclusive" focus of regulations (Cockayne 2012). As demonstrated in the analysis in the previous section, with the price of regulatory risk so high, it is only rational for banks to de-risk from these customers.

As de-risking from MTOs has continued, regulators have shifted their tone to discussing the importance of financial inclusion, but stopped short of making substantive changes to AML/CFT regulations. International bodies and U.S. regulators have responded to de-risking by reiterating the importance of a risk-based approach to customer due diligence, as well as discussing the goal of financial inclusion with little change to language about AML/CFT enforcement. The FATF Guidance on Inclusion states, "Financial institutions hold the business relationship and are accountable for it, and ultimately liable with respect to agents' compliance with AML/CFT requirements. It is recommended to balance regulatory concerns about agents with the financial inclusion objective" (FATF 2013). This, however, does little to address the problem of banks dropping MTO customers, which are considered high-risk in numerous categories.

Though AML/CFT regulatory risk is a primary driver of de-risking, the integrity of the international financial system actually depends on financial inclusion. It is in the interest of regulators for transactions to occur in the formally regulated financial system. If robust, unregulated alternatives become the norm, the "integrity" of the regulated system serves little purpose in attempts to isolate illicit actors. Pushing customers into the regulated sector makes them subject to more rigorous AML/CFT controls because banks are more competent at evaluating the legitimacy of transactions (Interview 1). A study affiliated with the World Bank and the IMF similarly concluded, "Measures that ensure that more clients use formal financial services therefore increase the reach and effectiveness of the AML/CFT controls" (Bester 2008).

Additionally, the AML/CFT risk of criminal actors does not disappear when they are pushed out of the formal system. The FATF cites the example of the Taliban laundering drug proceeds, “which returned to the use of [MTOs] after the implementation of more stringent Afghan banking rules” (FATF 2015). Durney notes, “The ironic result of de-risking is re-risking… you are sending [clients] to banks that probably can’t handle [the risk]” (Durney 2015). Because of its impact on financial inclusion of peripheral customers, de-risking is therefore counterproductive to the purpose of AML/CFT regulations. Preventing further de-risking and working to push more cash transactions under the regulatory umbrella would serve regulators’ goals of transparency and integrity in the financial system.

Regulators are increasingly recognizing that financial inclusion contributes to financial integrity. One Treasury official stated that AML/CFT and financial inclusion are “not necessarily contradictory” (Interview 1). The State Department views financial inclusion and financial transparency as “complementary” goals that reinforce each other (Interview 2). The FATF posits, “Protecting the integrity of the global financial system… requires covering the largest range of transactions that pose money laundering and terrorist financing risks” (FATF 2013). Similarly, Treasury’s FinCEN articulates the consequences of de-risking from MTOs: “Refusing financial services to an entire segment of the industry can lead to an overall reduction in [transparency] that is critical to making the sector resistant to the efforts of illicit actors” (FinCEN 2014).

Aside from being counterproductive to the goal of financial integrity, de-risking from MTOs has serious consequences for populations who rely on remittances for sustenance, and as an extension, on the development of impoverished and marginalized regions. Somalia is the quintessential case study for remittances. Up to $1.3 billion in remittances is sent to Somalia every year, amounting to 25-40 percent of Somalia’s GDP. Over 40 percent of Somalis rely on remittances to meet basic needs. Because of the high AML/CFT risk, Somali MTOs have been hit particularly hard by de-risking trends and have subsequently been pushed out of the regulated financial system ("Hanging by a Thread" 2015). These networks are resilient, however, and have resorted to carrying cash by hand on flights to transport it to the region (Barry 2016). Somali remitters are "literally moving millions of dollars in cash by suitcase… [they] work hand in glove with TSA to make sure the cash can get through" (Interview 2). It is important to note that despite losing their correspondent accounts, these cash transfer activities have continued, although they are occurring outside the regulated system, and often through actors with fewer AML/CFT controls. In the case of Somalia, de-risking therefore increases barriers to formal financial services and fails to prevent illicit transactions in the unregulated system.

