Vanderbilt Journal of Transnational Law

Volume 51
Issue 4 *October 2018*

Article 4

2018

Sustaining the Growth of Mobile Money Services in Developing Nations: Lessons from Overregulation in the United States

Amanda B. Kernan

Sustaining the Growth of Mobile Money Services in Developing Nations: Lessons from Overregulation in the United States

*Amanda Bloch Kernan**

ABSTRACT

Billions of people around the world are excluded from the formal financial system and forced to store, transfer, and borrow money by using inefficient and unsafe methods. The recent introduction of mobile money programs in developing countries is revolutionizing financial inclusion by allowing users to store and transfer money on their mobile phones, thereby eliminating the need to access a bank or an internet connection. Unfortunately, fears that these programs will be used to launder money and finance terrorism have led the international community to develop and implement restrictive anti-money laundering policies that will likely impede the growth and accessibility of these programs. This Article posits that these policies will ultimately cause financial institutions to terminate relationships with mobile money providers, resulting in less secure mobile money transactions and more transactions taking place through the informal economy. This conclusion is based on the history of money-service businesses in the United States, which lost access to financial services due to severe penalties, overzealous regulators, and stringent anti-money laundering regulations that were applied in unpredictable ways.

This Article encourages the international community to look to gatekeeper theory to create an anti-money laundering regime that incentivizes financial institutions to remain in the mobile money industry. By applying gatekeeper theory and creating an optimal liability regime, the international community will be able to incentivize financial institutions to remain in the industry while compelling them to dedicate the proper amount of resources

---

* I am very grateful to Helen Scott, Gerald Rosenfeld, and Karen Brenner of the Jacobson Leadership Program in Law and Business at NYU School of Law for their support on this Article. I also owe substantial appreciation to Emily Winston, Sarah Hewitt, and Sherry Wicker for their thoughtful comments and guidance. All errors are my own.

toward identifying and preventing money laundering and terrorist financing.

TABLE OF CONTENTS

I. INTRODUCTION

In Bangladesh, Sabina Begum works long hours as a seamstress and provides the only financial support for her parents and daughter, who live in a village three hundred kilometers away.[1] She does not have time to go to a bank and her only day off is during the weekend, when the bank is closed. In the past, she had to use a transport to send money to her family. She explained, "I used to give the money to bus drivers headed that way. Sometimes the money got lost or arrived late."[2] Now, Sabina goes to a local grocer every month, pays a small fee, and the grocer transfers money via a mobile phone to a tea shop in her family's village, where her father picks up the money.[3]

In Malawi, where thousands of people are suffering from hunger due to a drought, the Malawi Red Cross Society is utilizing mobile payments to feed ten thousand hunger victims in the country.[4] The organization provides mobile phones to its beneficiaries and sends families a monthly cash transfer of approximately USD$43. This cash allows families to purchase, over a five-month period, a fifty-kilogram bag of maize, five kilograms of beans, and two liters of cooking oil.[5]

In Liberia, teachers in remote locations often travel long distances to receive their salaries and are further burdened by administrative failures, logistical challenges related to the transport of cash, and corruption, which all tend to prevent teachers from receiving payment in full and on time. These breakdowns are devastating to education systems and the surrounding communities. In response, the Liberian government and the United States Agency for International Development (USAID) launched a program to pay rural teachers' salaries directly through mobile money platforms.[6] This pilot program aims to guarantee teachers their full salaries and prevent teachers from abandoning their classrooms for days at a time in order to withdraw their salaries from formal financial institutions.

These stories are becoming commonplace throughout the developing world. Mobile money platforms are providing populations

---

1. *See* Syed Zain Al-Mahmood, *Mobile Banking Provides Lifeline for Bangladeshis*, WALL ST. J. (June 23, 2015, 10:15 PM), http://www.wsj.com/articles/mobile-banking-provides-lifeline-for-bangladeshis-1435043314 [https://perma.cc/AE4G-LBVC] (archived Aug. 4, 2018).

2. *Id.*

3. *Id.*

4. *See* Mwayi Mkandawire, *Cash Transfers Helping Malawi Hunger Victims Survive*, MALAWI 24 (May 28, 2016), http://malawi24.com/2016/05/28/cash-transfers-helping-malawi-hunger-victims-survive/ [https://perma.cc/338E-5KN6] (archived Aug. 6, 2018).

5. *Id.*

6. *See* Arrington Ballah, *Gov't Launches Pilot Program to Pay Teachers' Salaries via Mobile Money*, BUSH CHICKEN (May 28, 2016), http://www.bushchicken.com/govt-launches-pilot-program-to-pay-teachers-salaries-via-mobile-money/ [https://perma.cc/VH6H-4J4J] (archived Aug. 6, 2018).

that have been excluded from the formal financial sector for generations—including poor migrants, women, and foreign aid recipients—with access to safe and secure financial services for the first time. By sending, receiving, and storing money on mobile phones, users are able to develop financial autonomy and avoid the risks associated with transacting in cash. Although mobile money programs are revolutionizing financial inclusion in the developing world, fears that these programs will be used to launder money and finance terrorism have led the international community to develop and implement restrictive anti-money laundering policies that will likely impede the growth and accessibility of these programs.

This Article argues that the anti-money laundering policies being promoted throughout the developing world will ultimately cause financial institutions to terminate relationships with mobile money providers, resulting in less-secure mobile money transactions and more transactions taking place through the informal economy. This conclusion is based, in part, on the history of money-service businesses in the United States, which lost access to financial services over the past decade due to overzealous regulators and excessive financial penalties related to financial institutions' anti-money laundering functions. The same policies that caused money-service businesses, which provide financial services for unbanked and underbanked communities in the United States, to go out of business are now being implemented in developing countries with respect to mobile money transactions.

In order to prevent financial institutions from refusing to participate in mobile money programs due to these restrictive anti-money laundering policies, this Article proposes that the international community look to gatekeeper theory to create a regime that incentivizes financial institutions to remain in the industry. The gatekeeper theory of liability imposes liability on professionals, or gatekeepers, for wrongs committed by their clients. Financial institutions providing services to money-service businesses in the United States were given gatekeeper-like responsibilities without the incentives required for a successful model, and international anti-money laundering policies are poised to cause the same result for financial institutions participating in mobile money transactions. A successful gatekeeper model requires, among other things, that the aggregate costs of wrongdoing exceed the aggregate costs of precaution, but this may not be the case when it comes to the current anti-money laundering regime. By applying gatekeeper theory, the international community will be able to encourage financial institutions to remain in the industry while compelling them to dedicate the proper amount of resources toward identifying and preventing money laundering and terrorist financing.

Part III of this Article sets forth the elements involved in a mobile money transaction and explores the implications of mobile money

programs on financial inclusion and financial integrity. Part III also discusses the regulation of mobile money across the world, particularly focusing on the Financial Action Task Force and its anti-money laundering Recommendations that are applicable to mobile money transactions.

Part IV provides an overview of the US anti-money laundering laws applicable to money-service businesses and explains how enforcement of those laws caused financial institutions to terminate their relationships with money-service businesses. This Part also demonstrates the similarities between US anti-money laundering laws and those being promoted in the international community.

Last, Part V proposes a solution to prevent international financial institutions from terminating their relationships with mobile money programs in the same way that US institutions terminated their relationships with money-service businesses. Because financial institutions are given gatekeeper-like responsibilities when it comes to preventing money laundering and terrorist financing, this Article argues that gatekeeper theory can be applied to create a functioning regime. In particular, it argues that the current policies will not lead to an optimal liability regime and discusses some of the ways in which an optimal liability regime can be achieved; that governments should increase the incentives for financial institutions to become and remain involved in mobile money transactions, including by offering corporate subsidies and rewards for identifying money launderers and terrorists; and that international governments should enable financial institutions to build reputational capital in the mobile money industry.

II. MOBILE MONEY SERVICES

Approximately 2.5 billion adults around the world lack access to a bank account. This unbanked population uses inefficient and unsafe methods to store money (often by hiding cash in their homes) and transfer money (often in person), and they are forced to pay exorbitant interest rates when borrowing money. While banks have not found it profitable to serve this population in the past, the Gates Foundation predicts that mobile phones will transform the lives of two billion poor people over the next fifteen years by providing them with access to bank accounts and financial services.[7] By allowing people to store and transfer money on their mobile phones, companies are serving poor customers in remote areas while profiting through small commissions on millions of transactions. This Part describes the technical aspects of

---

7. *See* BILL & MELINDA GATES FOUNDATION, OUR BIG BET FOR THE FUTURE: 2015 GATES ANNUAL LETTER 17 (2015), https://al2015.gatesnotesazure.com/assets/media/documents/2015_Gates_Annual_Letter_EN.pdf [https://perma.cc/9Q2T-AQ4Q] (archived Aug. 6, 2018).

a mobile money transaction, and then sets forth the financial inclusion benefits along with the financial integrity risks associated with mobile money programs.

A. *Mobile Money Transactions*

Mobile money is, essentially, a form of electronic money that requires neither a computer nor an internet connection. While most of the world lacks access to formal financial services, approximately 63 percent of the world's population owns a mobile device and most of the world is covered by mobile networks.[8] Through mobile money services, customers can convert cash into electronic money and vice versa through a nearby retail shop; store electronic value in the form of an account; and engage in electronic transactions, including sending remittances to family members in different locations and paying for goods and services.[9] The service consists of a financial service and a telecom service, and the provider of the financial service is required to comply with certain anti-money laundering requirements.

The Brookings Institution found that in 2014, sixteen markets had more mobile money accounts than bank accounts, and there were nearly three hundred million registered mobile money accounts globally.[10] While this number is promising, it represents only 8 percent of the mobile connections in the markets where mobile money services are available, meaning there are substantial opportunities to expand access to these services.[11]

While a variety of complex mobile money systems exist around the world, a study by the World Bank found that all mobile money transactions contain the same five elements or functions arranged in a specific order.[12] The first step always requires access to a mobile communications service, and this access is always provided by a mobile network operator (MNO).[13] MNOs provide both prepaid and postpaid services, depending on the MNO and the customer, and they are

---

8. *See Number of mobile phone users worldwide from 2015 to 2020 (in billions)*, STATISTA, https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/ (last visited Sept. 4, 2018) [https://perma.cc/R9Q4-NK53] (archived Aug. 6, 2018).

9. *See* Claire Alexandre & Lynn Chang Eisenhart, *Mobile Money as an Engine of Financial Inclusion and Lynchpin of Financial Integrity*, 8 WASH. J.L. TECH. & ARTS 285, 289 (2013).

10. JOHN D. VILLASENOR ET AL., THE 2015 BROOKINGS FINANCIAL AND DIGITAL INCLUSION PROJECT REPORT 8 (2015), http://www.brookings.edu/~/media/Research/Files/Reports/2015/08/financial-digital-inclusion-2015-villasenor-west-lewis/fdip2015.pdf?la=en [https://perma.cc/SRP2-LRML] (archived Aug. 6, 2018) [hereinafter BROOKINGS REPORT].

11. *Id.*

12. *See* PIERRE-LAURENT CHATAIN ET AL., PROTECTING MOBILE MONEY AGAINST FINANCIAL CRIMES: GLOBAL POLICY CHALLENGES AND SOLUTIONS 9–10 (2011).

