SYMPOSIUM
MOBILE MONEY IN DEVELOPING COUNTRIES: FINANCIAL INCLUSION AND FINANCIAL INTEGRITY

Introduction to Mobile Money in Developing Countries: Financial Inclusion and Financial Integrity Conference
Special Issue..................................................Jane K. Winn & Louis de Koker 155
The 2012 Revised FATF Recommendations: Assessing and Mitigating Mobile Money Integrity Risks Within the New Standards Framework.................................Louis de Koker 165
Governance of Global Mobile Money Networks: The Role of Technical Standards.................................Jane K. Winn 197
Privacy and Security Concerns Associated with Mobile Money Applications in Africa........Andrew Harris, Seymour Goodman & Patrick Traynor 245
The Role of UNCITRAL Texts in Promoting a Harmonized Legal Framework for Cross-Border Mobile Payments........Luca G. Castellani 265
Mobile Money as an Engine of Financial Inclusion and Lynchpin of Financial Integrity........................Claire Alexandre & Lynn Chang Eisenhart 285
The Role of Anti-Money Laundering Law in Mobile Money Systems in Developing Countries..................................Emery S. Kobor 303
Mobile Money, Financial Inclusion and Financial Integrity: The South African Case..................................Vivienne A. Lawack 317
M-Payments in Brazil: Notes on How a Country’s Background May Determine Timing and Design of a Regulatory Model........................................Gilberto Martins de Almeida 347
Safaricom and M-PESA in Kenya: Financial Inclusion and Financial Integrity.................................Mercy W. Buku & Michael W. Meredith 375
Reporting of Suspicious Activity by Mobile Money Service Providers in Accordance with International Standards: How Does it Impact on Financial Inclusion?.........................Miriam Goldby 401
Mobile Payments In The United States: How Disintermediation May Affect Delivery of Payment Functions, Financial Inclusion and Anti-Money Laundering Issues..........................Erin F. Fonté 419
This special issue of the *Washington Journal of Law, Technology & Arts* contains papers contributed to a conference held at the University of Washington School of Law on April 20, 2012. The conference, entitled *Mobile Money in Developing Countries: Financial Inclusion and Financial Integrity*, was organized by the University of Washington School of Law with the support of the Linden Rhoads Dean’s Innovation Fund, Deakin University School of Law, Australia, and the United Nations Commission on International Trade Law (UNCITRAL).

The conference provided an early opportunity to analyse the impact of the newly-released revised 2012 Financial Action Task Force (FATF) Recommendations on mobile money. ¹ These Recommendations were published in February 2012, and represent the most recent version of global standards for national anti-money laundering (AML), counter-terrorist financing (CTF), and proliferation financing efforts. The conference focused on the trade-off between financial inclusion as a development strategy

---

and financial integrity as a goal of prudential regulation and law enforcement, with specific reference to mobile money initiatives in developing countries and the new 2012 FATF standards.

Financial inclusion is an important social and economic policy objective for many developing countries. “Mobile money” refers to the use of a mobile phone handset to deposit, withdraw or transfer funds; and it holds great promise as a policy instrument for promoting financial inclusion. It provides a practical and cost-effective channel to extend basic banking services to many currently unbanked people in urban as well as remote rural areas. However, mobile money also introduces risks that must be mitigated, including risks of criminal activity. The FATF and its stakeholders seek to ensure that financial integrity risks—the risk of money laundering, terrorist financing, or proliferation financing—are addressed effectively and that bringing more people into the formal financial framework does not come at the expense of effective controls.

Even developed countries with sophisticated regulatory mechanisms find it difficult to pursue crime fighting and economic development strategies simultaneously within the framework of financial services regulation. The profound difficulty of integrating these two distinct strategies into an effective policy framework is exacerbated in the context of rapid technological change. It is therefore not surprising that developing countries working with fewer regulatory resources than developed countries face enormous challenges in trying to integrate crime fighting and economic development goals under conditions of rapid technological innovation.

When the issue of financial inclusion first surfaced in the context of deliberations about global financial integrity standards nearly a decade ago, discussions threatened to become polarized between the more developed countries that set the international AML and CTF agenda on the one hand, and the development community who feared that effective financial integrity controls would create insurmountable barriers to financial inclusion on the other. The FATF, in conjunction with the World Bank and the Asia-Pacific Group on Money Laundering, released a 2011 guidance document on financial inclusion that helped to bridge this gap and moved the debate in the direction of a new consensus that
financial integrity and financial inclusion goals could be complementary. This new understanding is now integrated into, and strengthened by, the 2012 revised Recommendations.

Speakers from a variety of organizations and countries participated in the conference, providing theoretical, institutional and legal insights into the search for effective strategies to pursue financial integrity and financial inclusion policy objectives. The order of the Articles in this special issue follows the order of the presentations in the conference program, starting with general perspectives on mobile money, financial inclusion and financial integrity before proceeding to various developing and developed country case studies.

Professor Louis de Koker of Deakin University commenced the discussion with an overview of the revised 2012 FATF Recommendations and their impact on mobile money models in developing countries. His Article highlights aspects of the new standards, especially the mandatory risk-based approach, that would facilitate innovative mobile money models. In general the new standards are supportive of new payment methods for the unbanked and underbanked, but a number of questions and implementation challenges remain. These include lingering uncertainty about aspects of the risk-based approach. In his Article he also points to broader integrity risks that require attention, especially cyber-crime threats and mobile money-related privacy concerns. Mobile money programs are operating in a number of countries where the privacy of users may not necessarily be respected or effectively protected.

Professor Jane Winn of the University of Washington School of Law follows by looking forward to the challenges of governing the global mobile money network that is now emerging. She first

---


considers the role of information and communication technology (ICT) standards in the governance of existing global payment networks, including the costs and benefits of private, market-oriented governance systems versus “coordinated” governance systems which permit national regulators to play a greater management role. Because market-oriented global ICT networks can be deployed more quickly, there is always a risk that supporters of a more coordinated approach will be overtaken by rapid technological change. Market-oriented management of global ICT networks may undermine compliance with financial integrity information privacy obligations in the absence of a strong national or international regulatory counterweight. Balancing both market and regulatory requirements in the development of a global mobile money remittance network will be challenging. Achieving that balance will become even more challenging if representatives of developing countries are recognized as stakeholders in the governance of global mobile money networks.

Andrew Harris, a Foreign Affairs Officer at the U.S. Department of State, Professor Seymour Goodman and Assistant Professor Patrick Traynor (both of the Georgia Institute of Technology) raise in their paper concerns regarding the privacy and security of mobile phone users in Africa, particularly in light of FATF recommendations requiring user transparency and the collection of transaction data.5 Any requirement of user transparency in nations with weak adherence to the rule of law and limited privacy protections leaves users vulnerable to abuse. Furthermore, the increasing complexity of mobile phone use that is characteristic of mobile money applications raises concerns regarding Africa’s preparedness for heightened security threats that come hand in hand with increased use. The Article closes with specific recommendations for policy actions by African nations to improve consumer privacy and cyber-security.

Luca Castellani, the head of the UNCITRAL Regional Centre for Asia and the Pacific, focuses on the relevance of the UNCITRAL electronic payment framework for mobile money.

---

5 Andrew Harris, Seymour Goodman & Patrick Traynor, Privacy and Security Concerns Associated with Mobile Money Applications in Africa, 8 WASH. J.L. TECH. & ARTS 245 (2013).
Existing legal frameworks, whether they are statutory or contractual in nature, are often insufficient to address all the relevant legal issues, especially in developing countries. Appropriate legal frameworks will be required to fill the gaps in existing law. International standards and model laws, such as those prepared by UNCITRAL, can assist developing countries in filling those gaps in national laws while also ensuring cross-border consistency and reducing barriers to interoperability. The Article reviews elements of existing international instruments and commercial practice, and argues for the preparation of uniform enabling legislative or contractual provisions for mobile payments.

Claire Alexandre, a former Senior Program Officer and Lynn Chang Eisenhart, a Program Officer, both of the Financial Services for the Poor program at the Bill and Melinda Gates Foundation, argue that there are three key synergies between financial inclusion and financial integrity. These are: (1) mobile money will help reduce dependency on cash, which is the common enemy of both financial inclusion and financial integrity; (2) mobile money generates data which is instrumental to the health and growth of both financial inclusion and financial integrity; and (3) mobile money accelerates the development of accounts, which are the backbone of financial inclusion and financial integrity. If mobile money is to deliver on its promises for both financial inclusion and financial integrity, however, regulatory barriers need to be removed.

Emery Kobor, the keynote speaker at the conference, is the assistant director for strategic policy in the Office of Terrorist Financing and Financial Crimes at the U.S. Department of the Treasury and a member of the U.S. delegation to the Financial Action Task Force. In his Article he argues that the application of

---


AML measures does not necessarily determine the success or failure of financial inclusion initiatives or their impact on economic growth. Successful payments system innovation, particularly payment tools targeting underserved markets, requires effective entrepreneurship operating in an environment of good governance and rational economic policies. AML safeguards support a stable and safe environment by deterring corruption and other forms of financial crime. This in turn helps to establish and maintain economic stability and preserve the rule of law, thereby creating a supportive environment for innovation and financial inclusion.

These general perspectives on financial inclusion, financial integrity and mobile money are followed by five papers providing national perspectives on mobile money regulation. The five countries (in alphabetical order) are Brazil, Kenya, South Africa, the United Kingdom, and the United States.

Gilberto Almeida of the Pontifical Catholic University of Rio de Janeiro discusses the regulatory framework for mobile money in Brazil.9 The Brazilian hyper-inflation period led to the development of a sophisticated payments platform and a vast network of banking correspondents all over the country. The Article notes the significance of the rapid expansion of “banking correspondents” which are often retail vendors authorized to serve as cash-in/cash-out points for traditional bank accounts for financial inclusion in Brazil. While Brazil has made impressive strides in financial inclusion in recent years, mobile money has not played a significant role in these policies to date. Almeida does note, however, the growing interest among Brazilian regulators in adding mobile payments to their financial inclusion strategies. The Article addresses key aspects of the current mobile money framework in Brazil and the ways in which Brazilian regulators responded to financial integrity challenges posed by mobile money.

Mercy Buku, the Senior Manager of Safaricom’s Money Laundering Reporting Office and Michael Meredith of the

---

University of Washington School of Law discuss Safaricom’s M-PESA mobile money program in Kenya. The M-PESA service is recognized globally for its economic and social success. Since March 2007 it has enrolled more than 15.2 million users and transferred more than 1.4 trillion dollars in electronic funds. Their Article traces the development of the M-PESA service in Kenya and considers the role that services like M-PESA might play in national and international AML and CTF efforts.

Professor Vivienne Lawacks, the Executive Dean of the Faculty of Law, Nelson Mandela Metropolitan University in Port Elizabeth, South Africa, analyses the South African legal and regulatory framework for mobile money and examines issues relating to financial integrity and financial inclusion as they present themselves in South Africa. While South African regulators developed a supportive framework for mobile money, it is not a fully inclusive framework. The author highlights the plight of undocumented migrants and argues for a better balance between the regulation of risk and access to the payment system through an enhanced implementation of a risk-based approach.

Miriam Goldby of the Centre for Commercial Law Studies, Queen Mary, University of London, considers in detail a specific customer due diligence obligation, namely the obligation to report suspicions of money laundering. The United Kingdom has adopted stringent regulations regarding the reporting of suspicious transactions combined with draconian sanctions for failure to comply. As might be expected under such circumstances, the result has been a blizzard of suspicious activity reports filed with U.K. law enforcement that produce few discernible financial integrity benefits. She considers what the impact might be in a developing country of adopting reporting requirements similar to those that the

---

United Kingdom adopted in response to FATF requirements. The Article argues that certain features of the U.K. suspicious activity reporting regime make it unsuitable for wholesale adoption into such a context.