Looking more broadly than the high-risk context of Somalia, de-risking may constrain development in impoverished regions. There is a clear link between access to financial services and economic growth. As markets develop, financial services drive economic growth by increasing the rate of capital accumulation and improving the allocation of capital (King & Levine, 1993). Furthermore, statistics about access to financial services and gender disparities are scarce, but it is reasonable to conclude that women are disproportionately harmed by de-risking (Durney 2015). In many developing countries, financial products, such as savings accounts, require a husband's signature or evidence of property rights, resulting in limited access for women (24). It is estimated that over half of women in Somalia receive remittances, which are the only cash funds that female caregivers can access and control, making them a vital component of women's economic activity ("Hanging by a Thread" 2015). Considering the evidence that women invest in drivers of human development, such as food and education, the disproportionate harm to women inflicted by de-risking will likely extend to a disproportionate constraint on development (Ranis 2000).

The consequences for development are relevant to the broader purpose of AML/CFT regulations, namely curbing the power and influence of criminal organizations and terrorist groups. Though criminal and terrorist activities do not necessarily exist because of poverty, there is a clear correlation between poverty and turning to terrorism (Interview 2). If de-risking, a consequence of AML/CFT regulations, perpetuates poverty in developing regions, it may in fact be counterproductive to the broader goals of combating criminal organizations and terrorist groups.

This section explored how AML/CFT regulations have resulted in de-risking from MTO customers, and the consequences of this de-risking on financial inclusion, financial integrity, and development in impoverished regions. The next section will assess potential consequences of de-risking from the perspective of the U.S. national security apparatus, particularly in areas of intelligence and law enforcement.

C. The National Security Apparatus

In addition to their purpose in protecting the integrity of the international financial system, AML/CFT regulations exist to serve as a tool of foreign policy. The national security apparatus leverages the dominance of the US dollar to support foreign policy objectives, from defeating al Qaeda to countering North Korea's belligerence (Zarate 2013). As articulated by Secretary Lew, "Economic sanctions have become a powerful force in service of … foreign policy objectives – smart power for situations where diplomacy alone is insufficient, but military force is not the right response" (Lew 2016). Though this section is not comprised of rigorous economic analysis, it is necessary to include the national security component when evaluating the consequences of AML/CFT regulations. The national security apparatus, including intelligence and law enforcement, values financial integrity as a contributing factor to national security. This helps explain why regulators value financial integrity in the game theory model, even in the absence of banks providing services to MTOs. Additionally, the national security apparatus benefits from AML/CFT in two ways. First, AML/CFT compliance obligations provide visibility into transactions that occur in the regulated system. Secondly, AML/CFT regulations combined with the use of targeted sanctions provide the ability to punish illicit actors by isolating them from the benefits of the formal financial system (Zarate 2013). De-risking, particularly in the MTO industry, pushes transactions outside of the regulated financial system and risks undermining both of these advantages.

AML/CFT regulations are designed to make banks the eyes and ears for law enforcement in the formal financial system. Reporting requirements mandated by the Bank Secrecy Act and the PATRIOT Act make banks "the first line of defense against money laundering" according to regulators (Zarate 2013). In particular, the PATRIOT Act greatly expanded the government's access to financial intelligence, or "FININT," as customer due diligence practices became more rigorous. FININT is valuable because it "can reveal clear contours of relationships… financial footprints don't lie" (Zarate 2013). The Financial Crimes Enforcement Network (FinCEN), a part of the Treasury Department, is the U.S. financial intelligence unit responsible for collecting, analyzing, and disseminating FININT. FinCEN processes 55,000 Suspicious Activities Reports (SARs) and generates over 250 findings per day (Shasky Calvery 2015). This volume of intelligence is a product of banks complying with reporting requirements on transactions in the formal financial system.