13. *Id.* at 12.

generally prohibited by data and privacy laws from viewing the content of a mobile communication, meaning they are content neutral.[14]

The second step in a mobile money transaction is the customer interface, where a customer gives an order to the mobile money system and receives information in response.[15] The third step is transaction processing, which typically involves a central computer that automatically handles the transaction instructions received through the customer interface.[16] The transaction processor assesses the feasibility of a transaction—for instance, if a customer seeks to transfer money to another user, the processor verifies that the customer has sufficient funds in his account and that no transaction limits would be breached by the transfer.[17] The fourth step involves account provision, such as retaining account balance information and transaction histories.[18]

The fifth and final step is always settlement of the transaction, and this step is always performed by a financial institution.[19] Here, the money that a sender puts into the system is delivered to the recipient, minus any fees involved in the transaction. A settlement between two accounts at the same financial institution generally requires just a reconciling of the accounts, while a settlement between accounts at different institutions requires a bank to transfer money from one account to the other.[20]

Retail outlets play a central role in mobile money transactions—they are used to open accounts and exchange cash for credit in the system, or vice versa. The retail outlet acts as the customer interface for both the user and the mobile money system, and it generates a small fee for facilitating each transaction.[21] Generally, in order to open an account or transfer money, a customer will bring cash to the retail outlet, which then takes the cash and transfers money from its own account to the customer's account. When a customer seeks to withdraw cash from its account, the retail outlet transfers money from the customer's account to its own account, and provides the customer with

---

14. *Id.*
15. *Id.* at 13.
16. *Id.*
17. *Id.*
18. *Id.* at 14.
19. *Id.* at 12, 15. The term "financial institution" refers to any natural or legal person who accepts deposits and other repayable funds from the public by way of business and/or provides money or value transfer services to its customers but does not include natural or legal persons who solely provide telecom services. *See* FIN. ACTION TASK FORCE, INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION 117–18 (2018), http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf [https://perma.cc/7AJ5-K94C] (archived Aug. 6, 2018) [hereinafter FATF RECOMMENDATIONS].
20. *See* CHATAIN, *supra* note 12, at 14.
21. *See id.* at 16.

cash. Retail outlets are usually required to maintain accounts at a traditional financial institution, but their transaction amounts and frequency limits are higher than individual customers' limits.[22]

While the first and last functions are always provided by an MNO and a financial institution, respectively, the middle three functions can be performed by the MNO, a financial institution, or a third-party provider. For example, Safaricom in Kenya, arguably the most successful mobile money system in existence, is an MNO that performs the functions of customer interface, transaction processing, and account provision.[23] The bank's only role is to hold the money in the system in a trust account. It does not monitor or control the day-to-day transactions of customers, only "the withdrawals from and deposits to the system by retail outlets that have bank accounts at the same bank."[24] Celpay in the Democratic Republic of the Congo, on the other hand, is a third-party provider that performs the functions of customer interface, transaction processing, and account provision.[25] It contracts with MNOs and banks in order to provide its payment services to customers, and it uses its own staff members instead of retail outlets to process transactions and maintain account records.[26] Since it does not use retail outlets, customers must cash-in and cash-out at a bank that has an agreement with Celpay, meaning all customers must have access to the bank as well as a bank account.

B. *The Benefits of Mobile Money*

1. Financial Inclusion

Financial inclusion is an essential facet of economic development, and mobile money services offer individuals who have always relied on inefficient informal financial services access to the formal financial sector. By safely and securely storing and transferring money on a mobile device, customers avert the risks associated with storing and transferring cash in person, such as robbery, fraud, police corruption, accidental fires or infestations, and significant currency depreciation.[27] Poor migrants are able to easily and cheaply send remittances home through these services; it is estimated that nearly

---

22. *See id.* at 17.

23. *See id.* at 22 ("Safaricom manages the transaction to the point of settlement . . . [and] manages records, processes the transaction, and provides both the interface and the mobile service.").

24. *See id.*

25. *See id.* at 23.

26. *See id.* at 23–24.

27. *See* Shanthi Elizabeth Senthe, *Transformative Technology in Microfinance: Delivering Hope Electronically?*, 13 PITT. J. TECH. L. & POL'Y 1, 7 (2012) (discussing physical security risks of storing physical cash rather than storing it in a mobile bank account).

$440 billion in remittances were sent in 2010, 75 percent of which was sent to developing countries.[28] In fact, 43 percent of Kenya's gross domestic product is now transferred via mobile products.[29] As customers grow their money in an account, they gain financial autonomy and develop a relationship with a banking service. This promotes entrepreneurship, empowers those who have traditionally been excluded from formal financial channels, and gives customers hope for a better economic future.

The growth of mobile money systems is particularly significant for women, who lack access to the financial sector in many places.[30] As of 2014, there was a difference of 7 percentage points between the percentage of men and of women with accounts at a formal financial institution or mobile money provider (65 percent versus 58 percent, respectively).[31] Mobile money allows women to engage in personal or business transactions from any geographic location with a mobile device, including their own homes, without others knowing about the transactions or being able to access their accounts.[32] Women are additionally able to receive funds via digital financial services directly from the government, which enables governments to promote policies aimed at increasing women's financial inclusion in developing countries.[33]

The rapid growth of mobile banking is poised to revolutionize the world on a macroeconomic level as well, as poor communities in developing nations become market participants for the first time. When customers exchange cash for electronic money, capital becomes mobilized in areas that have always been spatially excluded from financial institutions. Mobile money allows wire remittances, foreign investment, and foreign aid to reach villages directly, lowering the transaction costs and risks of corruption and fraud that are associated with the transfer of cash, which is difficult to trace and fungible.[34] This is particularly true in post-conflict and fragile zones, where foreign aid is deftly needed but financial institutions and landline infrastructure

---

28. *See* Jane K. Winn, *Governance of Global Mobile Money Networks: The Role of Technical Standards*, 8 WASH. J.L. TECH. & ARTS 197, 207 (2013).

29. Arthur Velker, *The Digital Revolution that Will Democratize Wealth, Insights with Chris Skinner*, IRISH TECH NEWS (Feb. 4, 2018), https://irishtechnews.ie/the-digital-revolution-that-will-democratize-wealth-insights-with-chris-skinner/ [https://perma.cc/7LA9-RZFY] (archived Aug. 6, 2018). Remittances totaled $429 billion in 2016. *Id.*

30. BROOKINGS REPORT, *supra* note 10, at 7.

31. *Id.*

32. *See* Senthe, *supra* note 27, at 57.

33. *See* BROOKINGS REPORT, *supra* note 10, at 7.

34. *See id.* at 8 ("[I]n Mexico, the government saved an estimated $1.3 billion annually by shifting to electronic payments. Other governments, such as that of India, have recognized the value of digital transfers to reduce 'leakage'—payments that do not reach recipients.").

are weak.[35] Mobile phone companies tend to expand their services into these areas before other major enterprises, making mobile money a safer and more reliable way to send aid.[36] Similarly, "[p]eople working on the front lines in conflict areas, disaster zones, or health crises need to get paid. Mobile payments are a way to do that quickly and efficiently."[37]

In countries where the rule of law is weak, corruption is particularly prevalent. Corruption reduces economic growth by discouraging private investment.[38] By transitioning from anonymous cash transactions to traceable electronic transfers, the opportunity for and incidence of corruption will decline. And, as economic development and financial inclusion expand to poor communities, the level of poverty and poverty-related crimes in those areas will decrease as well.[39] A report from the Imperial College and Citi found that a 10 percent increase in digital money readiness along with a commensurate increase in adoption for the countries included in the study could help up to approximately 220 million individuals enter the formal financial sector.[40] "This translates to an additional $1 trillion moving from the informal economy to the formal economy."[41]

Mobile money not only allows individuals and communities to become financial participants, but it also generates a significant amount of data that can be used to fight crime and promote financial inclusion initiatives and economic development. Regulators, for instance, can collect data from MNOs and financial institutions to identify and trace money laundering and terrorist financing transactions. Foreign aid organizations and private investors can analyze the data to better understand where their money is actually going and the efficacy of their programs.[42] For all of these reasons, mobile money programs represent a groundbreaking opportunity to improve the lives of disadvantaged people across the globe.

---

35. *See* Emery S. Kobor, *The Role of Anti-Money Laundering Law in Mobile Money Systems in Developing Countries*, 8 WASH. J.L. TECH. & ARTS 303, 308–10 (2013).

36. *See* CHATAIN, *supra* note 12, at 158 (discussing the importance of the expansion of mobile money services for financial inclusion, reduction of transaction costs, and improvement of nations' payment infrastructures).

37. Sue-Lynn Moses, *Dethroning Cash as King. Why These Major Funders Are So Hyped About Digital Money*, INSIDE PHILANTHROPY (May 27, 2016), http://www.insidephilanthropy.com/home/2016/5/27/dethroning-cash-as-king-why-these-major-funders-are-so-hyped.html [https://perma.cc/6F8K-TGPM] (archived Aug. 6, 2018).

38. Kobor, *supra* note 35, at 310.

39. *See* CHATAIN, *supra* note 12, at 145.

40. *See* BROOKINGS REPORT, *supra* note 10, at 7.

41. *Id.*

42. *See* Colin C. Richard, *How the U.S. Government's Market Activities Can Bolster Mobile Banking Abroad*, 88 WASH. U. L. REV. 765, 768 (2011).

2. Financial Integrity

By decreasing the use of cash and increasing the accessibility, safety, and traceability of financial transactions, mobile money programs have proven to promote financial inclusion and economic development. Therefore, governments around the world should be doing everything in their power to expand and protect the scope of these services. However, accompanying the development of mobile money systems are a plethora of risks, some actual and some perceived, that draw attention from both consumers and financial regulators, and fear of these risks carries the potential to restrain the growth of safe mobile money services.

In order for users, especially those who have always stored their money in cash, to "buy in" to mobile money and utilize the services being offered, they must feel confident that they can trust the system. Some of the financial integrity risks to consumers include fraud, such as SIM card skimming and swaps; technology risks and failures that could result in lost or stolen money; data and privacy breaches that could result in a consumer's identity being stolen or personal information being used by governments for improper purposes; and agent misconduct by the retail outlet or an employee in the system that could cause financial loss.[43]

Financial regulators and international governments are concerned with the stability and integrity of the financial system. There is substantial fear that mobile money channels will be used to launder money and finance terrorism. In a typical money laundering scenario, money is introduced into the financial system and then moved through several accounts (known as "layering") in order to obfuscate the origin of the funds.[44] The money can ultimately be returned to the money launderer, appearing as though it is from a legitimate source.[45] Money laundering is used by drug traffickers, arms dealers, and terrorists to enable criminal activity and utilize formal financial services, which are safer and cheaper than transacting in cash.[46] Mobile money programs rely on vast networks of agents to provide cash-in and out services, complicating the already difficult process of identifying and monitoring suspicious transactions and parties.

---

43. *See* Jamie M. Zimmerman, *The Emergence of Responsible Digital Finance*, CTR. FOR FIN. INCLUSION (July 21, 2014), http://cfi-blog.org/2014/07/21/the-emergence-of-responsible-digital-finance/ [https://perma.cc/QGW8-R8UW] (archived Aug. 6, 2018) (discussing the risks related to digital financial services).

44. *See* CHATAIN, *supra* note 12, at 35.

45. *See* Leslie Gutierrez, *Bolstering Competition in the International Remittance Market: A Proposal for Reforming the Current Regulatory Licensing Framework Governing Money Transmission Businesses*, 10 HASTINGS BUS. L.J. 207, 211 (2014).

46. *Id.* at 212.