Erin Fonté of Cox Smith Matthews discusses mobile banking/mobile payments in the United States.¹³ Unlike mobile banking/mobile payments services in developing countries, these developments in the United States have not been driven primarily by financial inclusion concerns but rather by competition to serve an affluent target market more effectively. But with a high usage rate of mobile devices by the unbanked/underbanked in the United States, financial inclusion may also be improved through new mobile products and services. The Article outlines the regulatory framework for mobile money in the United States and discusses the regulatory position relating to mobile money. The position taken by the U.S. Treasury Department and the Financial Crimes Enforcement Network (FinCEN) with respect to the revised FATF Recommendations on transparency, customer due diligence and new technology could have an impact on who is eligible to participate in mobile payments.

APPRECIATION

We record our appreciation to all the presenters at the conference and to those who were able to contribute Articles to this special edition of the Washington Journal of Law, Technology & Arts. The authors took care to reflect developments through mid-2012 to ensure that the Articles are current and contribute to the dynamic international mobile money discussion.

We also wish to express our appreciation to the following persons and organization that made special contributions to ensure the success of the conference and the preparation of this special edition. The financial support of the Linden Rhoads Dean’s Innovation Fund made the entire conference possible. Laura

---

Powell worked tirelessly all summer to prepare the Articles for publication. Victoria Parker provided invaluable editorial and administrative assistance, while Elizabeth Coplan and Kathy Kline provided invaluable event planning assistance. Michael Meredith helped complete the process of preparing the Articles for publication. As our primary liaison with the *Washington Journal of Law, Technology & Arts*, Scott Patrick Kennedy kept the Articles moving through the review process until their publication.
Mobile money holds great financial inclusion promise, but also poses financial integrity challenges. The Financial Action Task Force (FATF)—the intergovernmental global anti-money laundering (AML) and counter-terrorist financing (CTF) standard-setting body—expressed support for financial inclusion and mobile money as a means to decrease the use of non-transparent cash in many developing countries. In February 2012, FATF adopted a new revised set of standards. This Article considers the impact of these new standards on mobile money models in developing countries. It highlights aspects of the new standards that would facilitate innovative mobile money models, but also points to questions and challenges. The new standards are generally more facilitative of new financial services models for the unbanked and underbanked, but a number of key questions and
implementation challenges remain. These include mobile money-related privacy and cyber-crime concerns.

TABLE OF CONTENTS

Introduction..................................................................................166
I. The FATF and Its Standards..................................................167
II. 2012 FATF Recommendations: Mobile Money Perspectives ..............................................................172
    A. Introduction......................................................................172
    B. The 2012 RBA Principles ................................................173
    C. Other Relevant Measures .................................................177
III. Risk Identification, Assessment and Mitigation..............182
    A. Conceptual Uncertainties.................................................183
    B. Risk Assessment and Controls .........................................186
    C. Risk Assessment and Cross-Border Services...................188
IV. Broader Integrity Risks.........................................................189
    A. Cybercrime.......................................................................189
    B. Privacy and Surveillance..................................................191
Conclusion...................................................................................196

INTRODUCTION

The international anti-money laundering (AML) and counter-terrorist financing (CTF) standards set by the Financial Action Task Force (FATF) directly and indirectly guide the design of key elements of financial service delivery models.\(^1\) In the past few years, as an increasing number of countries adopted financial inclusion policies, it became evident that interpretations of these standards were negatively impacting initiatives to provide viable and appropriate financial services to consumers.\(^2\) In 2011 the

---


\(^2\) Hennie Bester et al., Implementing FATF Standards in Developing
FATF adopted a guidance paper providing greater clarity about ways to align financial inclusion and sound AML/CTF policies. In February 2012, FATF’s support for financial inclusion was taken a few steps further when it adopted a new revised set of standards. This Article focuses on the impact of these new standards on mobile money models in developing countries. It highlights aspects of the new standards that would facilitate innovative mobile money models, but also points to questions and challenges.

The current AML/CTF standards framework in relation to mobile money is best understood against the backdrop of the pre-2012 position. This Article therefore begins with a brief overview of the tensions between the FATF standards and innovative financial inclusion models.

I. THE FATF AND ITS STANDARDS

The FATF is an intergovernmental body that sets global AML, CTF, and proliferation financing (financing of weapons of mass destruction in contravention of United Nations Security Council Resolutions) (PF) standards. These standards, known as the FATF Recommendations, provide countries with benchmarks for AML, CTF, and PF laws, service provider practices, and international cooperation in criminal matters. The standards outline acts that every country should criminalize to meet the FATF objectives, and the client due diligence (CDD) measures that financial institutions should adopt to mitigate and respond to risks of money laundering (ML) and terror financing (TF) abuse. These CDD measures include identifying and verifying the identity of every client, monitoring the client’s transactions for unusual or suspicious activities, and reporting this information to a national financial intelligence unit.

---


Despite its limited membership—by 2012 FATF had 34 countries and two regional organizations as members—the FATF has been tremendously successful in positioning its standards as global standards: more than 180 countries endorse the FATF standards.\(^4\) This is remarkable, given that the FATF was created as a temporary task team in 1989 and has been operating under temporary mandates since its formation.\(^5\) One of the factors\(^6\) underlying the FATF’s success as a standard-setting body is its system of mutual evaluation of compliance with the standards, coupled with indirect economic penalties for non-compliance. The compliance system extends to non-members. Non-compliance can expose a country to countermeasures by compliant countries and their financial institutions. In practice, these countermeasures mean that transactions and business relationships with persons from such jurisdictions are closely scrutinized. These countermeasures add to the costs of doing business with such countries, slow down the pace of transactions, and in many cases may even lead to a termination of business relationships.\(^7\) The FATF’s name-and-shame campaign and the threat of economic penalties were sufficient not only to move countries towards compliance, but also to ensure that smaller regulators and many financial institutions reacted by adopting overly conservative rules and practices.\(^8\)

In the past years, increasing evidence emerged that FATF-

\(^4\) FATF RECOMMENDATIONS, supra note 1, at 7. The fact that major countries such as India, Russia, and China endorsed the FATF Recommendations and amended their laws to meet the standards before gaining membership in the body bears testimony to the weight and impact of this body.

\(^5\) The FATF’s current mandate was set in 2012 and will continue to 2020.

\(^6\) Other factors—including its network of FATF-style regional bodies that provide non-FATF member countries limited opportunity to participate in and provide input into its processes, as well as the FATF’s range of observer bodies—also increase ownership of, and support for, their standards.


Based rules and the conservative mindset of regulators were impeding innovative financial services models and channels. Transformational mobile money models, for instance, require a regulatory framework that allows accounts to be opened via mobile phones without contact with the service provider’s employees. Non-face-to-face engagement gives rise to identity fraud risks. These risks are higher in developing countries that lack national identification frameworks or other means to verify the identity of customers easily and securely. Furthermore, mobile money channels rely on large networks of agents, third-party service deliverers, and ATMs to provide cash-in and cash-out points. This introduces ML/FT risks and complicates the reporting of unusual and suspicious transactions. Regulators in many countries reacted with unease to proposed business models, concerned that the FATF may frown on the level of risk that such a model introduced. These concerns slowed down the design of appropriate regulatory frameworks for mobile money.9

The FATF’s initial response was to defend its standards and to blame inappropriate, conservative responses on national regulators.10 The FATF pointed out that many of the concerns could be addressed if regulators applied a “risk-based approach” (RBA). The FATF’s 2003 Recommendations allowed countries and financial institutions to implement an RBA in relation to certain aspects of the AML/CTF framework. In terms of the FATF’s RBA, countries are allowed to exclude activity from


10 See, e.g., Paul Vlaanderen, FATF President, Speech at the ESAAMLG 9th Council of Ministers Meeting (Aug. 21, 2009).
AML/CTF regulation where the activity was limited and posed a low level of ML/TF risk. Institutions were urged to consider adopting an RBA 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.

While the basic principles of an RBA were clear, there was little agreement about appropriate risk assessment and risk mitigation measures and the extent to which an RBA could be implemented. Concern that the FATF may disagree with a particular interpretation and may list a country as non-compliant impeded the implementation of robust RBA frameworks in many smaller countries. In 2007 the FATF began to issue guidance on the RBA for regulated institutions, professions, and businesses. The guidance was helpful, but focused mainly on the identification and mitigation of higher ML-risk; it shed little light on the management of low-risk scenarios and an RBA in relation to TF risk. Financial inclusion models typically focus on small, low-value transactions. If they could be classified as a “low risk” transaction, many potential clients could be serviced despite their lack of formal identification documentation.

In 2010 the FATF, under the Mexican presidency, recognized that regulators required more certainty before they would take

---

11 FATF refers to “ML/TF risk” but, as discussed in Section II.A, the RBA does not fully extend to TF risk. It is also important to note that the RBA does not extend to PF risk.
bolder action to implement an RBA that would support financial inclusion. Following a consultative process, the FATF issued a non-binding guidance paper on financial inclusion in 2011. These developments were not only the result of increased international support for financial inclusion, but were also linked to increased FATF concern about the integrity risk of financial exclusion (i.e., the risk that persons may not use the formal financial system and thereby limit the reach and effectiveness of AML/CFT controls to mitigate financial integrity risks in the economy as a whole).

The FATF’s financial inclusion guidance paper highlighted steps that countries could take to align financial inclusion and AML/CFT policies. The guidance paper also listed various country examples without necessarily endorsing those as FATF-compliant. The discussions that led to the adoption of the guidance paper informed the drafting of the revised FATF Recommendations that were adopted in February 2012. Unlike the guidance paper, the Recommendations are binding and hierarchically superior to guidance papers. It is therefore expected that the financial inclusion paper will be revisited to clarify some aspects and ensure that the guidance reflects the current Recommendations. During the course of 2012 the FATF will also revisit its mutual evaluation methodology. This methodology guides the country reviewers when they produce a country compliance report in relation to the FATF standards. Regulators will study the new methodology with interest as it will set out the questions that country assessors have to ask. These questions are often of greater relevance to the design of compliant regulatory models than the broad statements of the Recommendations themselves. It is expected that the measure to evaluate appropriate risk-based responses will feature prominently in the new methodology.

With this brief background, this Article turns its attention to aspects of the new revised Recommendations that are particularly relevant to mobile money.

---

14 FATF 2011 GUIDANCE, supra note 3.
II. 2012 FATF RECOMMENDATIONS: MOBILE MONEY PERSPECTIVES

A. Introduction

The 2012 Recommendations are revised Recommendations. They are in essence refined versions of the AML Recommendations that were initially adopted in 1990 and revised extensively in 2003, as well as the FATF’s Special Recommendations on Terrorist Financing that it adopted from 2001. The intention was not to effect a radical change, but rather to clarify the existing Recommendations, strengthen their consistency, and address issues that lowered compliance levels of countries. While the texts of many Recommendations were not changed, the Recommendations were restructured and refined. The forty Recommendations on Money Laundering and the nine Special Recommendations on Terrorist Financing were consolidated into a single text of forty Recommendations, accompanied by an expanded glossary and interpretive notes to key Recommendations. As a result, the numbering of the Recommendations changed (for example, the text of former Recommendation 5 that addresses CDD is now found in Recommendation 10) and some of the text of a few Recommendations was moved to the interpretative notes. Examples were added to the glossary and the interpretative notes to explain aspects of the standards. These examples are not mandatory but merely illustrative.

In 2008 the FATF’s mandate was expanded to address [full name] (PF). The 2012 Recommendations, unlike their predecessors, therefore explicitly address proliferation and require countries to implement targeted financial sanctions to comply with United Nations Security Council Resolutions (UNSCRs) relating to the prevention, suppression, and disruption of proliferation of weapons of mass destruction and its financing.\textsuperscript{15} These resolutions target proliferation activities of specific states, for example through targeted financial sanctions. The resolutions also aim to prevent

\textsuperscript{15} FATF RECOMMENDATIONS, supra note 1, at 13 (Rec. 7).
non-state actors from acquiring weapons of mass destruction, for example by requiring criminalization of acts such as the manufacture, acquisition, use, or transport of nuclear, chemical, or biological weapons, including the financing of such activities. The FATF’s focus on proliferation is, however, not well defined. The FATF’s guidance focuses mainly on PF, but the wording of the key anti-proliferation recommendation, Recommendation 7, extends it to also include broader anti-proliferation measures in terms of the UNSCRs. In addition, the concept of “PF” itself is quite broad; and the FATF has not agreed on a working definition for its own purposes.\textsuperscript{16} Clarity is important because regulators and regulated entities, including mobile money providers, are expected to meet the FATF standards on AML/CTF as well as PF.