Visibility into financial transactions of illicit actors is essential for the national security apparatus, but that visibility is at risk of diminishing in industries impacted by de-risking. De-risking may "entail a potential loss of visibility" for the government, depending on the volume of transactions pushed out of the regulated system and the resources the government is willing to spend to keep tabs on informal transfers (Zarate 2013). While the government certainly possesses the capabilities to acquire intelligence on illicit actors outside of the formal financial system, it becomes more difficult when targets are not identified a priori (Interview 1). The problem, in short, is that we don't know what we don't know. How many investigations begin because regulated financial institutions submit SARs? How many terrorism cases are built on evidence related to financial transactions? How many money-laundering cases come to light because a bank raises a red flag? De-risking decreases regulators' visibility into the flow of illicit funds. If the regulatory umbrella shrinks and illicit actors innovate around the formal financial system, de-risking may undermine the usefulness of banks as the first line of defense against money laundering.

De-risking also undermines the ability of the U.S. government to affect actors through the formal financial system. Regulators must balance the "core principle of isolating and exiling actors with the need to ensure rogue actors can be captured and affected by the legitimate financial system" (Zarate 2013). Isolating an actor from the formal financial system constitutes a form of punishment because the informal system is by definition illegitimate, less efficient, and more costly.

If robust alternative financial paths and networks develop, the cost of conducting business in the unregulated, informal financial system will be driven down. As regulators continue to push illicit and peripheral actors outside the umbrella of regulations, a greater need will arise for lower marginal costs in the unregulated financial sector. Suppliers of underground financial services will compete and innovate to drive down costs, for example, by leveraging technology to prevent theft. In the long run, if this isolation continues, the costs of operating in the informal financial system could bottom out at a lower average cost than the regulated system due to the absence of compliance costs. For example, the Euromarket exists because it enables financial institutions to transact in euros and avoid the costly compliance that comes with U.S. dollar transactions. Additionally, the current financial environment in Iraq provides an example of how alternative systems may develop. Iraq is considered one of the least banked countries in the world, and yet for decades, a network of financiers have provided money transfers and trade finance to those isolated from formally regulated banks (26). Clearly the financial environment of Iraq is not the exemplar, but its financial networks demonstrate it is possible to finance around the regulatory umbrella. In taking an approach that seeks to punish bad actors by isolating them, regulators are hastening the development of robust, efficient, alternatives to the formal financial system.

As alternative financial paths and networks develop and prove resilient, the impact of isolation from the regulated financial system will decline. This begs the question for the national security community, at what point should exclusion of a criminal actor be considered? Should it be the first step, or the most extreme measure? Secretary Lew has raised this issue: “We must guard against the impulse to reach for sanctions too lightly… we must be conscious of the risk that overuse of sanctions could undermine our leadership position within the global economy, and the effectiveness of our sanctions themselves” (Lew 2016).

Because illicit actors will always seek to adapt, it is notable that additional AML/CFT measures must be taken to counter the most serious, identifiable threats. Financial tools work best for national security objectives when narrow, known entities are targeted with specific U.S. goals in mind. The campaign against ISIL’s finances is illustrative of this sort of approach. To protect the integrity of the financial system, barriers have been erected to prevent ISIL's funds from being transferred through regulated banks (Interview 2). To proactively counter ISIL's ability to finance itself, Treasury has worked to decrease liquidity to its area of operations, by terminating government salary payments to occupied regions and choking off sources of revenue. The collaboration between governments and private financial institutions to enhance information sharing and counter ISIL financing has shown how the public and private sectors can work together against a specific threat (Interview 1). However, this example also demonstrates an organization that has evaded the regulated system fairly successfully. This begs another question: if informal, criminal MTO networks can go untouched by regulators and continue to operate successfully, is de-risking from legitimate MTO customers the best thing for the broader goals of financial integrity and inclusion?

This section sought to use economic analysis to explore the unintended consequences of AML/CFT regulations on banks, remittance services, and the national security apparatus and show how they have proved counterproductive to the goal of financial integrity. Financial institutions are operating in a risk-averse environment of regulatory uncertainty, which has altered their incentives to make de-risking the most rational decision. The adverse effects of de-risking on financial inclusion result in less visibility into the international financial system, perpetuating the de-risking cycle for banks and undermining the government's access to financial intelligence. For remittance companies, de-risking pushes transactions outside of the regulated system, raising operational costs and hindering development in underserved regions. These consequences are rooted in a regulatory regime that has shifted AML/CFT risk to financial institutions, distorting their incentives. The following recommendations seek to refine the current approach by building expectations about enforcement action.