The World Bank identified four primary risk categories that are currently guiding efforts to develop anti-money laundering legislation applicable to mobile money transactions: anonymity, elusiveness, rapidity, and poor oversight.[47]

Anonymity: The risk that a criminal gains access to mobile money services using a false identity. These risks are higher in countries with weak national identification frameworks or methods to verify a person's identity and are compounded by the fact that mobile money transactions often do not require face-to-face engagement.[48]

Elusiveness: The risk that criminals can use methods, such as mobile phone pooling and microstructuring (keeping transactions below the money laundering threshold), to prevent the detection of money laundering.[49]

Rapidity: The risk that criminals can use mobile money programs quickly and anywhere, aiding efforts to layer a transaction and obscuring the origin of funds to complicate a transaction.[50]

Poor oversight: Newly developed mobile money programs may fall outside the purview of current anti-money laundering regimes in certain countries, creating conditions that increase the likelihood of abuse arising from the three previous risks.[51]

Regulators are also concerned about the systemic risk inherent in the rise of successful mobile money programs. Monopolies are likely to emerge at multiple phases in the system. Due to the principal-agent relationship involved in most mobile money transactions, financial institutions retain legal responsibility for actions committed by retail outlets.[52] In order to manage those risks, financial institutions may deny agency status to independent players, locking them out of the system.[53] Moreover, most MNO-led models concentrate transaction activities in the hands of one or two telecom companies.[54] These companies maintain industry dominance and, in turn, concentrate the settlement of mobile money transactions in the hands of one or two financial institutions.[55] Interruptions to the mobile network service or a financial institution's ability to complete transactions could have a

---

47. *See* CHATAIN, *supra* note 12, at 33–35.
48. *See id.* at 33.
49. *See id.* at 34–35.
50. *See id.* at 35.
51. *See id.* at 35–36.
52. *See* Ignacio Mas, *Shifting Branchless Banking Regulation from Enabling to Fostering Competition*, 30 BANKING FIN. L. REV. 179, 185 (2015) (discussing the principal-agent relationship between financial institutions and retail outlets).
53. *See id.* at 185–86.
54. *See* Maria C. Stephens, *Promoting Responsible Financial Inclusion: A Risk Based Approach to Supporting Mobile Financial Services Expansion*, 27 BANKING FIN. L. REV. 329, 333 (2012).
55. *Id.*

catastrophic impact on the mobile money system in a country.[56] This risk is compounded by the fact that regulators will be more likely to focus their investigations on the few companies or institutions dominating the market, which, as discussed below, could cause participants to exit the industry.

Despite these risks, mobile money programs enable poor users to access safe financial channels, and governments should put substantial efforts and resources into promoting and expanding these programs.

III. INTERNATIONAL REGULATION OF MOBILE MONEY

Although many international governments realize the success of mobile money programs and are attempting to promote financial inclusion, many of the anti-money laundering policies developed to safeguard the integrity of the financial system will have the likely impact of hindering the growth and accessibility of safe mobile money services. This dilemma is rooted in the world's anti-money laundering laws and complicated by the fact that expanding financial services to the world's poor is not a particularly profitable enterprise.[57] This Part will describe the Financial Action Task Force (FATF), which guides and assesses international anti-money laundering laws, and will set forth the FATF Recommendations that are relevant to mobile money transactions.

A. *The Financial Action Task Force (FATF)*

The FATF was established in 1989 as a temporary intergovernmental task force in response to the United Nations' universal pledge to prevent money laundering.[58] Its development can be traced to the United States' "War on Drugs," which brought money laundering into the spotlight for the first time.[59] Due to the international component of money laundering, the G7 nations, led by the United States, created the FATF and quickly enacted a set of common standards, known as the "40 Recommendations," which were intended to be nonbinding benchmarks that governments could use to

---

56. *See id.*

57. *See* Richard K. Gordon, *Losing the War Against Dirty Money: Rethinking Global Standards on Preventing Money Laundering and Terrorism Financing*, 21 DUKE J. COMP. & INT'L L. 503, 505, 531 (2011) (discussing economic incentives, or lack thereof, faced by private institutions for complying with anti-money laundering laws).

58. *See* Winn, *supra* note 28, at 210.

59. *See* Ben Hayes, *Counter-Terrorism, "Policy Laundering," and the FATF: Legalizing Surveillance, Regulating Civil Society*, 14 INT'L J. NOT-FOR-PROFIT L. 5, 11 (2012).

formulate national anti-money laundering legislation.[60] Following the terrorist attacks of September 11, 2001, the FATF added eight (later nine) Special Recommendations on Terrorism Financing.[61]

Despite the fact that the FATF is only made up of thirty-six members and remains an informal international organization today, it has been extremely successful in guiding anti-money laundering legislation and enforcement regimes across the world. Over 180 jurisdictions along with the United Nations, the World Bank, and the International Monetary Fund (IMF) endorse the FATF standards.[62] The FATF's success and influence stem from its dual system of evaluation and enforcement. In 2002, the IMF, the World Bank, and the FATF agreed to a uniform system of assessment, including self-assessment and mutual assessment, to determine whether individual countries are adequately implementing the standards.[63] If a country fails the assessment, it may be subject to broad sanctions or countermeasures, such as a ban on states and external financial institutions doing business with financial institutions located within the assessed country.[64] This compliance system applies to both member and non-member countries, and the threat of economic penalties has led most countries to enact legislation in accordance with the FATF Recommendations.[65]

In the early 2000s, evidence emerged showing that vague rules coupled with conservative regulators were impeding the growth of innovative financial services.[66] In 2003, the FATF updated the Recommendations to allow countries and financial institutions to apply a risk-based approach to anti-money laundering frameworks.[67] Under the risk-based approach, countries may exclude activity from anti-money laundering regulation where the activity poses a limited risk of money laundering or terrorist financing.

> Institutions were urged to consider adopting a [risk-based approach] in terms of which customers, transactions, and services were divided into high-, standard-, and low-risk bands. Enhanced due diligence was required in cases where a high risk was identified. In cases where low risk was assessed, regulators could allow, and institutions could consider employing, simplified due diligence measures.[68]

---

60. *See id.* at 12.
61. *See id.*
62. *See* Winn, *supra* note 28, at 210.
63. Gordon, *supra* note 57, at 506.
64. *See id.* at 506–07.
65. *See* Louis de Koker, *The 2012 Revised FATF Recommendations: Assessing and Mitigating Mobile Money Integrity Risks Within the New Standards Framework*, 8 WASH. J.L. TECH. & ARTS 165, 168 (2015).
66. *See id.* at 168–69.
67. *See id.* at 169.
68. *See id.* at 170.

Due to ambiguity in the rules, countries feared the FATF would disagree with a given risk assessment, so they decided not to apply risk-based approaches. The FATF issued guidance on implementing an adequate risk-based approach in 2007,[69] but the guidance focused on identifying high-risk scenarios as opposed to low-risk scenarios.[70] In 2011, the FATF issued a guidance paper on financial inclusion that set forth steps that countries could take to promote financial inclusion while enforcing appropriate anti-money laundering (AML) policies.[71] Two years later, it published guidance meant to support the creation of AML/CFT[72] measures that could meet the goal of increasing financial inclusion while continuing to effectively combat money laundering and terrorist financing.[73] And, more recently, the FATF released a supplement that provides examples of countries' customer due diligence (CDD) measures adapted to the context of financial inclusion, with a specific focus on digital financial services.[74]

B. *FATF Recommendations Relevant to Mobile Money Networks*

The FATF Recommendations distribute responsibility for preventing money laundering and terrorist financing among the private and public sectors. While the Recommendations have been revised over time, the standards have always (1) required financial institutions to engage in customer due diligence, monitor customer transactions, and report suspicious activity to law enforcement, and (2) required governments to enact adequate legislation, supervise institutions, provide guidance regarding anti-money laundering and counter-terrorist financing programs, and investigate reports of

---

69. FIN. ACTION TASK FORCE, GUIDANCE ON THE RISK-BASED APPROACH TO COMBATING MONEY LAUNDERING AND TERRORIST FINANCING: HIGH LEVEL PRINCIPLES AND PROCEDURES (June 2007), http://www.fatf-gafi.org/media/fatf/documents/reports/High%20Level%20Principles%20and%20Procedures.pdf [https://perma.cc/3KLY-6XTS] (archived Sept. 5, 2018).

70. *See* de Koker, *supra* note 65, at 170.

71. FIN. ACTION TASK FORCE, ANTI-MONEY LAUNDERING AND TERRORIST FINANCING MEASURES AND FINANCIAL INCLUSION (June 2011), http://www.fatf-gafi.org/media/fatf/content/images/AML%20CFT%20measures%20and%20financial%20inclusion.pdf [https://perma.cc/SK2G-Q7SN] (archived Aug. 5, 2018) [hereinafter FATF ANTI-MONEY].

72. CFT stands for "combatting the financing of terrorism."

73. FIN. ACTION TASK FORCE, REVISED GUIDANCE ON AML/CFT MEASURES AND FINANCIAL INCLUSION (Feb. 2013), http://www.fatf-gafi.org/media/fatf/documents/reports/AML_CFT_Measures_and_Financial_Inclusion_2013.pdf [https://perma.cc/C7V8DMUY] (archived Sept. 5, 2018).

74. FIN. ACTION TASK FORCE, FATF GUIDANCE ON AML/CFT MEASURES AND FINANCIAL INCLUSION, WITH A SUPPLEMENT ON CUSTOMER DUE DILIGENCE (Nov. 2017), http://www.fatf-gafi.org/media/fatf/content/images/Updated-2017-FATF-2013-Guidance.pdf [https://perma.cc/S32B-FVG7] (archived Sept. 5, 2018). [hereinafter 2017 FATF GUIDANCE].

suspicious activity.[75] The primary objectives of the standards are to prevent criminals from accessing the financial system, identify criminals who have accessed the system, and open the flow of financial information from the private to the public sector to assist in investigations and prosecutions.[76]

The Recommendations applicable to the financial sector are designed to require that financial institutions identify their customers, gather information on an ongoing basis, create customer profiles, monitor transactions to ensure they are in line with the customer profiles, and report any suspicious activity that is not in line with the customer profiles to law enforcement.[77] Recommendation 10 requires that financial institutions identify and verify their customers' identities using reliable and independent source documents, and monitor their customers' transactions to ensure that the transactions being conducted are consistent with each customer's business and risk profile.[78] Institutions are also required to identify the beneficial owner of a customer and take reasonable measures to understand the ownership and control structure of the customer.[79] Recommendation 11 requires financial institutions to maintain transaction and account records for a period of five years in order to provide transactional information to law enforcement. [80] Financial institutions must maintain ongoing customer due diligence programs and promptly report any activity to a national financial intelligence unit that the institution suspects or has reasonable grounds to suspect involves funds that are the proceeds of a criminal activity or that are related to terrorism financing.[81]

It is important to note that financial institutions are required to design and implement their own preventive measures systems. [82] While governments must establish guidelines and provide feedback to assist financial institutions in this process, the Recommendations do not specify how institutions should design or implement these systems.

Both countries and financial institutions are required to identify and assess the money laundering and terrorist financing risks that may arise in relation to the development of new products and business practices, and the use of new or developing technologies for both new

---

75. *See, e.g., id.*; Gordon, *supra* note 57, at 511.

76. *See* Gordon, *supra* note 57, at 511 (discussing the main objectives of these FATF Recommendations).

77. *See* Model Regulation (2006) (on file with the U.N. Office on Drugs and Crime); Gordon, *supra* note 57, at 511.

78. FATF RECOMMENDATIONS, *supra* note 19, at 12.

79. *Id.* For country examples of simplified customer due diligence requirements regarding mobile money accounts, see 2017 FATF GUIDANCE, *supra* note 74, at 22.

80. FATF RECOMMENDATIONS, *supra* note 19, at 12.

81. *Id.* at 20.

82. *Id.* at 18.

and preexisting products.[83] There are various Recommendations specifically addressing money or value transfer services (MVTS) that apply to mobile money transactions.[84] Pursuant to Recommendation 14, providers of MVTS must be licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant FATF measures.[85] Recommendation 16 requires financial institutions to include originator information in wire transfer messages and to continue monitoring wire transfers to ensure the information remains with the transfer throughout the payment chain.[86] It also requires institutions to ensure they can take freezing action or prevent prohibited transactions when required by UN Security Council resolutions for the prevention and suppression of terrorism and terrorist financing.[87] Recommendation 17 does allow a financial institution to rely on third parties to perform customer due diligence, provided that certain requirements are met, but the financial institution maintains accountability for actions of its agents.[88]

Recommendations 26 to 35 address the responsibilities of government and law enforcement. Recommendations 26 and 27 require countries to ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations; that financial institutions are licensed or registered; and that supervisors have adequate powers to supervise, monitor, and ensure compliance by financial institutions.[89] Included in the supervisors' powers must be the power to compel production of "any information . . . that is relevant to monitoring such compliance, and to impose sanctions" for failure to comply.[90] Recommendation 29 requires countries to establish a Financial Intelligence Unit (FIU) that receives, analyzes, and disseminates suspicious transaction reports and other information regarding potential money laundering or terrorist financing. FIUs must also have access on a timely basis to the financial, administrative, and law enforcement information that they require to undertake their functions.[91] Countries must grant law

---

83. *Id.* at 15.