The RBA is a particularly prominent and now mandatory feature of the 2012 Recommendations. This approach is of key importance to mobile money and other financial inclusion initiatives.

\textit{B. The 2012 RBA Principles}

Recommendation 1 addresses risk assessment and the RBA principles that countries and institutions should implement.

The RBA is now mandatory for countries and institutions, but it is important to note that its application is limited to specific aspects of the AML/CTF framework. It can be used to expand or contract the regulatory sphere or to determine the nature of CDD measures to be implemented in respect of specific client, products or services. However, it cannot be used to argue that a country’s overall ML/TF risk is so low that it does not need to criminalize ML or TF. The RBA furthermore only extends to aspects of ML/TF, but leaves PF untouched.

The cornerstone of the RBA is risk assessment. Under Recommendation 1 countries are expected to “identify, assess and understand” their ML/TF risks. That assessment will then inform appropriate risk mitigation measures. Countries should apply an RBA to ensure that the risk mitigation measures are commensurate

\textsuperscript{16} FATF RECOMMENDATIONS, \textit{supra} note 1.
with the risks identified. Countries should also require their AML/CTF-regulated institutions to undertake risk assessments to mitigate their institutional ML/TF risks. Those institutional risk assessments should in turn be informed by the country’s risk assessment. Institutions should furthermore be required to adopt an RBA when they determine the extent of their CDD measures.

Where countries identify higher risks, they should adopt enhanced risk mitigation measures to ensure that the risks are adequately addressed. Where countries identify lower risks, they may—in strictly limited circumstances and where there is a proven low risk of ML/TF—elect not to impose AML/CFT obligations on institutions and businesses that should otherwise be regulated. They may also allow regulated businesses to implement simplified CDD in respect of low-risk clients, products and services. Simplified measures are, however, optional and conditional, while enhanced measures are mandatory where risks are high. In addition, the FATF has been cautious to ensure that country RBAs do not undermine key features of the AML/CTF system. The FATF has therefore set specific CDD measures in relation to types of clients, relationships, and activities that it deems as posing a universally high risk. The FATF does not allow countries to adjust that rating or the required risk mitigation measures even if certain types of clients, relationships, and activities pose a lower risk in a particular national context. Politically exposed persons17 and money or value transfer services are examples of customers and activities with set measures that should be applied.

The national RBA is mirrored in the RBA that is envisaged at an institutional level. Institutions must be required to assess their ML/TF risks and adopt prescribed or enhanced risk mitigation measures where risk is assessed or indicated as high. If the risk assessment presents an “adequate analysis” of risk,18 regulators

---

17 Politically exposed persons (PEPs) are generally defined as people who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, or important political party officials. PEPs, their family members, and close business associates may pose a corruption risk.

18 FATF RECOMMENDATIONS, supra note 1, at 64.
may permit institutions to adopt simplified measures where risks are assessed as low; however, simplified measures are not appropriate when there is a suspicion of ML/TF.\textsuperscript{19}

The Interpretive Note to Recommendation 10 provides far greater clarity than before about the RBA in relation to lower-risk products. The Interpretative Note lists non-binding examples of potentially lower-risk scenarios in relation to customers, country and regions and products, services and delivery channels. One of the examples is “financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.”\textsuperscript{20}

The Interpretative Note also provides more guidance regarding simplified CDD measures. Examples of possible measures include: verification of the customer and the beneficial owner identity after the establishment of the business relationship (for instance when transaction amounts exceed a defined monetary threshold); a reduction in the frequency of customer identification updates; or limited on-going monitoring of low-value transactions. The measures adopted must however be commensurate with the lower-risk factors. Whenever there is a suspicion of money laundering or terrorist financing, or where “specific higher-risk scenarios apply,”\textsuperscript{21} such simplified measures are not appropriate.

The meaning of “specific higher-risk scenarios,”\textsuperscript{22} is not quite clear. The phrase only appears in the discussion of low risk and simplified due diligence; it is not used elsewhere in the text of the Recommendations. Apparently the intention was to refer to the specific customers and activities where additional measures are required by the Recommendations, in other words, the matters addressed by Recommendations 12 to 16: politically exposed persons (PEPs); correspondent banking; money or value transfer services; and new technologies and wire transfers. The specific rules and procedures envisaged in these Recommendations therefore must be applied and cannot be simplified on the strength

\textsuperscript{19} Id. at 31.
\textsuperscript{20} Id. at 64.
\textsuperscript{21} Id. at 66.
\textsuperscript{22} Id.
of an institutional RBA, even though the institutional risk levels relating to those matters are very low. One implication is that mobile money providers should have appropriate risk management systems to determine whether a customer is a foreign PEP (one of the measures stipulated in Recommendation 12) and cannot dispense with such measures merely because their risk assessment reflects their PEP risk exposure as very low. This limitation compels providers to adopt risk mitigation measures that are disproportionate to the actual risk and runs counter to the regulatory principle of proportionality.23

Although the revised Recommendations improved the coherency of the RBA framework, some inconsistencies remain. Institutions are for instance compelled to undertake CDD in respect of business relationships, irrespective of value, but are not compelled to implement these measures in relation to non-account-based occasional transactions under US$/€15,000. Where an institution assesses its low-value account-based product as posing a low risk of abuse, it is still required to implement CDD measures, although they may be simplified. Many low-value financial inclusion accounts may never have a total amount of US$/€15,000 processed through them. Yet, the framework covers those accounts. Meanwhile a single transaction that involves US$/€14,000 is not required to be subjected to the FATF-envisaged CDD measures.

The RBA has furthermore not been extended to all CDD aspects. For example, it does not extend to the duty to determine whether clients were designated under UNSCRs for CTF purposes. This determination must be made irrespective of the degree of risk of doing business with a designated person under the name or names identified in terms of the UNSCR schemes.24 The PF measures have also been excluded from the RBA. Institutions will

---


24 The FATF view is that compliance with sanctions (i.e., identification of clients as designated persons for TF or WMD purposes) is not a function of risk. See FATF 2007 GUIDANCE, supra note 12, at 8.
therefore need to perform standard name-matching tests to compare client names with the listed names of UNSCR-designated persons as well as PEPs, even though their chances of transacting with such a person are assessed as very slim.\textsuperscript{25}

Despite these inconsistencies, the FATF’s RBA can be very helpful in removing FATF-related barriers to financial inclusion. Underlying this approach however, is an assumption that institutions will assess risks correctly and adopt simplified CDD when risks are assessed as low. The large-scale closure of accounts of Money Service Businesses by banks in response to often unfounded risk concerns has shown that this is not necessarily the case.\textsuperscript{26} Conservative institutions tend to overestimate risk and avoid it or adopt over-designed controls.\textsuperscript{27} Conduct of regulators and supervisors, such as harsh compliance enforcement action, may exacerbate this behavior. Adoption of simplified CDD measures is optional, but if institutions fail to do so when appropriate, financial inclusion can be undermined and financial exclusion risk would rise. Regulators have furthermore indicated that they are reluctant to intervene and force adoption of simplified measures where institutions decide that more stringent measures should be applied. It will therefore be vital for regulators and supervisors to create environments where institutions can assess and respond correctly to the different risk levels.

\textbf{C. Other Relevant Measures}

A number of other Recommendations are also relevant to mobile money.

Recommendation 15, for example, requires countries and financial institutions to identify and assess the ML/TF risks that

\textsuperscript{25} See Section III.B for questions regarding the value of these processes when CDD is simplified.

\textsuperscript{26} Bester et al., supra note 2, at 158-62.

may arise in relation to: (a) the development of new products and business practices, including new delivery mechanisms; and (b) the use of new or developing technologies for both new and pre-existing products. This recommendation tightens the wording of its 2003 predecessor by linking it directly to the RBA.\textsuperscript{28} Although this Recommendation is relevant to mobile money, it is largely superfluous in view of the more comprehensive and fundamental obligation of countries and financial institutions to assess all their ML/TF risks and to manage them appropriately.

The Recommendations addressing money or value transfer service (MVTS) and wire transfers are of greater relevance. An MVTS is defined in the glossary as referring to financial services that involve 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. Mobile money is an MVTS for purposes of the FATF standards.\textsuperscript{29}

In terms of 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.\textsuperscript{30} An exception is a financial institution that is already licensed and registered as such, allowed to offer MVTS and subject to the full range of applicable FATF measures.\textsuperscript{31} Mobile money account providers that are not licensed as such, for example

\textsuperscript{28} See FATF, FATF 40 RECOMMENDATIONS 6 (Rec. 8) (2003), available at http://www.fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf. In one respect a key measure of support for mobile money was weakened. The 2003 Recommendations urged countries “to encourage the development of modern and secure techniques of money management that are less vulnerable to money laundering.” \textit{Id.} at 9 (Rec. 20). This has now fallen away.

\textsuperscript{29} As in the 2003 set, MVTS as well as issuers and managers of means of payment (e.g., credit and debit cards, checks, traveler’s checks, money orders and bankers’ drafts, electronic money) are also defined as “financial institutions” for purposes of the FATF standards.

\textsuperscript{30} This is echoed in Recommendation 26, but that Recommendation requires regulation and supervision to ensure compliance with national AML/CFT standards.

\textsuperscript{31} FATF RECOMMENDATIONS, \textit{supra} note 1, at 69.
a telecommunications company, should therefore be licensed or registered to deliver such services. Any natural or legal person working as an agent for an account provider should also be licensed or registered by a competent authority, or the MVTS provider should maintain a current list of its agents accessible by competent authorities in the countries in which the MVTS provider and its agents operate. Those agents should be included in the AML/CFT programs of providers and should also be monitored for compliance with those programs.

MVTS providers are furthermore required to comply with the relevant requirements of Recommendation 16 in the countries in which they operate, whether directly or through their agents. Recommendation 16 requires MVTS providers to include specific and accurate originator (sender) information, and required beneficiary information, in their wire transfers messages, and to ensure that the information remains with the wire transfer or related message throughout the payment chain. They must furthermore ensure that they can take freezing action or prevent prohibited transactions when required by relevant UNSCRs on CFT or PF.

While Recommendation 16 gives rise to extensive general compliance obligations, it alleviates the overall compliance

---

32 *Id.* at 17 (Rec. 14).
33 *Id.*
34 There are some exceptions for example payments for goods or services using a credit, debit or prepaid card for the purchase of goods or services, as long as the card number accompanies all transfers flowing from the transaction. Person-to-person transfers using those cards as a payment system are, however, included in Recommendation 16. *See id.* at 70.
35 Confusingly the text of Recommendation 16 makes explicit reference to CFT only. However, it refers to sanctions against “designated persons and entities” and the definition of this concept in the glossary extends to targeted financial sanctions to support the control of WMD. *See Section III.B* for some practical difficulties that may arise regarding freezing of assets when identification requirements are simplified.
36 For example, cross-border wire transfers “should always contain: the name of the originator; the originator account number where such an account is used to process the transaction; the originator’s address, or national identity number, or customer identification number, or date and place of birth; the name of the beneficiary; and the beneficiary account number where such an account is
burden by means of a few pragmatic exceptions and rules, for example:

- Ordering financial institutions need not verify the identity of both parties to the transfer service. However, they must verify the sender’s identity and information while receiving institutions must verify the information of the beneficiary.

- Domestic wire transfers should also include extensive originator information, unless this information can be made available to the beneficiary financial institution and appropriate authorities by other means. In that case, the institution need only include the account number or a unique transaction reference number that will enable the transaction to be traced back to the originator or the beneficiary.