IV. Recommendations

Overall, the preventive paradigm of AML/CFT regulations is the right approach for financial integrity. As one observer noted, “If we scaled back the regime, it would be completely abused” (Interview 2). However, de-risking is fundamentally driven by avoidance of prohibitively costly compliance in low-profit industries. And as the consequences of de-risking become increasingly counterproductive to the goals of financial integrity, regulators must reconsider elements of the current approach.

The regulatory approach should be refined with two goals in mind. First, regulators should seek to maximize the benefits of the AML/CFT regime. For the government, this means visibility into transactions and the ability to affect actors by threatening to cut them off from the formal financial system. The private sector also benefits from transparency and integrity in the financial system. Banks profit from a good reputation based on integrity in their operations, and customers gain access to a more secure, transparent system. Second, regulators should strive to minimize collateral damage from de-risking in response to AML/CFT regulations. It is particularly desirable for actors operating on the periphery of the formal system, such as MTOs and impoverished populations in developing countries, to be pushed under the regulatory umbrella. This second goal therefore reinforces the first, because inclusion of peripheral financial actors expands visibility of transactions, and in turn, financial integrity.

The primary recommendation of this paper is for regulators to foster the expectation that enforcement will define a risk-based, proportionate approach to enforcement. This will decrease regulatory uncertainty and prompt banks to revise down the expected price of regulatory risk. Recall that the expected value in the game theory exercise fell as banks revised up the probability of enforcement and the expected fines. In lowering p and F by emphasizing a risk-based, proportionate approach, regulators can shift the payoff matrix in favor of financial inclusion.

While standard-setting bodies and regulators tend to discuss compliance principles for financial institutions, little is said about the principles guiding regulators' enforcement practices. Enforcement should be risk-based and proportionate in order to incentivize banks to take AML/CFT measures seriously, without making the cost of compliance prohibitively high. Changing the payoff matrix for banks in their decision to service customers or to de-risk is essential to preventing the continuation of de-risking trends (Interview 2). The assessment of risk should anchor on the threat posed to the integrity of the financial system, taking into account both the type and volume of transactions. For example, a bank laundering billions of dollars for drug cartels poses a greater AML/CFT risk to the integrity of the system than a remittance service unwittingly transferring hundreds of dollars to terrorist actors. In this case, the bank should receive a greater proportional penalty and enhanced scrutiny moving forward, and regulators should work with the MTO to cut off the flow of funds and improve its AML/CFT controls. It is important to note this story is not necessarily counter to how regulators would proceed today, but the existing regulatory uncertainty and lack of defined enforcement principles makes this outcome difficult for financial institutions to expect.

Currently, financial institutions expect disproportionate fines because of past regulatory actions. Enforcement fines are typically equal to the amount of illicit transactions processed. For example, BNP Paribas was fined $9 billion after transferring $8.9 billion connected to drug cartels ("BNP Paribas" 2014). As discussed previously, this case sends signals to banks that cause them to revise up their estimates for the price of their AML/CFT risk. Additionally, this fine grossly overstates the financial benefit BNP Paribas gained from these transactions. It would be reasonable to assume BNP Paribas made less than 1 percent on each transaction, and certainly no rate greater than 5 percent. In a decision to de-risk from a customer, a bank is considering the operational cost of compliance, the reputational risk of being subject to enforcement action, and the cost of a fine, making the choice of servicing a customer prohibitively high. A better starting point for the size of a fine is therefore the amount a financial institution profited off a series of transactions, with adjustments depending on an institution's track record and AML/CFT controls. Committing to a proportionate regulatory approach would help reduce the price of AML/CFT risk and revise the banks' payoff matrix to better support financial inclusion.