84. De Koker, *supra* note 65, at 178. An MVTS is defined as a financial service that involves the acceptance of cash, checks, other monetary instruments, or other stores of value, and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs.

85. FATF RECOMMENDATIONS, *supra* note 19, at 14.

86. *Id.* at 16.

87. *Id.*

88. *See* 2017 FATF GUIDANCE, *supra* note 74, at 23. This is particularly relevant to the mobile money context due to the participation of agents in mobile money transactions.

89. *Id.* at 27; FATF RECOMMENDATIONS, *supra* note 19, at 26.

90. FATF RECOMMENDATIONS, *supra* note 19, at 26.

91. *Id.* at 29.

enforcement authorities the ability to undertake money laundering and terrorist financing investigations, including the authority to access records kept by financial institutions, and must require law enforcement to appropriately conduct these investigations. [92] Last, countries must ensure there are a "range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with" persons that fail to comply with anti-money laundering and counter-terrorist financing requirements.[93]

The FATF 2017 Guidance recognizes that "applying an overly cautious, non-risk-based approach to AML/CFT safeguards when providing financial services . . . can have the unintended consequence of excluding legitimate consumers and businesses from the regulated financial system." [94] It therefore encourages countries, in certain lower-risk situations, to implement simplified customer due diligence measures and apply a risk-based approach to support access to basic financial services for unbanked and underbanked persons.[95]

IV. LESSONS FROM THE UNITED STATES: THE IMPACT OF RESTRICTIVE ANTI-MONEY LAUNDERING REGULATIONS AND ENFORCEMENT ON MONEY-SERVICE BUSINESSES

Money-Service Businesses (MSBs) are nonbank institutions that provide a myriad of financial services, often to unbanked and underbanked populations. [96] They include currency dealers or exchangers, check cashers, money order and traveler's check issuers, and money transmitters. [97] The Financial Crimes Enforcement Network (FinCEN) recognizes that "MSBs play an important role in a transparent financial system, particularly because they often provide financial services to people less likely to use traditional banking services and because of their prominent role in providing remittance services." [98] Nevertheless, legislative and enforcement actions over the past decade have resulted in financial institutions refusing to bank MSBs in the United States, causing them to go out of business. If international governments establish and implement anti-money laundering laws consistent with the FATF Recommendations, there is a strong possibility that international financial institutions will

92. *Id.* at 30–31.
93. *Id.* at 35.
94. 2017 FATF GUIDANCE, *supra* note 74, at 4.
95. *Id.*
96. FIN. CRIMES ENFORCEMENT NETWORK, STATEMENT ON PROVIDING BANKING SERVICES TO MONEY SERVICES BUSINESSES (Nov. 10, 2014), https://www.fincen.gov/sites/default/files/news_release/20141110.pdf [https://perma.cc/GUS2-7NRC] (archived Sept. 5, 2018) [hereinafter 2014 FINCEN STATEMENT].
97. *Id.*
98. *Id.*

similarly refuse to participate in mobile money transactions, since they will face the same types of issues that caused US financial institutions to terminate their MSB relationships.

This Part will provide a brief overview of US anti-money laundering laws, demonstrate the similarity between US anti-money laundering laws and the FATF Recommendations, and show how enforcement of US anti-money laundering laws caused financial institutions to terminate their relationships with MSBs, ultimately causing vulnerable populations to lose access to financial services and sending financial transactions underground.

A. *The United States' Anti-Money Laundering Regime*

The United States' anti-money laundering laws, in accordance with the FATF Recommendations, require covered institutions to comply with customer due diligence (which includes identifying and verifying the customer and monitoring customer activity), record-keeping, and suspicious activity reporting requirements.[99] Covered institutions include, among others, depository institutions, securities and futures industries, money-service businesses, and casinos.[100] Congress first enacted the Currency and Foreign Transactions Reporting Act, commonly referred to as the Bank Secrecy Act (BSA), in 1970.[101] The BSA has been amended and supplemented numerous times over the years as the government has intensified its focus on money laundering due to its connection first with drug trafficking and subsequently with terrorism.[102] The initial goal of the BSA was to detect, deter, and prevent money laundering by requiring financial institutions to report cash transactions in excess of $10,000 and maintain records of financial transactions.[103]

In 1992, Congress enacted the Annunzio-Wylie Anti-Money Laundering Act, which required covered institutions to file suspicious activity reports (SARs) detailing transactions identified as suspicious

---

99. Over time, the United States has updated and amended its anti-money laundering laws in response to the FATF Recommendations. *See History of Anti-Money Laundering Laws*, FIN. CRIMES ENFORCEMENT NETWORK, https://www.fincen.gov/history-anti-money-laundering-laws (last visited Sept. 5, 2018) [https://perma.cc/S7YA-SCBU] (archived Aug. 5, 2018) [hereinafter FinCEN *Anti-Money*]. It underwent the mutual evaluation processes in 2005–06 and 2015–16, and the Treasury has been responsible for improving anti-money laundering systems deemed non-compliant. *See* FATF ANTI-MONEY, *supra* note 71.

100. *See* FinCEN *Anti-Money*, *supra* note 99.

101. Currency and Foreign Transactions Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114 [hereinafter Bank Secrecy Act] (codified as amended in scattered sections of 31 U.S.C.).

102. *See* FinCEN *Anti-Money*, *supra* note 99 (including a history of U.S. anti-money laundering laws).

103. *See id.* (describing the goals of the anti-money laundering laws).

with FinCEN.[104] FinCEN was created by the Treasury and is primarily responsible for enforcing BSA regulations, though a variety of other government agencies and actors have become involved in anti-money laundering enforcement over the years.[105] A covered institution must file a SAR if it knows, suspects, or has reason to know or suspect that a transaction involves a financial crime or has no business purpose.[106] The information contained in SARs is vital to law enforcement efforts to combat money laundering and other financial crimes, and SARs are often used as a starting point for federal investigations into these crimes. In order to encourage institutions to assist the government in curtailing financial crimes, Congress added a safe harbor provision to the Annunzio-Wylie Anti-Money Laundering Act that provides immunity to a reporter for civil liability arising from a SAR.[107] However, courts are split on whether this grant of immunity is absolute or qualified based on the reporter having a "good faith basis" for filing the SAR.[108]

In 1994, Congress passed the Money Laundering Suppression Act, which requires MSBs to register with FinCEN.[109] MSBs are defined as entities that accept or transmit money; they are subject to SAR reporting requirements; and they must maintain detailed financial records and implement anti-money laundering programs.[110]

Federal anti-money laundering laws were enhanced significantly following the terrorist attacks of September 11, 2001. The US government determined that some of the hijackers received a total of $110,000 that originated in a United Arab Emirates bank and was sent

---

104. Annunzio-Wylie Anti-Money Laundering Act, Title XV, Pub. L. No. 102-550, 106 Stat. 4044 (1992) (12 U.S.C. § 1811); *see also* FinCEN *Anti-Money*, *supra* note 99.

105. *See* Cynthia J. Larose, *International Money Laundering Abatement and Anti-Terrorism Financing Act of 2001*, 30 J.C. & U.L. 417, 418 n.6 (2004) ("The FinCEN was created by administrative order in 1990 to provide other government agencies with an 'intelligence and analytical' network in support of the detection, investigation and prosecution on domestic and international money laundering and other crimes.") The PATRIOT Act gives FinCEN statutory life as a bureau within the Department of the Treasury. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 [hereinafter PATRIOT Act].

106. 12 C.F.R. § 353.3(b) (2017).

107. 31 U.S.C. § 5318(g)(3) (2012).

108. *See* Frank A. Mayer, III & Chad B. Holtzman, *The Need for Absolute Immunity When an Institution Submits a Suspicious Activity Report*, 32(2) BANKING & FIN. SERVS. POL'Y REP., Feb. 2014, at 14.

109. *See* FinCEN *Anti-Money*, *supra* note 99 (listing requirements of the Money Laundering Suppression Act).

110. *See* M. MacRae Robinson, *Easing the Burden on Mobile Payments: Resolving Current Deficiencies in Money Transmitter Regulation*, 18 N.C. BANKING INST. 553, 554–56 (2014) (describing the characteristics of MSBs).

to Florida Sun Trust Bank through formal financial channels.[111] Although the largest transaction of $69,000 was flagged as suspicious by the bank's anti-money laundering controls, the report was lost in the myriad of SARs that were generated by banks prior to the attacks.[112]

In response to the attacks, Congress enacted the USA PATRIOT Act, which made several additions to the BSA and enhanced the role of the Treasury and FinCEN.[113] The primary goal of the PATRIOT Act was to track and prevent transactions before they reached terrorists. Congress sought to achieve this goal by forcing transfers into formal channels and by tightening requirements on financial institutions to monitor those transfers.[114] The PATRIOT Act requires financial institutions to develop and implement an anti-money laundering program that establishes internal policies, procedures, and controls, a compliance officer, an ongoing employee-training program, and an independent audit function to test the program.[115] The PATRIOT Act also requires financial institutions to undertake additional customer due diligence, which includes customer identification procedures (institutions must verify a customer's name, birthdate, address, and identification number) prior to opening an account.[116] A new rule effective in May 2018 strengthened customer due diligence requirements on financial institutions by requiring them to identify and verify the beneficial owners of accounts, and maintain records on these beneficial owners.[117]

Federal anti-money laundering laws also focus on correspondent banking, which occurs where a financial institution carries out transactions on another institution's behalf. Due to the risk inherent in correspondent banking, financial institutions must also conduct due diligence on all non-US entities (such as foreign financial institutions) for which they maintain correspondent accounts.[118] Since 2006,

---

111. Bryan Mulcahey, *A Lose-Lose Scenario When the Federal Governments Starts a Theory with "Too Big": How the DOJ's AML Enforcement Policy Forces Remittances Underground*, 6 GEO. MASON J. INT'L COM. L. 107, 116 (2014).

112. *Id.* at 116–17.

113. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

114. *See* Mulcahey, *supra* note 111, at 117 (describing the main goal of anti-terrorism legislation after September 11, 2001).

115. 31 U.S.C. §§ 5311, 5318 (2012).

116. 31 U.S.C. § 5318 (2012).

117. *See* FIN. CRIMES ENFORCEMENT NETWORK, FREQUENTLY ASKED QUESTIONS REGARDING CUSTOMER DUE DILIGENCE REQUIREMENTS FOR FINANCIAL INSTITUTIONS (2016). https://www.ffiec.gov/bsa_aml_infobase/documents/FAQs_for_CDD_Final_Rule_(7_15_16).pdf [https://perma.cc/V86V-LDN8] (archived Aug. 5, 2018).

118. *See* 31 U.S.C. § 5318(i)(1) (2012); *see also* SEC, HSBC Deferred Prosecution Agreement Attachment A, http://www.justice.gov/opa/documents/hsbc/dpa-attachment-a.pdf (filed Dec. 11, 2012) [https://perma.cc/3HQ4-Q5S9] (archived Aug. 5, 2018)

financial institutions have monitored wire transfers to and from correspondent accounts using automated systems to track suspicious activity and are required to report suspicious activity to FinCEN.[119]

In addition, following the September 11 attacks, the Office of Foreign Assets and Control (OFAC) began to strictly enforce regulations and sanctions aimed at preventing transactions with persons or entities that could threaten national security.[120] Money transmission businesses are required to screen transactions to determine whether the sender or recipient of funds is listed on OFAC's Specially Designated National or Blocked Person (SDN) List, which identifies individuals and companies that may be connected with terrorism or drug trafficking.[121]

As shown in the chart in Appendix A, US anti-money laundering laws closely align with the FATF Recommendations.

B. *History of Enforcement & Result*

In 1997, over two hundred thousand MSBs operated in the United States, providing financial services estimated at $200 billion annually.[122] Over the past decade, strict enforcement of anti-money laundering laws by regulators coupled with numerous government investigations and massive settlement payments have caused banks to terminate their relationships with most MSBs. This has occurred notwithstanding the government continuously issuing policies and statements aimed at encouraging banks to continue banking MSB clients due to their critical role in providing financial services to unbanked and underbanked populations.