- Countries may adopt simplified identification requirements in relation to cross-border wire transfers involving amounts below US$/$€1,000. Simplified measures may allow party information to be limited to the name of the originator; the name of the beneficiary; and an account number for each, or a unique transaction reference number. This information need not be verified, unless there is a suspicion of ML/TF, in which case, each relevant financial institution should verify the information pertaining to its customer.

From a mobile money perspective, these rules and exceptions are especially helpful in relation to domestic, low-value wire transfers. However, as transaction values increase, the exceptions used to process the transaction. In the absence of an account, a unique transaction reference number should be included which permits traceability of the transaction.\(^\text{37}\) FATF RECOMMENDATIONS, \textit{supra} note 1, at 71.

\(^\text{37}\) The 2012 duty is more onerous than before. In terms of the previous standards, wire transfers below US$/$€1,000 could be exempted from CDD requirements. \textit{Id.}

\(^\text{38}\) It is not clear how this will be communicated between the two institutions or how the ordering institution will be able to comply, if they had no suspicion when receiving the funds but the suspicion was formed by the receiving institution.
will no longer apply and the standard requirements will have to be met.

The FATF standards also require service providers to report transactions that are suspected of involving ML/TF to the national Financial Intelligence Unit (FIU).\(^{39}\) Where a mobile money operator controls both the ordering and the beneficiary side of a wire transfer,\(^{40}\) the Interpretative Note to Recommendation 16 requires the operator to consider all the information received from both the ordering and beneficiary sides to determine whether a suspicious transaction report (STR) must be filed. The report should be filed in any country affected by the suspicious wire transfer, and relevant transaction information should be made available to the FIU.

The record-keeping standards are also relevant to the mobile money framework. Countries are required to ensure that financial institutions maintain, for at least five years, all necessary records on transactions, both domestic and international, in order to provide transactional forensic information to law enforcement.\(^{41}\) This duty extends to all records obtained through CDD measures, such as copies or records of identification documents (e.g., passports, identity cards, driving licenses, or similar documents), business correspondence, and internal notes on CDD in respect of each client. The records must be kept for at least five years after the business relationship comes to an end, or after the date of the occasional transaction.

While record-keeping has been a standard FATF obligation since 1990, it was broadened in 2012. Pre-2012, institutions were required to keep CDD records up to date. This duty has now been extended to documents collected under CDD processes. Financial institutions are required to ensure that documents, data or information collected under the CDD process is kept up to date and relevant by undertaking reviews of existing records, particularly for higher-risk categories of customers.\(^{42}\) Valid identification

---

\(^{39}\) Recommendation 20 does not explicitly extend to PF transactions. FATF RECOMMENDATIONS, supra note 1, at 19.

\(^{40}\) Id. at 73.

\(^{41}\) Id. at 15 (Rec. 11).

\(^{42}\) Id. at 66.
documents with expiry dates may need to be reviewed in the future to ensure that a copy of the current, unexpired document is on file. South Africa, for example, extended this obligation in 2010 to refugees. Refugees there obtain temporary government-issued identification documentation. Banks were instructed to ensure that refugee accounts are frozen when their identification document expires and that they should only be unfrozen when the client presents a new, valid temporary document. In South Africa this principle would also extend to other documents that have temporary validity such as drivers’ licenses and passports that are valid for fixed periods. A similarly strict interpretation of the FATF duty to keep documents up to date and relevant will lead to substantial increase in compliance obligations and potential hardship for many clients.

With this brief overview of key mobile money AML/CTF requirements under the new standards, this Article turns to risk assessment and mitigation.

III. Risk Identification, Assessment, and Mitigation

The FATF’s RBA enables regulators and mobile money providers to shape aspects of an AML/CTF risk control framework to better align financial inclusion and financial integrity objectives. A sound RBA is informed by risk assessments that present an “adequate analysis of the risk.” Proportional controls that mitigate the risks must then be designed, implemented, monitored and, where required, amended to manage the identified risks. Risk assessments must be revisited to ensure that assessments remain current and comprehensive. Superficially this may appear relatively easy, but important questions and challenges arise.

---


44 FATF RECOMMENDATIONS, supra note 1, at 64.
A. Conceptual Uncertainties

The FATF has not yet been able to reach consensus about the definition of risk. Given the RBA’s centrality to the new FATF framework, the absence of a consensus about this key concept is somewhat ironic.\(^{45}\) From a practical perspective it undermines the conceptual framework and uniformity required to ensure that country and institutional risk assessments inform one another.

There are of course globally accepted definitions of risk. The ISO 31000 (2009)/ISO Guide 73:2002, for example, define risk as the “effect of uncertainty on objectives.”\(^ {46}\) But there is not full agreement within the FATF that this definition is applicable to its RBA.

To add to the confusion, the risk questions that AML/CFT stakeholders pose may differ. Institutions often focus on ML/TF abuses that may render them liable, for example, by exposing them to fines for non-compliance with the law, or that may expose them to reputational risk. This is often the case where compliance officers lead the risk assessment processes. Regulators, on the other hand, require institutions to invest money to assess the likelihood of an abuse of their services or products for ML/TF purposes. Some of these transactions may hold little or no risk of direct negative financial impact on the institution and may even be profitable for the institution.\(^ {47}\) In short, institutions are concerned

---


\(^{46}\) “International risk management standards define risk as a function of the likelihood of occurrence and the consequence of risk events, where likelihood of occurrence is a function of the coexistence of threat and vulnerability. In other words, risk events occur when a threat exploits vulnerability. Formally, R, a jurisdiction’s level of ML risk, can be represented as: \( R = f(T, V) \times C \), where \( T \) represents threat, \( V \) represents vulnerability, and \( C \) represents consequence. Accordingly, the level of risk can be mitigated by reducing the size of the threats, vulnerabilities, or their consequences.” IMF, *supra* note 7, at 64.

\(^{47}\) The Australian regulator, for example, require reporting institutions to have an AML/CTF program to identify, mitigate and manage the risk of money laundering or terrorism financing that a reporting entity may reasonably face in providing designated services at or through a permanent establishment in Australia. See, e.g., Australian Anti-Money Laundering and Counter-Terrorism Financing Act § 84(2) (2006), available at http://www.comlaw.gov.au/Details/C2012C00375/Html/Text#_Toc321138619.
about the risk that employees may collude with criminals and facilitate money laundering or commit other breaches of the law that may render the institution liable or may cause damage to its reputation. They are not necessarily as concerned about a transaction that involves proceeds of crime of which its employees were unaware and where reasonable controls could not have prevented it. These transactions concern the regulator and the policymaker but not necessarily the institution, as chances of legal liability or reputational damage is small. While the institution may undertake a comprehensive risk assessment, its natural concerns and interests may skew the assessment.

Regulators may also have a more limited risk focus than often assumed in FATF discussions. A regulator may impose controls to keep proceeds of crime out of its regulated industry, despite the fact that it may move tainted funds to another regulated industry—where it becomes the concern of another regulator—or into the grey economy or to a neighboring country.

Policymakers generally have a broader perspective, but AML/CFT policymakers have not always been sensitive to the potential of money moving out of the formal economy into the informal economy or being trapped in that part of the economy. The FATF has also not yet determined whether to focus on the integrity of financial services or on the integrity of the economy, non-financial and non-formal, as a whole.48 Since 2001 it has focused on informal remittances, but not to the same extent on other informal financial services. Since 2011, however, it has voiced its concern about financial exclusion risks of people being forced or electing to transact using informal financial services, thereby limiting the reach and effectiveness of AML/CTF controls. Thus, the interplay between controls that preserve the integrity of formal financial services and those that push criminal activity into the underground economy requires far more FATF attention. This is even more important given that the 2012 FATF framework also extends to proceeds of tax crimes. The interplay between strict FATF-related controls and the movement of money in and to the

shadow or underground economy requires more attention than it received in the past.

Whether the assessment should gauge the risk of “substantial” or “significant” abuse—and the meaning of these terms would be debatable—or the risk of any abuse, however insignificant, has also not been settled. Generally the focus in respect to ML is on more significant abuse, measured by transactional value. More attention is therefore given to high-value transactions. Lower-value transactions, such as non-account-based transactions under US$/€15,000, may not be subject to any customer due diligence controls. The FATF, however, recognizes that small, low-value transactions may be relevant from a TF perspective.\(^49\) Two observations are relevant in this regard: (1) What poses a low risk from an ML perspective may not pose a low risk from a TF perspective, and institutions can only simplify CDD measures if both ML and TF risk levels are assessed as low; and (2) no provider of mass transaction services can state with confidence that the chances of processing one low-value transaction that indirectly supports a terrorist is low, especially when the country has even limited levels of TF risk. Statistically, the risk will increase as its business grows. A risk assessment that focuses on the chances of any TF abuse, however small, will therefore not tend to rate any risk as low.

Given that national risk assessments have to inform industry risk assessments and institutional risk assessments, the lack of conceptual clarity and commonality complicates discussions. In addition, the concept of “risk appetite” or “risk sensitivity” has not been sufficiently raised. Assessors are required to assess risk and to classify them into categories of “high” and “low” risk. That classification depends heavily on the assessors’ view of risk and of the benefit to be obtained when the risk is embraced. A person with a low-risk appetite would not tend to classify any risks as low, while one with a high-risk appetite would hold a different view. The FATF examples provide some guidance as to potential low-risk scenarios, but risk ratings depend very much on the context of

\(^{49}\) See FATF 2007 GUIDANCE, supra note 12, at 8; de Koker, Identifying, supra note 13, at 343-47; FATF 2011 GUIDANCE, supra note 3, at 19.
the assessment and the examples are not absolute or binding. Institutions cannot be expected to assess this risk correctly and confidently without guidance from their governments, and in many developing countries little guidance has been forthcoming.

B. Risk Assessment and Controls

Despite these uncertainties, a number of mobile money risk assessment models were developed to assist regulators and providers in undertaking risk assessments.

The World Bank, for example, identified four key ML/TF risk factors in relation to mobile money: anonymity (anonymous usage); elusiveness (ability to avoid the identification and tracing of parties to the transaction); rapidity (the speed of transacting); and poor oversight (limited regulation and supervision).\(^{50}\) The Groupe Speciale Mobile Association (GSMA) uses a risk assessment methodology constructed around these factors and assesses ML/TF risks that may stem from customers, merchants and retailers or agents, or that may stem from cross-border functionality.\(^{51}\) The FATF developed a risk matrix identifying risk factors, risk mitigants, and potential risk levels in relation to new payment methodologies, including mobile money. The work that commenced in 2006\(^{52}\) was further refined in 2010.\(^{53}\) In 2010 the United States Agency for International Development (USAID) also produced a comprehensive mobile financial services matrix that


includes an assessment of financial crime risks. 54

While these methodologies are helpful, they still need to be applied sensibly in each country and in relation to specific products in order to identify the relevant risks and to respond appropriately to each. This exercise is complicated by the fact that risk control measures themselves may produce risks that must be adequately addressed. Client identification processes, for example, increase the risk of data theft. In other cases they raise questions regarding the sensibility of the standard control measures that institutions are compelled to adopt.

For example, in a lower-risk context client identification may be simplified and verification may be postponed. On the other hand, service providers are required to scan names of clients against UNSCR lists of terrorists and persons associated with proliferation of weapons of mass destruction. Where a name match occurs, the transaction must be frozen. An investigation must be undertaken to determine whether the party to the transaction was the party listed by the relevant UNSCR. If not, the money can be released. Scanning and processes to ensure that such transactions are frozen add compliance costs to the business model. These costs may be disproportionate to the benefits in cases where simplified identification and verification measures are adopted. In essence, the benefit would be limited to the cases where a listed person uses his or her listed name to conclude such a transaction. That would be highly unlikely, especially as the simplified identification measures may not be sufficiently robust to compel such a person to use their actual name. Simplified identification measures also increase costs to investigate cases where name-matching occurs. The provider cannot undertake an appropriate background check based on the client information that it holds to determine whether or not it is a false match. The investigation itself may prove very difficult in a developing country environment. An innocent consumer would also bear some of the impact, having the transaction frozen until it can be established that the match was false. In essence, the measures will pose a burden for providers and

for customers whose names happen to match those of persons who were listed, but it will not be effective to prevent the listed persons from using the services.