In addition to providing guidance on an enforcement approach, regulators should set a ceiling for the legal and financial liabilities banks face due to Know Your Customer's Customers compliance obligations. The extent to which banks are liable for the AML/CFT risk posed by their MTO customers' affiliates and correspondents is not clear. When one considers the path of a remittance – from an MTO, to a clearinghouse in the UAE, then through a series of hawala networks to its final end beneficiary – it seems unreasonable to transfer all the AML/CFT risk to the bank where the transaction originates, and yet banks currently face endless liability for the transaction. Reducing the AML/CFT risk associated with Know Your Customer's Customers obligations will further alter the payoff matrix in support of financial inclusion.

These recommendations fit into a broader need to reconsider the zero tolerance approach to AML/CFT in the formal financial system. There should be room for banks to make "honest mistakes," especially considering that illicit actors will always find ways around the formal financial system. Tolerance for honest mistakes may lead to a moral hazard problem concerning AML/CFT violations, but there is indirect evidence that regulators are competent at distinguishing intentional transgressions.

If tolerance for honest mistakes is not embraced, continuing on the current path of de-risking and prioritizing integrity over inclusion will result in the rise of viable alternatives to the regulated financial system, diminishing the benefit of AML/CFT regulations. Regulators should instead seek to prioritize inclusion beyond statements of its importance. It does no good for the FATF to talk about inclusion, when banks still shoulder the AML/CFT risk of their customers and their customers' customers.

V. Conclusion

AML/CFT regulations have resulted in the unintended consequence of de-risking, which has impacted a range of constituencies due to a combination of regulatory risk and business drivers. This paper conducted an economic analysis of qualitative data to gain a broad understanding of the impact of AML/CFT regulations and concluded that the problem, which is rooted in regulatory risk and uncertainty, warrants a reconsideration of the enforcement approach. Recommendations sought to reduce uncertainty and the regulatory burden placed on financial institutions in order to reorient the payoff matrix towards supporting financial inclusion. Ideally, as the price of regulatory risk is reevaluated, there will be increased opportunities for financial institutions to explore market solutions to the broader challenges associated with financial inclusion, which will serve to reinforce the integrity of the international financial system.

Interviews

Interview 1: Director for Middle East Issues, Office of Terrorist Financing and Financial Crimes, U.S. Treasury Department.

Interview 2: Analyst, Office of Threat Finance Countermeasures, Bureau of Economics and Business Affairs, U.S. State Department.

Interview 3: Former Special Adviser to the Under Secretary of Treasury for Terrorism and Financial Intelligence, U.S. Treasury Department.

Interview 4: Consultant, Deloitte.

References

"American regulators wield a big stick, but not always fairly," The Economist, 27 February 2016, http://www.economist.com/news/finance-and-economics/21693603-american-regulators-wield-big-stick-not-always-fairly-whoops-apocalypse

"Bank Secrecy Act" Pub. L. No. 91-508, 84 Stat. 1114-1124 (1970)

Barry, R. and Ensign, R. L. 2016. "Losing Count: U.S. Terror Rules Drive Money Underground", *The Wall Street Journal*, http://www.wsj.com/articles/losing-count-u-s-terror-rules-drive-money-underground-1459349211

Bester, H. 2008. "Implementing FATF Standards in Developing Countries and Financial Inclusion: Findings and Guidelines," World Bank, www.cenfri.org/documents/AML/AML_CFT percent20and percent20Financial percent20Inclusion.pdf.

Cockayne, J. and Shetret, L. 2012. "Capitalizing on Trust: Harnessing Somali Remittances for Counterterrorism, Human Rights and State Building," Global Center on Cooperative Security, http://globalcenter.org/wp-content/uploads/2012/07/CapitalizingOnTrust.pdf

Curry, T. J. 2016. "Remarks Before the Institute of International Bankers," Washington, D.C., http://www.occ.treas.gov/news-issuances/speeches/2016/pub-speech-2016-25.pdf

Durney, T. and Shetret, L. (November 2015), "Understanding Bank De-Risking and Effects on Financial Inclusion", Global Center on Cooperative Security, http://www.globalcenter.org/wp-content/uploads/2015/11/rr-bank-de-risking-181115-en.pdf