The US government began recognizing the adverse impact that an overly-conservative anti-money laundering regime could have on the MSB industry in early 2005. JP Morgan Chase and North Fork Bank,

---

[hereinafter SEC HSBC] (noting that correspondent accounts are high risk because the bank lacks a direct relationship with the customer that initiated the wire transfer).

119. *See* SEC HSBC, *supra* note 118.

120. *See Counterterror Initiatives in the Terror Finance Program, Focusing on the Role of the Anti-Money Laundering Regulatory Regime in the Financial War on Terrorism, Better Utilization of Technology, Increased Information Sharing, Developing Similar International Standards, and the Formation of Terrorist Financing Operations Section (TFOS) Before the S. Comm. on Banking, Housing & Urban Affairs*, 108th Cong. 193 (2004) (statement of R. Richard Newcomb, Director, Office of Foreign Assets Control).

121. *See Office of Foreign Assets Control—Sanctions Program and Information*, U.S. DEP'T OF THE TREASURY (July 23, 2018), https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx [https://perma.cc/S2UM-TJ3R] (archived Aug. 5, 2018).

122. *Bank Secrecy Act's Impact on Money Services Businesses: Hearing Before the Subcommittee on Financial Institutions and Consumer Credit of the Committee on Financial Services, US House of Representatives*, 109th Cong. 11–12 (2006) (statement of the Office of the Comptroller of the Currency).

which were among the last banks still providing account services to MSBs, notified about twenty money transmittal businesses with hundreds of outlets in grocery stores and travel agencies that their bank accounts would be closed by the end of March 2005.[123] On March 8, 2005, FinCEN led a fact-finding meeting to identify the reasons that MSBs were unable to access banking services.[124] At the meeting, MSB participants noted that hundreds of MSBs had lost their banking privileges and banks noted the difficulty in separating suspicious activity from legitimate businesses. [125] Bank representatives explained that they could not afford the high costs of doing in-depth due diligence in an area of business deemed "risky" and that they wanted to avoid the regulatory scrutiny that seemed to occur whenever they provided banking services to MSBs.[126]

FinCEN recognized that the inevitable result of shutting down MSB accounts would be to drive those looking for banking services to illegal operations.[127] On March 30, 2005, FinCEN, along with the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), the Office of Thrift Supervision (OTS), and the National Credit Union Administration (NCUA), issued a joint statement to address their expectations regarding banks' obligations under the BSA for MSBs.[128] The Joint Statement noted that MSBs "are losing access to banking services as a result of concerns about regulatory scrutiny, the risks presented by money services business accounts, and the costs and burdens associated with maintaining such accounts," and it said the concerns stem, in part, "from a misperception of the requirements" of the BSA. [129] In particular, there is an "erroneous view that money services businesses present a uniform and unacceptably high risk of money laundering or other illicit activity. The Money services business industry provides valuable financial services,

---

123. *See* Nina Bernstein, *Antiterror Efforts Squeeze Money Transfer Operations*, N.Y. TIMES (Mar. 16, 2005) ("[B]ecause of pressure from federal banking regulators, one bank after another has rejected its money transmittal customers unfairly lumping together licensed, reputable businesses and risky, illegal operations, mainly to eliminate the risk of an oversight and bad publicity.").

124. *See generally An Update on Money Services Businesses Under Bank Secrecy and USA PATRIOT Regulation: Hearing Before the Committee on Banking, Housing and Urban Affairs*, 109th Cong. (2005) [hereinafter *Update on MSBs*].

125. *See id.*

126. *See id.*

127. *Id.*

128. FIN. CRIMES ENFORCEMENT NETWORK, JOINT STATEMENT ON PROVIDING BANKING SERVICES TO MONEY SERVICE BUSINESSES (Mar. 30, 2005), https://www.fincen.gov/sites/default/files/guidance/bsamsbrevisedstatement.pdf [https://perma.cc/83MF-NCFC]

(archived Sept. 5, 2018).

129. *Id.*

especially to individuals who may not have ready access to the formal banking sector."[130] In addition,

> the [BSA] does not require . . . banking institutions to serve as the *de facto* regulator of the money service business industry. Banking organizations that open or maintain accounts for money-service businesses should apply the requirements of the Bank Secrecy Act on a risk-assessed basis, as they do for all customers, taking into account the products and services offered and the individual circumstances.[131]

The banking agencies subsequently released interagency guidance that set forth the minimum steps that financial institutions should take when banking MSBs.[132] The guidance covered minimum BSA due diligence expectations, BSA/anti-money laundering risk assessments, due diligence for higher-risk customers, and identification and reporting of suspicious activity.[133] On May 26, 2005, the Subcommittee on Oversight and Investigations of the Committee on Financial Services in the U.S. House of Representatives held a hearing where the banking agencies again encouraged banks to provide account services to MSBs.[134]

Although it was clear that the banking agencies wanted banks to provide financial services to MSBs, banks were still required to determine for themselves what constituted reasonable due diligence and suspicious activity, and uncertainty remained regarding whether banks' views on these issues would align with regulators'. At the May 26 hearing, the Director of the American Bankers' Association (ABA) testified that it was on the direction of regulators that banks were exiting the MSB industry: "I must take issue with my friend . . . who said it was a misperception on the part of the banking industry. It was no misperception, it was comments from field examiners who told us to eliminate these accounts because they were in fact high risk."[135] The

---

130. *Id.*

131. *Id.*

132. FIN. CRIMES ENFORCEMENT NETWORK, INTERAGENCY INTERPRETIVE GUIDANCE ON PROVIDING BANKING SERVICES TO MONEY SERVICES BUSINESSES OPERATING IN THE UNITED STATES (Apr. 26, 2005), https://www.fincen.gov/sites/default/files/guidance/guidance04262005.pdf [https://perma.cc/U88G-GUBQ] (archived Sept. 5, 2018).

133. *Id.*

134. *See generally The First Line of Defense: The Role of Financial Institutions in Detecting Financial Crimes: Hearing Before the Subcomm. on Oversight and Investigations of the H. Comm. on Fin. Servs.*, 109th Cong. (2005) (noting that the purpose of the BSA is to improve financial integrity by utilizing formal financial channels to gather information and prosecute criminals).

135. *See id.* at 34, 38 ("The check cashing and MSB industry suffers greatly from the perception that we are inordinately high-risk as compared with other financial institutions or businesses. It would appear that this conclusion has been reached by Federal bank examiners and adopted unfortunately by banks with little attention to the actual compliance record.").

Director of the ABA also noted that there was a 40 percent increase in SAR filings over the past year.[136] He attributed this phenomenon to regulatory scrutiny of SAR filings rather than increased criminal activity.[137]

Notwithstanding the interagency guidance and encouragement from the government, banks remained skeptical as to whether their anti-money laundering systems would comply with the BSA, and MSBs found it even more difficult to gain access to banking services. In the year following the May 26 hearing, three national banks stopped offering services to MSBs and the U.S. House of Representatives held another hearing on June 21, 2006 to address the issue.[138]

Representatives from the industry explained that the regulatory scrutiny that accompanies MSB accounts alters banks' cost-benefit analysis of providing services to MSBs and forces banks to either increase fees or exit lines of business.[139] Banks across the board were making the decision to invest their resources in more profitable and less-risky lines of business, causing a "state of crisis" for MSBs.[140] For instance, only two banks were serving check cashers and money remitters at the time of the hearing, meaning there would be a catastrophic impact on the industry if one or both were to exit either business.[141] And money remitters were losing access to banking services because regulators deemed remitters "high risk," even though the average remittance was only $243.[142] The National Money Transmitters' Association noted that

> [the government's] attempts to protect the banking system from the risk [money remitters] pose have backfired badly by threatening to destroy the best ally law enforcement has in the fight against money laundering. . . . Although regulators say that they do not hold banks responsible for our supervision, that is exactly what is happening. Under such conditions, it does not make sense for any bank to keep us as a customer.[143]

Over the next several years, despite the government's insistence that MSBs did not pose a high risk of money laundering and that

---

136. *Id.* at 35.

137. *Id.* (testifying that the number of SARs filed will continue to skyrocket if the regulators continue to "second guess SAR decisions made by the financial sector").

138. *See generally Bank Secrecy Act's Impact on Money Services Business: Hearing Before the Subcomm. on Fin. Inst. and Consumer Credit of the H. Comm. on Fin. Servs.*, 109th Cong. (2006).

139. *See id.* at 41.

140. *See id.* at 39.

141. *See id.* (likening the label of MSB to a scarlet letter).

142. *See id.* at 37 (listing seven national banks that terminated their relationship with MoneyGram, including Bank of America two months before the hearing), 42, and 142 (noting that hundreds of agents' accounts were terminated in the past 18 months, and most businesses being closed are minority-owned and used businesses in poor neighborhoods).

143. *See id.* at 42.

financial institutions were not required to be the *de facto* regulator of MSB clients,[144] the government significantly intensified its focus on anti-money laundering controls at banks and regulatory concerns caused even more banks to terminate MSB clients. By 2012, sanctions for anti-money laundering violations totaled $3.5 billion, up from $26 million in 2011, and the Treasury and the OCC defended their hardline stance against financial institution anti-money laundering failures at a hearing before the Senate in March 2013.[145] And, in 2013, the Department of Justice (DOJ) launched its disastrous Operation Chokepoint.

Operation Chokepoint was ostensibly created to target mass-market consumer fraud by preventing "access to the banking system by the many fraudulent merchants who had come to rely on the conscious assistance of banks and processors in facilitating their schemes."[146] In connection with Operation Chokepoint, the FDIC released a list of thirty lines of business deemed "high risk" and the DOJ issued over fifty administrative subpoenas to banks and third-party payment processors. In response to the subpoenas and the declaration that certain businesses were "high risk," banks began terminating their account relationships with the targeted businesses, especially short-term lenders, even though the businesses were operating legally and providing financial services to people without access to traditional banking services.[147] The FDIC rescinded their list of "high risk" businesses and the House Oversight and Government

---

144. *See generally Regulation of Money Services Businesses: Hearing Before the Subcomm. on Fin. Inst. and Consumer Credit of the H. Comm. on Fin. Servs.*, 111th Cong. (2010); *see also generally Patterns of Abuse: Assessing Bank Secrecy Act Compliance and Enforcement: Hearing Before the S. Comm. on Banking, Housing, and Urban Aff.*, 113th Cong. (2013) [hereinafter *Patterns of Abuse*].

145. *See Patterns of Abuse*, *supra* note 144, at 31 ("A truly robust anti-money laundering framework . . . requires effective anti-money laundering/CFT program implementation by financial institutions, buttressed by strong enforcement efforts when those efforts fall short of the mark. When anti-money laundering/CFT safeguards are not effectively implemented and compliance lags, money launderers, terrorist financiers, and other illicit actors freely abuse our financial system. . . . [A] secure global framework is essential to the integrity of the U.S. financial system . . . we engage several intergovernmental and international organizations . . . to develop, assess and facilitate implementation of effective anti-money laundering/CFT laws around the world."); OCC Statement (noting that OCC regulators make use of both formal and informal enforcement actions and that "[i]n some cases, banks ceased engaging in a particular line of business as a result of the OCC examination . . . and the OCC article required approval should the bank decide to restart that particular line of business or service").

146. *Hearing Before the Subcomm. on Reg. Reform, Commercial and Antitrust Law of the H. Comm. on Judiciary*, 113th Cong. 2 (2014) (statement of Stuart F. Delery, Assistant Att'y Gen., Civil Div.).

147. *See* Ruth Ravve, *Congress launching hearings on complaints businesses targeted by "Operation Choke Point"*, FOX NEWS POLITICS (Mar. 24, 2015), http://www.foxnews.com/politics/2015/03/24/congress-launching-hearings-on-complaints-businesses-targeted-by-operation.html [https://perma.cc/XZ5H-RQ7Q] (archived Aug. 3, 2018).