A number of risk-control models suggest controlling the risks introduced by simplified identification measures through enhanced monitoring of transactions. Transactions are monitored to identify unusual transaction patterns. Monitoring is more effective when institutions know enough about their clients to identify when a client acts contrary to his or her normal or expected pattern of behavior. The less an institution knows about a client, the less value standard-monitoring processes may produce. Closer monitoring may in fact just generate longer lists of potentially unusual or suspicious transactions that do not lend themselves to further investigation.

Many standard low-risk controls, especially transaction and balance limits, are based on assumptions that they lower the usefulness of the product for ML or TF abuse. However, an increasing number of cases are emerging where criminals are patient and work in groups to abuse these products to launder money.55 While the incidence of abuse may therefore be higher than anticipated, the total amounts involved in these abuses should generally be far lower than amounts laundered through standard and higher-risk products. The ML risk may therefore still be regarded as low compared to other products, but whether the same can be said of TF risk is unclear.56 Simplified control measures, however, tend to attract abuse; and it is realistic to expect that abuse of these products will increase in future.

C. Risk Assessment and Cross-Border Services

It is challenging to undertake an assessment of a particular product’s AML/CTF risk. The challenges multiply when the mobile money model attempts to operate cross-border and the assessment, and controls must satisfy different regulators working

55 Isern & de Koker, supra note 9, at 5 (discussing micro and nano-structuring, i.e. splitting large amounts of dirty money into small or very small transactions). See also Section IV.A for the 2012 PostBank fraud.
56 See also Section III.A.
within different national legal frameworks. In many cases the countries may not share the same definition of ML/TF offenses. The FATF provides a flexible framework allowing countries to determine, for example, whether money laundering offenses can be committed negligently or only intentionally and whether it extends to proceeds of all crimes or only to proceeds of specific serious offences. Legal differences such as these, combined with different national crime and law enforcement environments, mean that a product may be assessed as posing a low risk in one country if offered only in that country, but may have a higher risk profile in another country if it operates across borders.

Encouraging developments in this context are comprised in the Southern African Development Community’s attempt to coordinate the development of ML laws among its members to support the development of cross-border financial services in the region.57 Greater legal uniformity will also support a regional RBA approach.

IV. Broader Integrity Risks

Much of the current integrity attention is devoted to ML/TF risk assessment and mitigation. However, broader, non-ML/TF-specific financial integrity risks of mobile money should also receive attention. This Article closes with a brief overview of some concerns regarding cybercrime and surveillance.

A. Cybercrime

Mobile money uses high-technology channels that are designed to be secure to the extent that the service provider can mitigate risks. However, there are also risks that originate on the user side. If the client fails to protect secure access details or if a virus infects the phone, the client is exposed to risk. Viruses pose an increasing risk as cheap smartphones spread through developing countries.

Ensuring that new users protect their access details and removing viruses from phones in remote rural areas where technical expertise is limited are challenging. This provides criminals and terrorists with new ways to profit from crime and to disrupt systems.

As mobile money networks and providers grow, employee risk also increases. Low-value accounts of the South African PostBank were, for example, targeted in a sophisticated theft on New Year’s Day in 2012. Although facts are still emerging, it appears that an organized crime group opened 103 small accounts in false names over a long period. This was done despite the fact that PostBank subjects all its clients to CDD processes before opening an account. The criminals also bribed an employee who was able to obtain security codes and could access the bank’s transactional control systems to identify accounts with large balances. The syndicate then raised the daily withdrawal limits on the false accounts to about US$55,000 per day, transferred money from the large accounts to the network of small accounts in false names and over the course of three days withdrew about US$3 to US$4 million dollars from ATMs in more than 5,000 withdrawals in different regions of South Africa.

Inside information is also essential in the schemes involving Subscriber Identification Module (SIM) swap frauds. In these schemes, fraudsters obtain sufficient details of a bank client who operates his bank account via a mobile phone and fraudulently request a SIM swap at the mobile phone provider. They use the swapped SIM to intercept and divert the randomly generated security passwords that are linked to the account. This enables them to operate the client’s account and divert funds without the client receiving account activity alerts from the bank.58

Cybercrime is, of course, very relevant to the providers of mobile money services. Mobile money services require a wide range of stakeholders to cooperate closely. To prevent vulnerabilities due to different security practices, standardization is required. One example of security standardization is the model of

the Payment Card Industry Security Standards Council. The Council was formed in 2006 by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc., to formulate open industry standards for global payment security.\(^{59}\) The Council has more than 600 global participating organizations representing industry stakeholders around the world.\(^{60}\) The Council’s standards range from management of security to technical matters regarding software and encryption. While standards such as these are crucial for the secure development of mass services, they challenge regulators to understand and evaluate the standards and their implementation by regulated institutions. They also require regulators to be vigilant to ensure that standards and requirements are proportional and do not unnecessarily limit market entry.

**B. Privacy and Surveillance**

One of the key objectives of the AML/CTF framework is to ensure law enforcement access to financial information of clients. While law enforcement and anti-crime social benefits of financial transparency is recognized,\(^ {61}\) it is important to be sensitive to potential abuse of financial information as well. An appropriate framework must be in place to ensure that the global movement to increase access to financial information is not abused by national governments to increase their access to private information.

The FATF standards are not designed to protect client information against inappropriate access and usage by government

---

\(^{59}\) *About the PCI Security Standards Council*, [OFFICIAL PCI SECURITY STANDARDS COUNCIL SITE](https://www.pcisecuritystandards.org).


agencies. This is not the purpose of these standards. However, if the current move towards transparency of financial information to government is not counter-balanced by appropriate controls, the AML/CFT standards may give some governments an excuse to invade privacy for their own political purposes.

This type of abuse is difficult to prove, but there are indications that concern is justified. A number of allegations have been made regarding selective implementation of AML/CFT laws against political opponents or to pursue other policy objectives. In addition, many countries lack sufficient and effective protective measures to prevent such abuse. The governance structures of some FIUs, for example, are not sufficiently robust to protect them from abuse for political purposes. The Egmont Group, a select group of national FIUs, and the World Bank undertook a survey in 2008 to probe aspects of FIU governance. Sixty-five FIUs participated in the survey, and the results provide grounds for concern. While many FIUs appear to meet basic good

62 “On the political level, two common problems frequently hinder efficient implementation of AML/CFT regimes in post-communist countries. The first is ‘selective implementation’ – that is, using AML/CFT laws to target political opponents. The other problem is ‘political risk.’ This means, governments and individual decision-makers adopting strong AML/CFT measures take the risk of being forced out of office by actors who prefer to maintain the unregulated status quo. Certain cases in Central Asia may illustrate ‘selective implementation.’” Elias Götz & Michael Jonsson, Political Factors Affecting AML/CFT Efforts in Post-Communist Eurasia: The Case of Georgia, 12 J. OF MONEY LAUNDERING CONTROL 59, 68 (2009).


governance requirements, a significant number do not meet these requirements and may therefore be vulnerable to political influence. For example, a significant number of the heads of FIUs (for example, 46 percent of the heads of administrative FIUs) are appointed by a minister, cabinet, or head of state. Additionally, 34 percent are appointed to fixed terms of office, while 62 percent do not have fixed terms. In more than half of the respondent FIUs, some other state body or judicial authority has access to the FIU’s data holdings, while 62 percent reported that they can (or must) disclose their findings or the results of their analyses to a superior authority (for example a ministry, government, or supervisory authority). It is encouraging that the new Recommendation 29 and its Interpretive Note seek to strengthen the autonomy of an FIU and the security and confidentiality of its information. Improvements will however take time to effect and in some countries may prove less effective than hoped.

In the mobile money context, the powerful access mechanisms of the AML/CTF framework and relatively weak anti-abuse and privacy protection mechanisms converge with the powerful data-generating and capturing ability of mobile telecommunications. Communication data reveal the views and social patterns of users. Mobile phone handsets can act as tracking devices enabling the tracing and location of users. Where the phone is used for financial services, the data is enriched by the payment and spending pattern of the user. In the past few years, an increasing number of developing countries imposed SIM-card registration requirements to ensure that users of mobile phone services are identified. Mobile phone service providers must identify and verify their contract and non-contract clients in processes that mirror AML/CTF client identification requirements. The policy objective behind these registration requirements is to use the data for law enforcement purposes and to prevent the abuse of these services by criminals. The data generated through mobile phone usage is therefore linked to a specific individual and can potentially provide a rich profile of that user.

A Wikileaks/International Privacy release of a cache of documents in 2011 showed that many large software companies have developed and marketed mass surveillance software to governments, including undemocratic and oppressive regimes. The
software enables governments to combine, manage and mine different sources of mass surveillance data and has been employed in relation to mobile phone usage as well.64

South Africa, one of the leading financial inclusion jurisdictions, stands accused of extensive intelligence surveillance of communications, both legal and, allegedly, illegal.65 Despite a modern constitution and rule of law, indications are that communications are intercepted for political purposes. Leaked recordings of taped telephone discussions of prosecutors, for example, scuttled the corruption prosecution of the current president of South Africa. South African mobile phone service providers have furthermore not been protective of client privacy when law enforcement requests information, sometimes releasing information on the promise that due legal processes will be followed and providing data of clients who are not subject to any criminal investigation.66

65 “[T]he National Communications Centre (NCC) [i]s an obscure, high tech facility set up in Gauteng during the 1990s. By 2008 it boasted a staff complement of some 300. The NCC’s telecommunications and computer equipment can intercept and analyse [sic] large volumes of voice and [I]nternet traffic, both indiscriminately by listening for keywords, and in a targeted way by focusing on individual phone numbers, email addresses and even voice prints. To date, the NCC has operated outside the bounds of national legislation, including the Regulation of Interception of Communications and Provision of Communication-related Information Act (Rica), which allows interception only with a judge’s warrant. The NCC, has relied on the loophole that it supposedly intercepts ‘foreign’ communications only, which is not regulated by domestic law. However, in practice the NCC has defined ‘foreign signals’ to include cross-border communications where one of the parties is in South Africa and the other abroad. And because of the globalization of [I]nternet traffic, many emails, voice-over-internet conversations and communication via social media such as Facebook and Twitter - even if both end parties are in South Africa - would also be susceptible.” Drew Forrest & Stefaans Brümmer, Spooks Bid for New Powers, MAIL & GUARDIAN, Feb. 3, 2012, available at http://mg.co.za/article/2012-02-03-spies-bid-for-new-powers.
66 This approach elicited a very strong judicial comment in S. v. Agliotti 2011 (2) SACR 437 (GSJ) (S. Afr.), available at http://www.saflii.org/za/cases/ZAGPJHC/2010/129.html, an organized crime prosecution that failed, amongst others because the integrity of mobile phone records was questionable. The evidence revealed a cooperative and informal relationship between the
AML/CFT systems can provide information that supports appropriate law enforcement. Mobile money can improve the lives of millions of vulnerable people in developing countries. However, the good that these systems can do should not blind us to the potential for abuse and the need for appropriate controls. Lack of protection and lack of trust, on the other hand, may undermine the usage of mobile money. For a variety of reasons, new users of formal financial services often continue to use informal services in parallel. Where users believe that their transactions may be monitored to their detriment, they may withdraw from formal services or use it only for transactions that can be monitored without any negative result for them.67 Such conduct would continue to sustain the grey economy and undermine the pro-

forensic investigators of telecommunications operators and law enforcement. It highlighted instances where records were provided before due legal process was followed; where large amounts of data were provided with no official being able to account for the whereabouts or the use of the records; and the request and provision of records of persons who had no involvement in criminal conduct, including the records of the senior and highly respected counsel of the defense: Judge Kgomo commented as follows:

Abuse of the system by the police was demonstrated by Hodes SC during cross-examination of these cellphone ‘experts’. For example, he elicited evidence to the effect that cellphone records of the accused’s attorney; himself, Hodes SC, accused’s counsel herein; his (Hodes’) father’s, also an advocate who has nothing to do with this case; other clients of accused’s counsel, Hodes SC like one Peter Skeet; phones of private attorneys’ firms and private investigator Warren Goldblatt; among many others, were subpoenaed and obtained by the police from the cellphone companies. This elicited a question from me at one stage to the effect whether if and when this country’s State President’s phone records were subpoenaed, whether they (the cellphone companies) would issue them out without much ado. The answer was that those records would be extracted and handed over without asking another question. It is my considered view that if this state of affairs did occur or does occur and is allowed to persist, WE SHOULD ALL BE AFRAID, VERY AFRAID!!!