"BNP Paribas Agrees To Plead Guilty and To Pay $8.9 Billion for Illegally Processing Financial Transactions for Countries Subject to US Economic Sanctions," Department of Justice, 30 June 2014, http://www.justice.gov/opa/pr/bnp-paribas-agrees-plead-guilty-and-pay-89-billion-illegally- processing-financial

Department of Treasury 2005. "US Money Laundering Threat Assessment," http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/mlta.pdf

Coker, M. 2016. "How Islamic State's Secret Banking Network Prospers," *The Wall Street Journal*, http://www.wsj.com/articles/how-islamic-states-secret-banking-network-prospers-1456332138?mod=djemalertNEWS

FATF 2015. "*Emerging terrorist Financing Risks,"* http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

FATF 2013a. "Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion," http://www.fatf-gafi.org/topics/financialinclusion/documents/revisedguidanceonamlcftandfinancialinclusion.html

FATF 2013b. "*The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing,"* http://www.fatf-gafi.org/media/fatf/documents/reports/Role-of-hawala-and-similar-in-ml-tf.pdf

FATF 2015. "*Emerging terrorist Financing Risks,"* http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

FinCEN 2014. "FinCEN Statement on Providing Banking Services to MSBs," http://www.fincen.gov/news_room/nr/html/20141110.html

Global Center on Cooperative Security Report 2015. "Hanging by a Thread: The Ongoing Threat to Somalia's Remittance Lifeline," https://www.oxfam.org/sites/www.oxfam.org/files/file_attachments/bn-hanging-by-thread- somalia-remittances-190215-en.pdf

King, R. G., & Levine, R.. (1993). Finance and Growth: Schumpeter Might be Right. *The Quarterly Journal of Economics*, *108*(3), 717–737. Retrieved from http://www.jstor.org/stable/2118406

"KPMG Global Anti-Money Laundering Survey," KPMG LLP, 2014, http://www.kpmg.com/KY/en/IssuesAndInsights/ArticlesPublications/PublishingImages/global- anti-money-laundering-survey-v3.pdf Parry, H. 2014, "Money laundering and Sanctions Compliance—A Survey of Global Trends," Thomson Reuters white paper, https://risk.thomsonreuters.com/sites/default/files/GRC01413.pdf

Lew, J. 2016. "Remarks of Secretary Lew on the Evolution of Sanctions and Lessons for the Future at the Carnegie Endowment for International Peace," https://www.treasury.gov/press-center/press-releases/Pages/jl0398.aspx

Makin, P. and Clark, D. 2014. "Safer Corridor for Remittances," FSD Africa, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/306312/Safe- corridors-Remittance-technology-options.pdf

Nakamura, L. Leonard I. Nakamura: "Information Externalities: Why Lending May Sometimes Need a Jump Start", Business Review, January/February 1993

Ranis, G., Stewart F. and Ramirez A. 2000. "Economic Growth and Human Development," *World Development* 28, no. 2, 197-219. http://www.econ.yale.edu/~granis/papers/cp0546.pdf

Rushe, D. "Standard Chartered fined $300m by US financial watchdog," *The Guardian*, August 20, 2014.

Shasky Calvery, J. FinCEN Director, 2015. "Remarks Delivered at the Predictive Analytics World for Government Conference", Washington, D.C., https://www.fincen.gov/news_room/speech/pdf/20151013.pdf

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001," Pub. L. No. 107-56, 115 Stat. 272 (2001), http://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf.

Viswanatha, A. and Wolf, B. "HSBC to pay $1.9 billion U.S. fine in money-laundering case", Reuters, Dec 11 2012;
http://www.reuters.com/article/us-hsbc-probe-idUSBRE8BA05M20121211

Wolfsberg Group 2014. "Wolfsberg Anti-Money Laundering Principles for Correspondent Banking," http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg-Correspondent-Banking- Principles-2014.pdf

World Bank. 2015. “Fact finding summary from de-risking survey,” http://documents.worldbank.org/curated/en/2015/11/25481336/fact-finding-summary-de-risking-surveys

Zarate, J. C. (2013). *Treasury's war: The unleashing of a new era of financial warfare*. PublicAffairs.