Reform Committee initiated an investigation of the Operation, but by that time the damage had been done.

> By shutting down the bank accounts of these legally operating businesses, what they're actually doing is forcing these businesses to deal solely in cash, which is completely opposite of what they have said their intention is . . . It's a whole lot easier to launder money with cash than having to go through a financial institution.[148]

The House Committee's investigation found that Operation Chokepoint forced banks to terminate relationships with a wide variety of lawful merchants simply because the government deemed the business lines "high risk," not because actual fraud or money laundering was discovered.[149] In November 2014, FinCEN released yet another statement encouraging banks to provide account services to MSBs by employing a risk-based approach.[150] The statement noted that "MSBs play an important role in a transparent financial system, particularly because they often provide financial services to people less likely to use traditional banking services and because of their prominent role in providing remittance services."[151]

Due to enhanced scrutiny from regulators and the potential for large fines if banks make a compliance-related mistake, banks have decided not to work with businesses they deem to be high risk, including MSBs. FinCEN continues to encourage banks to provide account services to MSBs and expects banks to take a risk-based approach in assessing customer relationships rather than exiting entire lines of business—an approach known as "de-risking"—but the risk of banking businesses that may be high risk is simply not worth the compliance cost to banks. Ironically, the "result of de-risking is re-risking," since bad actors will leave cautious banks and turn to institutions unequipped to handle them.[152] As the managing director for financial crimes enforcement at JP Morgan Chase explained, "[w]e are kind of in a Ping-Pong match between financial inclusion and avoiding regulatory scrutiny and we are the ball."[153]

---

148. *Id.*

149. *Id.*

150. *FinCEN Statement on Providing Banking Services to Money Service Businesses*, FIN. CRIMES ENFORCEMENT NETWORK (Nov. 10, 2014), https://www.fincen.gov/news/news-releases/statement [https://perma.cc/PWM8-87ZB] (archived Aug. 3, 2018).

151. *Id.*

152. Ian McKendry, *Banks Face No Win Scenario on AML 'De-Risking'*, AMERICAN BANKER (Nov. 17, 2014), https://www.americanbanker.com/news/banks-face-no-win-scenario-on-aml-de-risking [https://perma.cc/A2ET-XMYE] (archived Aug. 3, 2018).

153. *Id.*

C. *Conservative Approach to Mobile Money Anti-Money Laundering Regulations Already Being Felt around the World*

In contrast to the rapid growth of mobile money services in developing parts of the world, mobile money has not enhanced financial inclusion in the United States. This is likely due, at least in part, to the fact that banks are prohibited from settling financial transactions for customers without performing customer due diligence and applying know-your-customer (KYC) procedures. Regulatory agencies have taken the position that the BSA's anti-money laundering regulations apply to banks engaged in mobile money transactions, and the former FinCEN director specifically stated that the revised FATF Recommendations will apply to financial institutions that use "new technologies" to provide financial services.[154] In the United States, mobile banking generally consists of bank account holders using a smartphone to make a transaction or check their account; mobile banking is not used to provide financial access to the unbanked or underbanked.[155] An estimated 7 percent of US households lack access to a bank account and an additional 19.9 percent have a bank account but still use an alternative financial service at least once per year, and are thus classified as "underbanked."[156] These populations continue to make use of alternative financial services, such as check cashers, payday lenders, and money orders (all MSBs), and have to incur the high fees associated with the use of these services.[157] While most of the unbanked population has access to a mobile phone in the United States, mobile banking services are not aimed at providing services to the underserved.[158]

Although many developing countries that employ a robust mobile money network are still in the process of establishing anti-money laundering laws that comply with the FATF standards, consequences

---

154. *See* Mulcahey, *supra* note 111, at 107.

155. *See* Erin F. Fonté, *Mobile Payments in the United States: How Disintermediation May Affect Delivery of Payment Functions, Financial Inclusion and Antimoney Laundering Issues*, 8 WASH. J.L. TECH. & ARTS 419, 445 (2013) ("Mobile payments in the United States are currently about affluence and advertising, not access . . . Other countries, including developed and developing nations, have outpaced the United States in mobile payments adoption.").

156. *See 2015 FDIC National Survey of Unbanked and Underbanked Households*, FED. DEPOSIT INS. CORP. (June 29, 2017), https://www.fdic.gov/householdsurvey/ [https://perma.cc/AK8Z-UGET] (archived Aug. 3, 2018).

157. In his TED talk, economist Dilip Ratha explains that money transfer services "structure their fees to milk the poor," though the CEO of Western Union posits that anti-money laundering compliance costs coupled with the difficult barriers to entry into the market lead to the high fees for remittances. *See* Ben Schiller, *The Fight For The $400 Billion Business Of Immigrants Sending Money Home*, FAST COMPANY (Apr. 28, 2017), https://www.fastcompany.com/3067778/the-blockchain-is-going-to-save-immigrants-millions-in-remittance-fees [https://perma.cc/B48G-P9DL] (archived Aug. 3, 2018).

158. *See* Fonté, *supra* note 155, at 449.

of the anti-money laundering regime and the policies behind the standards can already be seen. For instance, an analysis undertaken by the FATF to assess the impact of countries' AML/CFT regimes on financial inclusion found that customer due diligence requirements were too stringent in certain countries.[159] In Zambia, Tanzania, and Bangladesh, for example, the strict requirements "were impeding access of certain low risk categories of customers to finance."[160] The FATF also found that lower capacity countries in particular have been having difficulty striking a balance between financial inclusion and customer due diligence requirements.[161] It reported that "[i]n one country, although the financial sector was very interested in offering financial inclusion products with simplified CDD, their requests for reconsideration of the stringent CDD framework of the country were dismissed by the authorities."[162]

In Kenya, for example, the Central Bank of Kenya has said that BitPesa, a remittance service, does not comply with the bank's money transmission and remittance regulations.[163] As a result, the company's telecom service, Safaricom, terminated its relationship with BitPesa, even though the company claims that its policies do comply with the country's anti-money laundering regulations.[164] In addition, in a March 2017 Report,[165] the U.S. State Department alleged that Kenya's M-PESA system (among other international systems), which has thirty million subscribers and has been credited with bringing 2 percent of Kenyan households out of extreme poverty, remains

---

159. *See* 2017 FATF GUIDANCE, *supra* note 74, at 26.

160. *Id.*

161. *Id.* at 29.

162. *Id.*

163. *See* Lester Coleman, *Telecom/BitPesa Legal Tangle Over AML Threatens Mobile Payments in Kenya*, CCN (Dec. 1, 2015), https://www.ccn.com/telecombitpesa-legal-tangle-aml-threatens-mobile-payments-kenya/ [https://perma.cc/XC8V-ZG6N] (archived Aug. 3, 2018).

164. *See* Ian Allison, *Bitcoin versus M-Pesa: Digital payments rumble in the jungle*, INT'L BUS. TIMES (Dec. 2, 2015), https://www.ibtimes.co.uk/bitcoin-versus-m-pesa-digital-payments-rumble-jungle-1531208 [https://perma.cc/3ZH7-BGPF] (archived Aug. 3, 2018) ("BitPesa has implemented anti-money laundering/KYC policies that comply with Kenyan legal and regulatory requirements. We have freely submitted them to the Central Bank of Kenya, as well as regulators in other jurisdictions in which we operate. We hold ourselves to the highest standards when it comes to anti-money laundering/KYC compliance."). The chief legal and compliance officer of BitPesa says the company "continues to work with Kenya's central bank" and asserts that, in order for regulations to stop stifling technological innovation in the country, "regulators could work with innovators to see how the technology applies in order to create legislation or engagement rules." Lester Coleman, *BitPesa: Regulators' Disconnect with Blockchain Firms Hurting Innovation in Kenya*, CCN (Dec. 24, 2016), https://www.ccn.com/bitpesa-regulators-disconnect-blockchain-firms-hurting-innovation-kenya/ [https://perma.cc/AVC2-M5PY] (archived Aug. 3, 2018).

165. BUREAU FOR INT'L NARCOTICS & LAW ENFORCEMENT AFFAIRS, U.S. DEP'T OF STATE, INTERNATIONAL NARCOTICS CONTROL STRATEGY REPORT, VOL. II 116 (2017).

vulnerable to money laundering.[166] It remains to be seen what impact, if any, this allegation will have on financial institutions' involvement in M-PESA transactions.

V. ENTER THE GATEKEEPERS: A PROPOSAL TO PREVENT ANTI-MONEY LAUNDERING POLICIES FROM HINDERING THE SUCCESSFUL GROWTH OF MOBILE MONEY PROGRAMS

A. *What Went Wrong?*

As discussed above, in response to anti-money laundering policies and enforcement actions against financial institutions, US banks have terminated their relationships with MSBs. If international governments establish and strictly enforce anti-money laundering laws based on the FATF Recommendations, financial institutions may ultimately refuse to participate in mobile money transactions as well. In order to prevent this from occurring, the international community can look to gatekeeper theory and create a regime that incentivizes financial institutions to remain in the industry. In particular, an optimal liability regime should replace the current liability regime, governments should employ incentives to encourage financial institutions to settle mobile money transactions, and financial institutions should be enabled and encouraged to build reputational capital in the field.

1. Gatekeeper Theory

The gatekeeper theory of liability imposes liability on professionals for wrongs committed by their clients. Under traditional gatekeeper theory, a gatekeeper is an intermediary party with the capacity to monitor and influence the conduct of its client.[167] Gatekeepers are generally retained as agents to perform a service for a principal and through their role they are granted access to information that puts them in a unique position to evaluate whether

---

166. *See* Amy Westervelt, *In The Rush Toward A Cashless Society, The Poorest Are At Risk Of Further Exclusion*, HUFFINGTON POST (Feb. 16, 2018), https://www.huffingtonpost.com/entry/cashless-society-poor-exclusion_us_5a857082e4b0ab6daf463c4a [https://perma.cc/8W88-7ZKN] (archived Aug. 3, 2018).

167. *See generally* Reinier H. Kraakman, *Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy*, 2 J.L. ECON. & ORG. 53 (1986); *see also* JOHN C. COFFEE, JR., GATEKEEPERS: THE PROFESSIONS AND CORPORATE GOVERNANCE 2 (2006) ("First, the gatekeeper may be a professional who is positioned so as to be able to prevent wrongdoing by withholding necessary cooperation or consent. For example, an investment banking firm can refuse to underwrite the issuer's securities if it finds that the issuer's disclosures are materially deficient. . . . [A] second and superior definition of the gatekeeper is an agent who acts as a reputational intermediary to assure investors as to the quality of the 'signal' sent by the corporate issuer.").

the principal has violated or may violate the law.[168] Gatekeepers acquire reputational capital over many years that they pledge to ensure the accuracy of their representations, and a gatekeeper would not rationally risk losing its reputational capital for a single client or fee.

In the capital markets, where gatekeeper theory has been applied and incorporated into the law for many years, gatekeepers include accountants who certify that a corporation's financial statements comply with generally accepted accounting principles; lawyers who ensure that a corporation submits accurate and required financial disclosures; securities analysts who evaluate and make recommendations regarding the value of securities; underwriters who review and investigate a company before a securities offering; and credit rating agencies who rate a corporation's securities.[169] Gatekeeper theory has been applied more broadly as well to refer to any informational intermediary who provides verification or certification services.[170] For instance, Underwriters Laboratories, Inc. (UL) is a nonprofit organization that tests various appliances and generates labels for approved products, certifying to the public that the product is safe.[171] The Occupational Safety and Health Administration (OSHA) has authorized UL as an independent testing and certifying organization for certain OSHA procedures, and the UL mark now appears on twenty billion products each year.[172] Similarly, private certification standards exist for food (OECD), education, and healthcare facilities, among others. While gatekeepers take many forms, a successful gatekeeper model tends to require the same basic elements.