Id.

financial inclusion objectives of the FATF. Abusive practices will also undermine the usage of mobile money when users discover that their service providers shared damaging information that exposed users to government repression.

Thus, appropriate protection of financial information should receive more attention. Greater emphasis on privacy and circumspection about the quality of governance in countries where mobile money projects are launched will assist in protecting the integrity of mobile money.

CONCLUSION

Mobile money holds much promise for the developing world. However, it holds both good and bad. The FATF’s attention is presently focused on the integrity consequences of mobile money within its limited objectives of AML/CFT/PF. The FATF, regulators and service providers still have some way to go before clarity is reached about appropriate mobile money and risk assessment and mitigation. However, there are also broader integrity issues that are relevant to providers, consumers and society at large that should be reflected in risk management practices to ensure that mobile money functions with integrity in all developing countries.
GOVERNANCE OF GLOBAL MOBILE MONEY NETWORKS: 
THE ROLE OF TECHNICAL STANDARDS

Jane K. Winn*
© Jane K. Winn

Cite as: 8 WASH. J. L. TECH. & ARTS 197 (2013)
http://digital.law.washington.edu/dspace-law/handle/1773.1/1197

ABSTRACT

Mobile money has the potential to be an effective policy instrument for financial inclusion in developing countries, but it also has the potential to fuel money laundering and terrorist financing. The 2012 revised Financial Action Task Force standards attempt to strike a workable balance between the goals of financial inclusion and financial integrity in developing countries. Mobile money schemes are mostly based in national markets, however, and are not normally designed to address the need of poor migrants for cheap, effective cross-border remittance services. Demand for such cross-border remittance services may drive the development of technical standards to build global markets from national ones. As in other global governance contexts, regulatory competition among both developed and developing countries is likely to arise, and be shaped by network externalities, the economics of platform markets, and new governance institutions as well as national government strategies. If such standard-setting efforts treat

* Charles I. Stone Professor, University of Washington School of Law, Seattle, Washington. Thank you to Louis de Koker, Laura Powell, Mike Meredith, and Vickie Parker for their feedback; all errors remain mine alone. This research was funded by University of Washington Royalty Research Fund Grant 65-2740.

This Article was presented at the Mobile Money in Developing Countries: Financial Inclusion and Financial Integrity Conference held in April 2012 at the University of Washington School of Law with the support of the Linden Rhoads Dean’s Innovation Fund.
compliance with AML/CTF as requirements, then the growth of global networks might promote both inclusion and the development of “integrity by design” in global mobile money technologies. Co-regulatory mechanisms already in place in the United States and European Union for managing the interface between technical standards and legislation might provide some helpful models for accomplishing this. Ensuring that the governance of global mobile money networks is effective, legitimate, and accountable from the perspective of stakeholders in both developed and developing economies will be difficult, however.

**TABLE OF CONTENTS**

Introduction ..................................................................................198
I. Globalization, Migration, and Remittances ...........................206
II. Mobile Money: Financial Inclusion and Financial Integrity .................................................................................208
III. Standards, Networks, and Platforms........................................213
IV. Governance and Regulatory Competition ............................220
V. Integrity by Design ...............................................................227
VI. Co-Regulation for Global markets........................................232
Conclusion ...................................................................................242

“This notion of standards, as boring as it is, is really the plumbing of the Internet economy,” Thibeau said. “It turns out that you can only go so far . . . until you come up with standards. Standards build markets. Standards help the pie grow bigger.”¹

**INTRODUCTION**

Globalization integrates what once appeared to be separate national markets, creating new challenges and opportunities in its

wake. Opportunities spawned by globalization are not exclusively for the wealthy and educated in developed countries: the volume of migration by the world’s poor seeking a better life has also grown enormously in recent decades. Even when the poorest economic migrants enjoy modest success, however, they face another challenge: finding safe, inexpensive ways to send relatively small amounts of money back home. If they have migrated within a country that has a robust domestic remittance system, then this challenge is easily overcome. But most poor migrants live in countries that have made little progress in financial inclusion, or have migrated abroad and so must find a cross-border remittance mechanism.

This Article was written for a conference examining the impact of financial inclusion and financial integrity strategies on the growth of mobile money services in developing countries. In this Article, “mobile money” refers to mobile financial services generally, including mobile payments and mobile banking. As a

---

2 “There are far more international migrants in the world today than ever previously recorded, and their number has increased rapidly in the last few decades…[in 2000, there were an estimated 150 million migrants; in 2010, there were an estimated 214 million].” INT‘L ORG. FOR MIGRATION, WORLD MIGRATION REPORT 2010, THE FUTURE OF MIGRATION: BUILDING CAPACITIES FOR CHANGE 3 (2010).


5 There is no generally accepted definition of “mobile money,” but the definition used in this Article has been used in other contexts. See generally Janine Firpo, E-Money–Mobile Money–Mobile Banking–What’s the Difference?, BLOGS.WORLDBANK.ORG (Jan. 21, 2009), http://blogs.worldbank.org/psd/e-money-mobile-money-mobile-banking-what-s-the-difference; PIERRE-LAURENT CHATAIN, ANDREW ZERZAN, WAMEEK NOOR, NAJAH DANNAOUI & LOUIS DE KOKER, PROTECTING MOBILE MONEY AGAINST FINANCIAL CRIMES xxvii (2011) (mobile money “refers to a financial service in which customers send and receive monetary value via a mobile phone. This includes retail payments and remittances from one person to another or between businesses. Salary and benefit distributions into mobile-linked accounts are also encountered in some countries. M-money accounts can be provided by many types of institutions,
result of the success of mobile payment schemes in countries such as Kenya\textsuperscript{6} and the Philippines, mobile money has emerged as a game-changing strategy for financial inclusion in developing countries.\textsuperscript{7} For the purposes of this Article, financial inclusion is defined as “. . . a state in which all people of working age have access to a full suite of quality financial services that includes payment services, savings, credit, and insurance. These services are provided at affordable prices, in a convenient manner, and with dignity for the clients.”\textsuperscript{8} In 2009, the World Bank estimated that the unbanked population of the world was 2.7 billion, or 70 percent of the adult population in the developing world.\textsuperscript{9} Financial inclusion has been shown to increase economic growth, reduce income inequality and help alleviate poverty for this population.\textsuperscript{10}

In this Article, “financial integrity” refers to controls over financial services that support anti-money laundering and counter-terrorist financing as well as conventional control objectives including disclosure to investors and management decision-making. Although compliance with international anti-money


\textsuperscript{7} George B. Radics, Development and Mobile-Banking in the Philippines (2011) (unpublished draft) (on file with author).


laundering and counter-terrorist financing (AML/CTF) guidelines has been seen as a barrier to the use of mobile money for financial inclusion in other developing countries, the 2012 revisions to Financial Action Task Force (FATF) AML/CTF guidelines reflect efforts to address these concerns.\footnote{FIN. ACTION TASK FORCE, INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION: THE FATF RECOMMENDATIONS (2012) [hereinafter 2012 FATF RECOMMENDATIONS], available at http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%20(approved%20February%202012)%20reprint%20May%202012%20web%20version.pdf.} In developing countries, AML/CTF policies may sometimes appear to be dictated by external stakeholders, while safety and soundness concerns including the management of operational risks may appear to be more within the purview of national regulators.\footnote{Rainer Hülsse, Even Clubs Can’t Do Without Legitimacy: Why the Anti-Money Laundering Blacklist Was Suspended, 2 REG. & GOVERNANCE 459 (2008); Claire Alexandre, Ignacio Mas & Daniel Radcliffe, Regulating New Banking Models to Bring Financial Services to All, 54 CHALLENGE 116 (2011).} This Article will focus on those areas of financial market regulation conducted by national regulatory authorities where the two different strategies overlap, while conceding that there may be significant areas where they do not overlap or may even be at odds with each other.\footnote{Exploring possible conflicts between FATF Guidelines and national financial services regulatory objectives is beyond the scope of this Article. On potential conflicts between transnational anti-money laundering efforts and national regulatory objectives, see generally 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 (2011); Mariano-Florentino Cuellar, The Mismatch Between State Power and State Capacity in Transnational Law Enforcement, 22 BERKELEY J. INT’L L. 15 (2004).}

To date, most efforts to promote the development of mobile money as a financial inclusion strategy have centered on national markets. As adoption rates grow for mobile money within national markets in developing countries, increased attention will turn to the possible use of mobile money for cross-border remittances.\footnote{DALBERG GLOBAL DEV. ADVISORS, CGAP LANDSCAPE STUDY ON INTERNATIONAL REMITTANCES THROUGH MOBILE MONEY (2012), available at http://www.gsma.com/developmentfund/wp-content/uploads/2012/03/2012landscapestudyoninternationalremittancesthroughmobilemoney.pdf.}
Demand for such cross-border remittance services will fuel demand for the development of a global mobile money network architecture based on a wide range of different types of “standards.” In English, the word “standard” can refer to a bewildering array of different things, however. In U.S. legal academic writing, a “standard” may refer to regulatory guidance or an open-ended principle contained in judicial precedent as opposed to a formal legal rule. In social science or policy analysis, it might be a reference to “normative standards and advisory guidance” issued by “private regulators.” In engineering, “standard” may refer to measurement standards, product and process standards, management standards, or interoperability standards. In this Article, the term “technical standard” will generally be used to refer to engineering standards, while the term


16 For example, the OXFORD ENGLISH DICTIONARY online version recognized 28 separate meanings for “standard” as a noun (rather than an adjective or verb), with numerous sub-classifications within each of those 28 meanings. Standard Definition, OXFORD ENGLISH DICTIONARY, http://www.oed.com/view/Entry/188962?rskey=w0q1fc&result=1#eid (last visited Sept. 16, 2012).


“standard” without qualification will generally refer to legal and political norms.

The architecture of global markets is increasingly defined by information and communication technology (ICT) interoperability standards. This is because in recent decades, business administration has migrated from traditional bureaucracies and paper communications to network organizations linked by computers. The rise of ICT networks as the backbone of economic organization together with decades of trade liberalization are major factors contributing to the rise of global markets from what were once geographically remote local markets. Technical interoperability can be achieved in a wide variety of ways, including proprietary technologies that operate as de facto standards such as the Microsoft Windows operating system. Technical interoperability can also be achieved through open, collaborative processes such as open source software development or public standard-setting processes such as those conducted under the auspices of the International Organization for Standardization (ISO) or the Internet Engineering Task Force. Governance of technical standard-setting processes and managing the “interface” between national laws and technical standards are fundamental tasks that must be accomplished in order for any global market to function at an operational level. Interface here is used a metaphor for a “regulatory tool” or “mechanism choice.” When ICT networks operate in both developing and developed countries simultaneously, these governance and management challenges become even more complex and difficult.