First, there must be a metaphorical gate to keep.[173] Without the gatekeeper's permission, which can be manifested in a variety of ways, an entity is unable to access the market. Sometimes, the gatekeeper's role will be required by law before the client can access a market or complete a transaction: an attorney or an auditor can refuse to deliver an opinion that is necessary for a transaction to close based on discrepancies in the corporation's financial statements or disclosures. Other times, an enterprise will simply be unable to enter a market

---

168. *See* Kraakman, *supra* note 167, at 54.

169. *See* COFFEE, *supra* note 167.

170. *See generally* Frank Partnoy, *Second-Order Benefits from Standards*, 48 B.C. L. REV. 169 (2007) (discussing private actors who sell regulatory licenses that enable market participants to reduce their costs).

171. *See id.* at 184.

172. *See* UNDERWRITERS LABS., THE UL SAFETY MARK: ON TIME MARKET ACCESS TO NORTH AMERICA AND BEYOND (2012), https://uk.ul.com/wpcontent/uploads/sites/21/2014/05/298.UL_Safety_Mark_EN_P.pdf [https://perma.cc/SDT4-DXKA] (archived Aug. 3, 2018).

173. *See* Lawrence A. Cunningham, *Beyond Liability; Rewarding Effective Gatekeepers*, 92 MINN. L. REV. 323, 334 (2007); *see also* COFFEE, *supra* note 167.

without gatekeeper verification: an investment bank can prevent an enterprise from entering the capital markets by refusing to underwrite the issuer's securities. Under either scenario, the gatekeeper is an intermediary with the power to prohibit an entity from accessing a market.

Second, the gatekeeper must be able to monitor its client and assert influence over its client's actions, thereby deterring wrongdoing. A critical component of the gatekeeper's ability to exercise control over its client is through its role in resolving an informational asymmetry that would otherwise exist. [174] Take, for instance, credit rating agencies. By providing the public with information about the creditworthiness of a financial instrument at a low cost, credit rating agencies enable investors to participate in the market and allow corporations to raise capital. [175] This role becomes even more important as securities become increasingly complex, since fewer investors are able to adequately assess the information that they do have. And, by providing assurance to investors that a corporation's disclosures are accurate, gatekeepers compel corporations to make accurate disclosures. Without gatekeepers' diligence and certification, corporations would be incentivized to economize on the information asymmetry and profit at the expense of investors, making investors hesitant to invest out of fear that they would be sold "lemons."[176] Gatekeepers, by acting as informational intermediaries, lower corporations' ability to economize on information asymmetries, thereby forcing them to act in a lawful manner.

Third, the gatekeeper must have acquired reputational capital over many years that it pledges to ensure the accuracy of a corporation's representations and which it would not rationally sacrifice for a single client or fee. According to Professor John Coffee, a seminal figure in the academic literature on gatekeeper theory, this pledge of reputational capital is the key feature that distinguishes gatekeepers from other types of certifiers. [177] In order for a gatekeeper's verification to be credible, the gatekeeper must have spent many years performing similar services for numerous clients. The more often a firm is retained to serve as a gatekeeper, the more expertise it builds in its field and the more valuable its pledge of accuracy becomes.[178] In most markets, the mere name of a specific

---

174. *See* Andrew F. Tuch, *Multiple Gatekeepers*, 96 VA. L. REV. 1583, 1594 (2010).

175. *See, e.g., Wall Street and the Financial Crisis: The Role of Credit Rating Agencies: Hearing Before the Permanent Subcomm. on Investigations*, 111th Cong. (2010) (statement of Richard Michalek, Former Vice President Sr. Credit Officer, Structured Derivative Products Group, Moody's Investors Service), https://www.hsgac.senate.gov/imo/media/doc/STMTMICHALEKRichardFormerMoodys.pdf [https://perma.cc/TT7N-WDK7] (archived Aug. 3, 2018).

176. *See* Tuch, *supra* note 174, at 1595.

177. *See* COFFEE, *supra* note 167.

178. *See* Cunningham, *supra* note 173, at 334.

gatekeeping firm providing its stamp of approval suffices to signal to the market that a corporation's disclosures are accurate.

Fourth, there must be an optimal liability regime in place that incentivizes the gatekeeper to perform its gatekeeping function and to do so properly. Optimal deterrence theory posits that liability rules will influence the conduct of actors, who make rational behavioral decisions based on the known legal consequences of their actions.[179] In the gatekeeping context, an optimal liability regime is twofold. First, in order to incentivize a gatekeeper to take on a gatekeeping role in the first place, the aggregate costs of wrongdoing must exceed the aggregate costs of precautions.[180] Second, on a normative level, because a gatekeeper receives a smaller payout for certifying information than the principal makes from the transaction, a lesser expected penalty should suffice to deter the gatekeeper from making a false certification.[181] This is especially true given the loss in reputational capital that a gatekeeper would suffer as a result of verifying a false representation.

Last, there must be adequate competition in the gatekeeping industry; the costs of entry cannot be prohibitive. If gatekeeping responsibilities for an entire industry are concentrated in the hands of a few firms, the reputational effect of failure begins to wane. In addition, without active competition, firms are able to maintain their business without investing in innovative technology or research, leading to organizational slack.[182] Lock-in problems may also arise once a firm has been chosen—a client may be reluctant to switch gatekeeping firms because it becomes costly and outsiders will wonder whether the switch indicates a problem with the client. That being said, where a gatekeeper operates a near monopoly, the firm may be more equipped to resist pressure from the client.[183]

2. Financial Institutions Treated as Gatekeepers

By viewing US anti-money laundering laws and enforcement policies through the lens of gatekeeper theory, it becomes apparent why financial institutions have, for the most part, retreated from offering their services to money-service businesses: financial institutions were given gatekeeping responsibilities without the necessary incentives for a functional model. If international anti–money laundering laws are applied to financial institutions that settle

---

179. *See* Tuch, *supra* note 174, at 1606 (citing STEVEN SHAVELL, ECONOMIC ANALYSIS OF ACCIDENT LAW (Harv. Univ. Press 2007)).

180. *See id.*

181. *See id.*

182. *See* COFFEE, *supra* 167, at 318.

183. *See id.*

mobile money transactions in a similar fashion, we can expect mobile money customers to lose access to stable banking institutions as well.

In the MSB context, financial institutions are treated as gatekeepers in a variety of ways. Financial institutions are third parties that can and have prevented MSB participants from entering the market. MSBs, such as money transmitters and check cashers, require banking services in order to operate, and when banks refuse to take on MSBs as clients, MSBs are unable to carry out transactions for their customers.[184]

Furthermore, financial institutions are required by law to monitor their clients—and, in the case of MSBs, their clients' clients—and ensure they are complying with applicable laws and regulations. However, as described in Part V.B, financial institutions lacked the information necessary to monitor the MSBs' clients, and they had to rely on MSBs to institute their own anti-money laundering controls, including customer due diligence and KYC.[185] Although it was extremely difficult for banks to identify suspicious activity taking place at the MSB-customer level, the government continued to hold banks accountable for monitoring and reporting on those customers. "[O]ne banker has analogized this process as running a railroad and being expected to monitor everyone who takes your trip to see if their trip is legitimate."[186]

And, in several instances, an investigation of an MSB led the government to criminally investigate or prosecute the MSB's bank due to the bank's failure to "properly administer the MSB account."[187] Banks ultimately determined that the costs of compliance outweighed the fees generated by banking MSBs. For instance, in 2012, HSBC was fined a record $1.2 billion after the Senate Permanent Subcommittee on Investigations found that the bank had failed to put in place adequate anti-money laundering controls.[188] Even though this fine was focused on HSBC's own anti-money laundering controls, the bank shortly thereafter withdrew their services from MSBs. This decision was likely due, at least in part, to the fact that it would be difficult for the bank to ensure that its MSB clients were deploying their own

---

184. MSBs are licensed by the state, and states generally require MSBs to have a banking relationship in order to comply with the regulations. *See generally Update on MSBs*, *supra* note 124.

185. MSBs engage in a high volume of cash transactions with third party customers who are unknown to the MSB's bank, meaning the bank could not verify the customers' identities or obtain first-hand knowledge regarding the transaction. *See infra* Part V.B.

186. *Update on MSBs*, *supra* note 124, at 47.

187. *Id.*

188. *See* Rebecca Brace, *Money-service businesses seek new banking suitors as regulations bite*, EUROMONEY (June 19, 2013), http://www.euromoney.com/Article/3220753/Money-service-businesses-seek-new-banking-suitors-as-regulations-bite.html [https://perma.cc/27SN-SWX3] (archived Aug. 3, 2018).

adequate anti-money laundering controls. Regulators, rather than address the issue of MSB controls directly, focused their attention on the banks providing services to the MSBs, which have much greater technological and financial resources.[189]

Despite all of these gatekeeper-like responsibilities, financial institutions lacked the incentives necessary for a gatekeeper model to properly function. Financial institutions made very little money banking MSBs, they gained no advantage from their reputational capital in the industry since there was no competition and very little transparency, and there was not an optimal liability regime in place, as shown by the severe penalties placed on the financial institutions for wrongs committed by other parties.[190]

It appears possible, and even probable, that international anti-money laundering laws, which are based on and nearly identical to US anti-money laundering laws, will have a similar deterrent effect on financial institutions that operate or are involved in mobile money programs. As in the MSB context, financial institutions that settle mobile money transactions are treated as gatekeepers without the necessary incentives that exist in a successful gatekeeper model.[191] For the gatekeeper model to work, there needs to be an optimal liability regime in place and gatekeepers must be properly incentivized to perform their responsibilities. Neither characteristic exists in the mobile money context. Yet we *want* financial institutions to take on some of the monitoring and influencing duties that the law already assigns to them: financial institutions have greater resources at their disposal for preventing money laundering and terrorism, they are far more stable sources of banking than smaller, local outlets, and they have the capacity to provide their customers with access to global financial services. For all of these reasons, the international community should review the current anti-money laundering recommendations and consider amending the laws to align with the gatekeeper theory model.

---

189. *See id.* (quoting a commentator as stating that "[i]f you want to fine someone, fine someone who has got money"); *see also Update on MSBs*, *supra* note 124, at 35 ("The more heat that is brought on the banking industry, the less it can afford to appear to be associated with those who look even slightly suspicious to some eyes.").

190. *See infra* Part V.B.

191. *See infra* Appendix A.

B. *Solutions Based on Gatekeeper Theory*

There are a variety of steps based on gatekeeper theory that the international community can and should take to prevent financial institutions from avoiding or eventually exiting the mobile money business. To be clear, this Article is not arguing that financial institutions are gatekeepers in mobile money transactions in the same way that gatekeepers exist in the financial markets. Gatekeepers in capital markets resolve information asymmetries and increase market transparencies, resulting in a lower cost of capital. In mobile money transactions, financial institutions are a necessary participant in a financial transaction. However, as discussed above, international anti-money laundering laws assign financial institutions gatekeeper-like responsibilities and gatekeeper theory can therefore be applied to create a functioning regime.

1. Implement an Optimal Liability Regime

First, international legislatures should determine the optimal level of liability and ensure that regulators enforce anti-money laundering laws in a consistent, fair, and predictable manner. The history of MSBs in the United States indicates that the current anti-money laundering regime, if enforced similarly in the mobile money context, places too much regulatory liability on financial institutions involved in mobile money transactions. Optimal liability in mobile money programs must be achieved on multiple levels. First, there is an institution's anti-money laundering program itself. Not only is it important that financial institutions do their best to prevent money laundering and terrorist financing, but also there is a strong advantage to having bad actors attempt to use formal financial channels: the money is far more easily traceable than cash. Governments should align with financial institutions in the fight against money laundering and terrorist financing, rather than attack the institutions for political purposes in an attempt to gain a big payday and significant publicity.

Regulators should work closely with financial institutions to design and implement their anti-money laundering programs. If regulators detect anti-money laundering deficiencies, rather than fine the institution large sums of money, regulators should help the institutions improve their programs. As part of the anti-money laundering program, it makes sense to apply a risk-based approach, but regulators and institutions must be able to differentiate between high-risk transactions and low-risk transactions. If all mobile money transactions are ultimately deemed "high risk," since it is difficult for an institution to truly know the participants in the transaction, or if financial institutions are required to determine for themselves what constitutes "high risk," financial institutions will exit the industry,

leaving companies with less stability and resources to complete the transactions.[192]

Moreover, at a transactional level, when money laundering is detected by an institution, we want the institution to quickly and without concern for its own liability notify the government and coordinate with the government to identify the wrongdoer. FATF Recommendation 20 requires countries to implement a reporting system in line with the US reporting system along with sanctions for failure by a financial institution to file a suspicious activity report.[193] However, there are a variety of differences between developed and developing countries that may prevent this system from being effective in the developing world. For instance, the FATF (rightly) set forth instances where it may be appropriate to apply simplified customer due diligence procedures, such as where there is difficulty obtaining proof of identity and address and with respect to certain low-risk products.[194] But where simplified customer due diligence measures are used, institutions may lack the information necessary to file a suspicious activity report, potentially resulting in harsh penalties for failure to file the report.

Furthermore, compliance with reporting requirements is expensive and requires substantial expertise along with resources. Institutions in developing countries may lack the resources necessary to establish and employ sophisticated reporting systems, and if they decide to settle mobile money transactions, they will likely pass compliance costs onto consumers through increased service fees, reducing mobile money accessibility.[195]

Moreover, because the FATF standards do not apply a risk-based approach to the reporting of suspicious activity, institutions must report suspicious transactions that are low value and high volume, like many mobile money transactions.[196] This system will likely result in

---

192. *See supra* Part V.B. The World Bank has created a tool that allows a country or a financial institution to put information regarding specific money laundering and terrorist financing parameters into an excel template and the module produces a risk assessment of the product. *See* 2017 FATF GUIDANCE, *supra* note 74, at 7. If the assessment indicates a low risk of money laundering or terrorist financing, the country or financial institution can be more confident in applying simplified AML/CFT measures to that product. While this tool is certainly a step in the right direction towards identifying situations under which simplified CDD measures should be applied, institutions cannot be confident that their use of the tool will protect them from liability, especially if the country has not amended its regulations to allow simplified CDD measures relating to that product.

193. FATF RECOMMENDATIONS, *supra* note 19, at 20.

194. *See* FATF ANTI-MONEY, *supra* note 71 (providing illustrations of methods for verifying a person's address and identity where that person lacks a formal registered address or formal identification).

195. *See* Miriam Goldby, *Reporting of Suspicious Activity by Mobile Money Service Providers in Accordance with International Standards: How Does it Impact on Financial Inclusion?*, 8 WASH. J.L. TECH. & ARTS 401, 411 (2013).

196. *See id.*

institutions filing numerous reports as a defensive policy, to protect themselves from harsh sanctions, to government units ill-equipped to handle or be able to effectively review and investigate genuine cases of money laundering or terrorist financing.[197]

The optimal level of liability for a financial institution involved in a mobile money transaction must be low enough to encourage the institution to remain in the industry but high enough to encourage the institution to take proper precautions in ferreting out bad behavior. Regulators should encourage financial institutions to only report truly suspicious behavior and refrain from punishing financial institutions for failing to report behavior that, when reviewed in hindsight, was not actually suspicious or indicative of a financial crime. This can be achieved by conducting annual workshops where regulators and financial institutions review a variety of SARs filed over the previous year and discuss whether or not a SAR was necessary in that instance. These workshops should include multiple institutions to ensure that regulators enforce the law consistently across institutions.

Additionally, if a financial institution fails to identify and report suspicious activity in line with a country's anti-money laundering laws, the government should hold the institution accountable, but on a much smaller scale than what has happened in the United States.[198] Like the federal sentencing guidelines in the United States, legislatures could determine a sliding scale for anti-money laundering-related penalties *ex ante*. Doing so would have the dual effect of (1) reducing concern within institutions that they will be subject to excessive fines for nonprofitable services while (2) restricting regulators from seeking excessive fines. If regulators are aware that they will only be able to penalize financial institutions a limited amount of money for failing to file a SAR in relation to a mobile money payment, they will be more likely to coordinate with the institution in the first place rather than initiate an expensive and time-consuming investigation. Similarly, if a financial institution does identify suspicious activity that took place, the government should grant that institution absolute immunity from liability related to that transaction *and* the anti-money laundering control failure that led to that transaction being missed and should instead work with the institution to prevent that from happening in the future.[199]

---

197. Defensive SARs are not limited to developing countries. In the past, the FATF has criticized countries for low volumes of SARs, resulting in over-reporting to appease the FATF. *See id.* at 415.

198. For a chart depicting BSA AML fines for MSBs between 2012 and 2015, see KRISTIN PULLAR, ADVANCING FINANCIAL CRIME PROFESSIONALS WORLDWIDE, BLANKET DE-RISKING OF MONEY SERVICE BUSINESSES 4 (2016).

199. *See* Goldby, *supra* note 195, at 416 (noting that in certain circumstances, it may be most effective to do away with the traditional SAR system and instead grant government agencies access to an institution's records on a person under investigation).

2. Offer Financial Institutions Incentives

· Second, in order to encourage financial institutions to become or remain involved in mobile money programs, governments should increase the incentives for providing services. Mobile money transactions generate low fees for financial institutions but represent high risks for sanctions and other penalties. Governments could offer corporate subsidies or tax incentives to institutions that settle mobile money transactions, especially for consumers that lack access to formal financial services. Corporations enjoy the benefits of subsidies in numerous industries that are considered beneficial for the public, such as low-income housing development, clean energy resources, and agriculture. By providing large swaths of populations with access to affordable and stable financial services, mobile money services are crucial to increasing financial inclusion in developing countries and certainly fit into the types of social goals covered by government subsidies.

In fact, governments could go even further and reward institutions that identify criminals attempting to utilize the services for financial crimes. For instance, in line with the reputational capital model, governments should publicize when a financial institution identifies or prevents money laundering or terrorist financing. Doing so would both convey to the community that the financial institution is playing a role in preventing money laundering and increasing financial integrity, and signal to money launderers and terrorist financiers that they will have difficulty laundering money through the institution.

3. Build Reputational Capital

Last, we should enable financial institutions to build reputational capital in the mobile money industry. Reputational capital is imperative in a gatekeeper model because it cannot be achieved without expertise and resources, and it signals to consumers—who, in developing countries, are particularly skeptical of digital banking services to begin with—that their money will be safe and their financial transactions properly processed. Building reputational capital requires financial institutions to become involved in and remain in the mobile money industry, which, as discussed above, will not take place without an optimal liability regime or financial incentives for financial institutions. In addition, a properly functioning reputational capital market requires both competition and transparency. Governments should incentivize multiple financial institutions in their country to provide mobile money services and should refrain from promoting or aligning with only one institution. For instance, Kenya's communications regulator faced significant criticism after shelving a recommendation to split up Safaricom's market dominance by obliging the company to implement interoperability between M-PESA and

other mobile money services.[200] As a result, Safaricom and Airtel Kenya are now piloting an interoperability program.[201]

Without a competitive market, financial institutions would not have to preserve and protect their reputation for providing safe and reliable services and they could afford to be less accountable toward their clients, potentially leading to a "race to the bottom." In coordination with increasing competition, governments should enhance transparency in the mobile money field so participants can differentiate between good and bad service providers. For instance, governments can create a database or rating system that signals to the marketplace whether a financial institution accurately and expeditiously settles mobile money transactions, and, as discussed above, regulators should broadcast instances of financial institutions identifying or preventing suspicious activity. This is in sharp contrast to the current system in the United States, which requires absolute confidentiality when a covered institution files a SAR.[202]

VI. CONCLUSION

As set forth in this Article, the anti-money laundering policies being promoted throughout the developing world are likely to cause financial institutions to terminate their relationships with mobile money providers, resulting in less-secure financial transactions for unbanked and underbanked populations. This conclusion is based on the history of MSBs in the United States, which lost their access to banking services due to severe penalties, overzealous regulators, and stringent anti-money laundering regulations that were applied in unpredictable ways. This Article has proposed that the international community and international legislatures look to the gatekeeper theory of liability to create anti-money laundering systems that will encourage financial institutions to become and remain involved in mobile money transactions. Once an optimal liability regime has been created and there are proper incentives and competition in place, financial institutions will be able to safely and securely facilitate

---

200. *See* James Barton, *Kenya regulator under fire for timid approach to Safaricom's dominance,* DEVELOPING TELECOMS (Jan. 4, 2018), https://www.developingtelecoms.com/business/regulation/7524-kenya-regulator-under-fire-for-timid-approach-to-safaricom-s-dominance.html [https://perma.cc/T9XY-9RZD] (archived Aug. 3, 2018). Although there are three mobile operators in Kenya, Safaricom claims 72 percent of wireless connections and 81 percent of mobile money users. *Id.*

201. *See Safaricom, Airtel to pilot mobile money interoperability on Monday,* CIO EAST AFRICA (Jan. 19, 2018), https://www.cio.co.ke/safaricom-airtel-test-mobile-money-interoperability-monday/ [https://perma.cc/4GM7-GFAM] (archived Oct. 1, 2018).

202. *See FinCEN Rule Strengthens SAR Confidentiality,* FIN. CRIMES ENFORCEMENT NETWORK (Nov. 23, 2010), https://www.fincen.gov/news/news-releases/fincen-rule-strengthens-sar-confidentiality [https://perma.cc/SPX6-XU2Z] (archived Aug. 3, 2018).

mobile money transactions throughout the developing world, thereby allowing people who have always lacked access to banking services the opportunity to participate in the financial system for the first time.

Appendix A

	US Anti-Money Laundering Laws	FATF Recommendations
AML Program	Financial Institutions (FIs) must establish AML programs including internal policies, procedures, and controls; designate a head compliance officer; perform ongoing employee training programs; and develop an independent testing mechanism. PATRIOT Act § 352.	Countries must implement laws requiring FIs to create and implement an AML program that takes into account the money laundering and terrorist financing risks for the country. Recommendation 1.
Risk Determination	FIs must create a formal risk profile to identify products, services, and customers that create higher risk. PATRIOT Act § 352.	FIs must determine the extent of their CDD measures using a risk-based approach (RBA). Recommendation 10.
Recordkeeping	FIs must maintain all documents used to establish identify for five years after a relationship ends; FIs must maintain currency transaction report (CTR) and SAR documents for five years after filing a report. BSA, 31 C.F.R. 1010.410(a)(4); 1010.430; 1010.306(a)(2).	FIs must maintain, for at least five years, all necessary records on transactions to enable them to comply swiftly with information requests from authorities. FIs must keep all records obtained through CDD measures for at least five years after the business relationship is terminated. Recommendation 11.
Reportable Transactions	FIs must report CTRs over $10,000 in one business day. BSA. 31 C.F.R. 1010.311.	Countries should consider the feasibility and utility of a system where FIs report large cash transactions "above a fixed amount." Interpretive Note to Recommendation 29.
KYC: Customer Identification Program	FIs must gather and verify their customer's identification before opening an account. PATRIOT Act § 326.	FIs must gather and verify their customer's identification before opening an account, including identifying the beneficial owner. Recommendation 10.

KYC: Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD)	FIs must determine the expected and normal activities for a customer and must monitor the customer's activity to determine whether it diverges from the expected customer profile. PATRIOT Act § 352.	FIs must determine the expected and normal activities for a customer and must monitor the customer's activity to determine whether it diverges from the expected customer profile. FIs must also undertake CDD measures when carrying out certain transactions over USD/EUR 15,000 or where there is suspicion of money laundering or terrorist financing, or when the FI has doubts about the veracity of previously obtained customer identification data. Recommendation 10.
Suspicious Activity Reporting	FIs must identify suspicious activities and report them through the use of SARs. FIs must file SARs for, among others, insider abuse; violations aggregating to $5,000 or more where a suspect can be identified; violations aggregating to $25,000 or more regardless of a potential suspect; and transactions aggregating to $5,000 or more that involve potential money laundering or violations of the BSA. BSA. 12 C.F.R. 21.11(c).	If an FI suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, it must report its suspicions to a financial intelligence unit. Recommendation 20.

***