Different national governments respond to the challenges of

---


22 See, e.g., Howard Williams, Internet Governance: Exploring the Development Link, 58 COMM. & STRATEGIES 81 (2005); CGAP, supra note 18.
globalization in different ways because they take their institutional endowments and local political and economic culture into account when designing strategies. In the “varieties of capitalism” approach developed by Hall and Soskice, some countries can be identified as “liberal market economies” (LMEs) and others identified as “coordinated market economies” (CMEs). The most noteworthy LMEs include the United States, the United Kingdom, Canada, Australia and New Zealand, while Germany, France and Japan are noteworthy examples of CMEs. In the context of mobile money as a financial inclusion and financial integrity strategy, the general LME/CME distinction might also be applied to the political economy of developing countries: Kenya seems to be a “developing country LME” while India seems to be a “developing country CME.” As a global network architecture for mobile money begins to emerge, distinct regulatory competition strategies may also emerge for developed LME, developed CME, developing LME and developing CME countries. As in all global markets defined by ICT networks, however, national regulatory competition strategies may be affected by economic variables such as strong network effects or the emergence of platform markets.

The 2012 FATF Guidelines strengthened the “Risk-Based Approach” to AML/CTF compliance efforts by making it mandatory rather than optional. Regulators in developing countries will need more sophisticated tools than most now possess to demonstrate their compliance with this expanded Risk-Based Approach mandate. One common benefit of technical standards is reducing barriers to the diffusion of innovations. Although attention in mobile money standard-setting efforts is currently focused primarily on reducing barriers to its adoption, standardization efforts could also be focused on reducing the cost

---


24 See infra Section III, Standards, Networks, and Platforms for further discussion of network effects and platform markets.

of demonstrating compliance with guidelines. With regard to computer security generally, it is now proverbial that “[s]ecurity is best baked in to the network, not bolted on later.”26 With regard to information privacy, an analogous concept is known as “Privacy by Design.”27 If technical standards for mobile money could be used to promote financial inclusion and reduce compliance costs simultaneously, such a result might be labeled “Integrity by Design.” Unless AML/CTF compliance issues are included in the scope of mobile money standard-setting activities, however, such a result is very unlikely, given the current security issues in the ICT networks of many developing countries.28 The flood of computer security and information privacy problems currently facing developed countries as a result of underinvestment in security in the past and the difficulty of retrofitting effective security and privacy functions onto existing systems suggests what the costs might be of postponing AML/CTF compliance considerations in the global mobile money context.29

Ensuring that the governance of global mobile money networks is effective, legitimate, and accountable from the perspective of stakeholders in both developed and developing economies will be difficult.30 The calculus of consensus building regarding


28See generally Andrew Harris, Seymour Goodman, & Patrick Traynor, Privacy and Security Concerns Associated with Mobile Money Applications in Africa, 8 WASH J.L. TECH. & ARTS 245 (2013).


30See generally Anne Peters, Lucy Koechlin & Greta Fenner Zinkernagel, Non-State Actors as Standard Setters: Framing the Issue in an Interdisciplinary Fashion, in NON-STATE ACTORS AS STANDARD SETTERS 1 (Anne Peters, Lucy Koechlin & Greta Fenner Zinkernagel eds., 2009); Benedict Kingsbury, Nico
technology governance in the global information economy is complex and uncertain under the best of circumstances. If the shortest route to bringing technological innovations to market is adopted to achieve financial inclusion goals, the result may be the inadvertent creation of barriers to efficient compliance with AML/CTF mandates. But if technological innovation is required to take a back seat to the integration of compliance functions, then financial inclusion may suffer. If participation in governance is conditioned on technological sophistication and familiarity with global ICT standard-setting processes, then many developing country stakeholders will be disenfranchised. But if ICT technical standard-setting processes become too politicized, then the standards they produce may fail to achieve any market adoption at all. Some resolution of these issues will be necessary in order for a global mobile remittance network to succeed politically as well as economically.

I. GLOBALIZATION, MIGRATION, AND REMITTANCES

Although the term “globalization” only came into widespread use during the 1990s, the current wave of economic globalization is not the first. The first wave of globalization occurred between 1870 and 1914, even though it was not given that label at the time. Although trade in goods increased, the hallmark of this first globalization was the mass migration of as much as 10 percent of the world’s population over this period. The scale of this migration has never been seen before or since. It was halted by the outbreak of World War I and law reforms during the interwar years intended to restrict immigration from the Old World in Europe and Asia to the New World of North and South America.


The second wave of globalization occurred between 1950 and 1973, and was ushered in by trade liberalization policies and technological innovations such as the containerization of shipping. This wave of globalization consisted largely of increased volume of trade in goods. Migration was modest in scope and involved as much migration of professionals out of developed countries to developing countries as workers from developing countries to developed ones.

The third wave of globalization began in 1974 and continues through today. Migration is again accelerating, with hundreds of millions leaving developing countries in pursuit of economic opportunity, at the same time that trade in goods continues to increase. Although the absolute numbers of migrants may be unprecedented, the current rate of migration affects only a tiny percentage of world population.

Economic migrants send home remittances, so the global market for remittances has grown together with migration. According to official estimates, the equivalent of US$440 billion in remittances was sent in 2010, although the actual volume of remittances is probably much higher. Of this amount, approximately US$325 billion or roughly 75 percent was sent to developing countries. The total volume of remittance flows to many developing countries dwarfs direct foreign investment and foreign aid payments, and may equal 25 percent or more of GDP in some developing countries.

Economic migrants from developing countries often send relatively small amounts of money. Relative to the amount being transferred, remittance fees are often very high, averaging 10 percent of the principal transmitted. As a result, many migrants rely on informal remittance systems. Informal remittance services

---


35 Id.

offer fertile ground for money laundering and terrorist financing. If migrants were provided access to inexpensive, efficient remittance services, this could promote increased financial inclusion and financial integrity at the same time.

II. MOBILE MONEY: FINANCIAL INCLUSION AND FINANCIAL INTEGRITY

“Financial deepening” has long been understood to play an important role in the development process:

Economists have long contemplated the nature of complex links between financial development and economic growth . . . . Since the early 1990s, a growing body of [work by economists] has provided strong theoretical and empirical support for the hypothesis that financial development fosters economic growth.37

In developing countries, widely disparate access to modern financial institutions and the persistence of traditional sources of finance, often create barriers to financial deepening and economic development:

A developed financial system broadens access to funds; conversely, in an underdeveloped financial system, access to funds is limited and people are constrained by the availability of their own funds and have to resort to high cost informal sources such as money lenders. Lower the availability of funds and [increase] their cost, fewer would be the economic activities that can be financed and hence lower the resulting economic growth.38

---

The idea of finding ways to provide banking services to the poor in developing countries slowly began to gain momentum during the 1990s.\footnote{John Conroy, Jamie Bedson & Nina Nayar, Banking with the Poor Network: A History of Asia’s Regional Microfinance Network 1990-2010 (2001), available at http://www.fdc.org.au/data/BWTP_Corporate_History.pdf.}

In 1999, United Nations Secretary-General Kofi Annan estimated that half of the six billion people that then constituted the world’s population had never even made or received a telephone call.\footnote{Kofi Annan, U.N. Secretary-General, Opening Address at the ITU Telecom Opening Ceremony, ITU: Committed to Connecting the World, (Oct. 9, 1999), quoted in Clay Shirky, Half the World, Clay Shirky’s Writings About the Internet (June 30, 2002), http://shirky.com/writings/herocomeseverybody/half_the_world_old.html.} Around the same time that observation was offered, liberalization of telecommunications markets in the wake of the WTO telecom agreement was triggering a communications revolution in many developing countries.\footnote{Peter Cowhey & Mikhail M. Klimenko, The WTO Agreement and Telecommunications Policy Reform (World Bank, Policy Research Working Paper No. 2601, 2001), available at http://siteresources.worldbank.org/INTRANETTRADE/Resources/Cowhey_Klimenko1.pdf.} The entry of China into handset and telephone switching equipment markets also helped to fuel the growth of mobile communications in developing countries by reducing equipment prices.\footnote{See generally Eric Harwit, China’s Telecommunications Revolution (2008).} Because telephones were not a major platform for the delivery of financial services in any country in the world during the 1990s, the connection between telephones and financial inclusion was not obvious to anyone at the time. During the 2000s, however, the sudden diffusion of mobile communications in developing countries emerged as the \textit{deus ex machina} which unexpectedly made many financial inclusion problems look less intractable. As The Economist pointed out, “In places with bad roads, unreliable postal services, few trains and parlous landlines, mobile phones can substitute for travel, allow quicker and easier access to information on prices, enable traders
to reach wider markets, boost entrepreneurship and generally make it easier to do business.”

The success of some early mobile payments schemes in Kenya, South Africa and the Philippines helped to bring the issue of AML/CTF compliance for mobile payments into focus. The first international treaty to recognize the connection between national anti-money laundering efforts and the control of international crime was the 1988 United Nations Convention on the Illicit Traffic in Narcotic Drugs and Psychotropic Substances. In 1989, the FATF was established at the initiative of what were then known as the G7 nations following the adoption by the United Nations General Assembly of a universal pledge to halt money laundering. Membership of the FATF started with 16 countries, and over the years gradually expanded to the current 36 members, including 34 countries and 2 regional organizations; international organizations such as the World Bank and International Monetary Fund (IMF) are observers. Regional FATF-style bodies are granted associate member status. In addition, nearly 150 other countries have committed to compliance with FATF guidance even though they are not members. In 1990, FATF issued a set of 40 Recommendations, and these were supplemented by Special Recommendations on Terrorist Financing that it adopted in 2001. The Recommendations were revised in 1996, 2003, and 2012. The

---

44 Buku & Meredith, supra note 6.
46 Radics, supra note 7.
48 NICOLAS RYDER, FINANCIAL CRIME IN THE 21ST CENTURY: LAW AND POLICY 16 (2011) (The G7 nations included Canada, France, Germany, Italy, Japan, United Kingdom, and United States).
FATF is not a formal international organization established by a treaty, but rather a very vigorous and surprisingly durable *ad hoc* task force, although it also has the support of the United Nations. Members of the FATF have committed to implement the recommendations and agreed to be subject to multilateral surveillance, peer review and the publication of the International Cooperation Review Group list (formerly known as the Non-cooperative Countries and Territories list). FATF works to ensure compliance with its Guidelines by requiring member countries to undertake an annual self-assessment, as well as mutual evaluations.

In 2000 and 2001, FATF published lists identifying 23 “non-cooperating countries and territories” that it found were not trying hard enough to fight against global money laundering. After a country was “blacklisted”, FATF worked with its regulators to help them bring their national regulatory systems into compliance with its guidelines. The blacklist’s regulatory bite came from the fact that FATF members in good standing were expected to take “counter-measures” to protect their economies from the risks of money laundering originating in blacklisted countries. The counter-measures required financial institutions in member states to conduct enhanced customer due diligence before engaging in financial transactions with any individuals or entities in blacklisted countries. Given the expense of such enhanced due diligence, the practical result of being placed on FATF’s blacklist was that the volume of financial transactions into and out of a country could be sharply restricted. The FATF blacklist turned out to be more effective at getting the attention of “non-cooperating countries and territories” than its sponsors may have anticipated which in turn unleashed an intense backlash. When the World Bank and IMF

---

joined the chorus of protests from developing countries about FATF’s lack of transparency and due process in its enforcement efforts, FATF backed off the blacklist strategy after only two years.  

As financial inclusion became a more prominent issue in the development community, it did not take long for concerns to emerge about what impact stringent AML/CTF requirements might have on financial inclusion strategies in developing countries. As part of the move to Risk-Based Approach to compliance, FATF published reports on how its Risk-Based Approach could be applied to new payment methods including mobile money, and issued guidance on financial inclusion policies generally. Whether these efforts by FATF are enough to counteract the impression left from its use of the blacklist to coerce compliance, however, remains unclear. In 2011, the Alliance for Financial Inclusion produced for the G20’s Global Partnership for Financial Inclusion a study of the impact of various global standard-setting organizations, such as FATF and the Basel Committee, on financial inclusion policies of five developing countries.

All [five] country case studies identified the FATF as the [standard-setting body] with the most significant impact on regulatory innovation in relation to financial inclusion. The degree of impact

53 Hülsse, supra note 12.
is mainly driven by concerns regarding the substantial penalties for non-compliance with the FATF Recommendations. The FATF framework is the only standards surveyed in this study with significant punitive measures for non-compliant jurisdictions, most notably the potential loss of correspondent banking relationships. These punitive measures may apply to members as well as non-members. Such penalties may have far-reaching economic impacts on a non-compliant country if it results in economic and financial isolation. As a result, regulators are understandably hesitant to adopt measures that may expose their countries to reputational damage and the potential loss of corresponding bank relationships.\footnote{GLOBAL P'SHIP FOR FIN. INCLUSION, GLOBAL STANDARD SETTING BODIES AND FINANCIAL INCLUSION: INSIGHTS AND LESSONS FROM FIVE COUNTRIES: BRAZIL, KENYA, MEXICO, THE PHILIPPINES, AND SOUTH AFRICA 9 (2011), available at http://www.gpfi.org/sites/default/files/documents/Global\%20Standard\%20Setting\%20Bodies\%20and\%20FI.pdf.}

With time, recognition by FATF member countries that financial inclusion promotes the migration from the more opaque cash economy to the more transparent formal economy may help to ameliorate this legacy of mistrust and uncertainty in developing countries.\footnote{Peter Dittus & Michael Klein, On Harnessing the Potential of Financial Inclusion 17 (Bank for Int’l Settlements, Working Paper No. 347, 2011), available at http://www.bis.org/publ/work347.pdf.} The 2012 FATF Guidelines reflect the ongoing effort of FATF member countries to emphasize the complementarity of financial inclusion and financial integrity policies.\footnote{See generally 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 (2013).}

III. STANDARDS, NETWORKS, AND PLATFORMS

In financial markets, ICT standards play an important role in increasing the “velocity” of assets by reducing transaction processing times; increasing transparency for lenders, borrowers,
and regulators; reducing transaction costs; improving accuracy of data processing; and reducing compliance monitoring costs for both managers and regulators.\textsuperscript{60} ICT standards are one type of technical standard. Technical standards are documents that establish engineering norms for products or processes. The International Organization for Standardization (ISO) has defined standards as:

\begin{quote}
[A] document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context[.] . . . based on the consolidated results of science, technology and experience, and aimed at the promotion of optimum community benefits.\textsuperscript{61}
\end{quote}

Formal standards are developed by standard-developing organizations (SDOs) and are often a type of “public good.” Public goods are goods that are non-rivalrous (meaning that consumption by one person does not diminish the possibility of consumption by another) and non-excludable (meaning that it is not possible to prevent anyone from enjoying its use). Classic examples of public goods include ideas, national defense or broadcast television. Formal standards are often a particular type of public good known as a “club good” which is non-rivalrous but exclusive. Classic examples of club goods include telephone or cable television networks. Formal standards are normally copyrighted by the organization that produced them, and must be purchased by anyone wishing to use them, so they do not normally qualify as pure public


goods. Formal or *de jure* standards may be contrasted with *de facto* standards which emerge from practice but which may lack any form of legal recognition. For example, the Microsoft Windows operating system is a *de facto* standard for personal computer software, but it is not a formal standard.62 *De facto* standards may function as both “private goods” (i.e., private property) and club goods simultaneously.

From an economic perspective, public goods are often problematic because there are usually insufficient market incentives to produce them in the quantities required by the public.63 For example, a national highway system has many of the characteristics of a public good. A government may choose to make its national highway system non-excludable and pay for its construction with government revenues, or it may permit a private organization to build the highway and then exclude users who do not pay tolls to recapture the costs of its construction. In the absence of either government construction using tax revenues or a license to operate a highway as a toll road, however, a national highway system is unlikely to emerge because private parties would normally have no incentive to build it.

Technical standards function as economic infrastructure that reduces barriers to the dissemination of technological innovation, and increases consumer welfare by ensuring technical interoperability among products made by different producers. As with other public goods, market forces alone may not produce the optimal level or design of technical standards because private parties may prefer to focus their attention on private goods for market production. The economic benefits of proprietary technologies may be concentrated on the owner of the technology while their costs are spread over a large group of users, but with standards, the benefits are spread over a large group of users while the costs are concentrated on a smaller group of producers.

62 As a matter of national regulatory culture, regulators in LMEs such as the United States are more willing to treat *de facto* standards as equivalent to formal standards, while regulators in CMEs are more inclined to deny that they are standards at all. That debate is outside the scope of this Article.

Because they produce widespread benefits, the development and promotion of technical standards are normally pivotal elements of national industrial policy in developed market economies. By contrast, treating proprietary technologies as de facto standards conflates the private nature of proprietary technologies and the public nature of “standards” as that term is defined by ISO.

The governance framework for technical standard setting may vary significantly between LMEs and CMEs, with LMEs favoring a “bottom up” private sector driven approach while CMEs favor a “top down” government orchestrated approach. Although issues related to the governance of technical standard-setting processes may be controversial, there is more of a consensus regarding the costs and benefits of using standards. The social and economic benefits of standardization include:

- Reducing costs through the simplification of complex processes;
- Reducing learning costs for new producers;
- Allowing producers to exploit economies of scale;
- Lowering transaction costs between transacting parties;
- Promoting market information and confidence by signaling product quality, or the compatibility of products or components;
- Reducing compliance costs; and
- Increasing competition among producers, lowering prices to consumers.

---


However, the costs of standardization may also be substantial and include:

- Reducing product variety;
- Imposing costs of achieving compliance with standards and obtaining certification of compliance;
- Imposing one-time switching costs for established products to comply with subsequent standards; and
- Increasing switching costs away from obsolete or sub-optimal standards.

Formal public international standard-setting organizations that may have jurisdiction over ICT technical standards include the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the International Telecommunications Union (ITU); each of these organizations has a formal, public counterpart in each country that chooses to participate in them. While the processes used by these global technical standard-setting organizations seek to be transparent and inclusive, they may also be slow, bureaucratic, and out of touch with conditions in the markets in which the standards are to be implemented.67

Technological change in markets for ICT products may be very rapid, and because consumer demand for new ICT products often depends on their interoperability with other ICT products, there is also a need for rapid development of ICT standards. In order to ensure that ICT standard development can keep pace with rapid technological innovation in global ICT markets, new forms of private international standard-developing organizations known as “consortia” or “fora” have emerged in recent years.68 These new

---


ICT SDOs range in size from a small handful of members working closely together to thousands of members scattered around the world collaborating by means of Internet communications. The Internet Engineering Task Force (IETF), developer of the Transmission Control Protocol/Internet Protocol (TCP/IP) standard which defines the Internet, and the World Wide Web Consortium (W3C) are examples of large, informal ICT standard-developing organizations with members around the world. By contrast, EMVCo, the ICT SDO for the European EMV payments standard, has only four members: American Express, JCB, MasterCard, and Visa. Informal private ICT SDOs are often referred to as consortia, and because they are generally exempt from regulation by national governments, they can often develop standards more quickly and efficiently than formal, public ICT SDOs.69

Although consortia may not be formally recognized under international law as a source of technical standards,70 what they lack in formal legal status, they often make up for in market power.71 This will be true if consortia standards define networks

---


70 The status of standards issued by formal international SDOs such as ISO, IEC and ITU comes in part from the recognition that their adoption as national standards provides countries with a defense to claims brought under the WTO Technical Barriers to Trade Agreement. See generally Scott Kennedy, The Political Economy of Standards Coalitions: Explaining China’s Involvement in High-Tech Standards Wars, 2 ASIA POL’Y 41 (2006).

71 In principle, ISO does not work directly with consortia. It normally reissues national standards submitted by national standard setting bodies (e.g., ANSI, the British Standards Institute, Association Française de Normalisation (AFNOR), Deutsches Institut für Normung (DIN), Japanese Standards Association, etc.) as international standards, or develops international standards. However, ISO does maintain two back doors—a “fast track” process and a “publicly available submission” process—that under certain circumstances permit consortia to submit standards directly to ISO for review without first getting them adopted by a national standards body.
characterized by strong “network effects.”72 Network effects are created when strong positive and negative externalities drive consumers to use only one network, which may give the network operator a dominant market position as well as de facto regulatory authority over network participants.73 Markets operating within ICT networks may also be characterized as “multi-sided platforms.”74 The operator of a platform market may contribute to the success of the platform by setting prices to attract certain participants to it. Such a strategy consists of imposing high prices on those who have the most interest in the success of the platform, and low prices to those who have the least interest. Classic examples of such pricing strategies include the use of advertising revenues to subsidize the purchase of newspapers by consumers, or selling a video game console at cost, and then setting the price to end users of computer games high enough to subsidize the development of new games.

If a global platform for mobile remittances emerges, and its operators enjoy significant market power based on strong network effects, then national regulators could find themselves under pressure from their own citizens clambering to enjoy its positive network effects to give such a platform local market access. If a global network operator has enough market power, it may be able to resist pressure to bear the cost of “localizing” its services to comply with regulations in each national market it enters. Under such circumstances, national regulators may be forced to choose between granting citizens access to a global network and exercising their authority in their national markets. This issue has already emerged in global electronic payment services with regard to the authority of global card payment services companies such as Visa and MasterCard to control the terms and conditions under

72 See generally CARL SHAPIRO & HAL VARIAN, INFORMATION RULES (1999).
which their services are supplied in different countries around the world.75

IV. GOVERNANCE AND REGULATORY COMPETITION

Regulatory competition refers to competition among different sovereigns for mobile economic resources such as labor and capital by offering different regulatory regimes to attract them.76 “Race to the bottom” regulatory competition strategies generally involve regulatory regimes that externalize the costs of attracting mobile economic resources onto someone other than the owner of the resource either inside or outside of a sovereign’s territory. For example, using weak labor and environmental protection laws to attract foreign investment may externalize some production costs onto workers and citizens affected by pollution within that country while allowing foreign investors to enjoy increased profits as a result of lower nominal production costs. “Race to the top” or the “California effect” is the opposite strategy: a sovereign with market power can require producers to internalize more production costs than other sovereigns do. California used this strategy successfully when it required the use of catalytic converters on all cars sold in California. When other sovereigns followed California’s example, then producers that had adapted to the stricter California standard had a competitive advantage over producers that had not yet done so. The analysis of regulatory competition becomes even more complex when national governments are competing with non-state and hybrid regulators


whose scope of authority is ambiguous and whose regulatory tools are different.\footnote{Burkard Eberlein, Kenneth W. Abbott, Julia Black, Errol Meidinger & Stepan Wood, \textit{Transnational Business Governance Interactions: Conceptualization and Framework for Analysis}, \textit{7 Reg. \& Governance} (forthcoming 2013).}

With regard to a global network for mobile remittances, regulatory competition could arise among both developed and developing countries to shape the governance framework for mobile money networks. In addition to network externalities and the economics of platform markets, regulatory competition in global markets is shaped by the interaction of nation states with new private global governance institutions by a new trend:

\textit{[T]he delegation of regulatory authority from governments to a single international private-sector body that, for its area of expertise, is viewed by both public and private actors as the obvious forum for global regulation. In that particular issue area, such a private body is what [Büthe and Mattli] refer to as the focal institution for global rulemaking. This simultaneous privatization and internationalization of governance is driven, in part, by governments’ lack of requisite technical expertise, financial resources, or flexibility to deal expeditiously with ever more complex and urgent regulatory tasks.\footnote{BÜTHE \& MATTLI, supra note 18, at 5.}}

The FATF is clearly a “focal institution of global rule-making” for financial integrity, while the Society for World-Wide Interbank Telecommunications (SWIFT) is a focal institution for global remittances executed by banks. It is unclear now what institution, if any, will emerge as the focal institution for the emerging global mobile remittance network.

In the information technology field, the question of what kind of “focal institution of global rule-making” should govern the Internet remains a matter of considerable and persistent international controversy. The current focal institutions for the
Internet include the IETF and W3C, which are informal collaborative networks of individuals and organizations, and the Internet Corporation of Assigned Names and Numbers (ICANN), a California non-profit corporation backed by the U.S. government. While many citizens and governments in LMEs support the management of the Internet by IETF, W3C and ICANN precisely because they are private, many citizens and governments in many CMEs (as well as authoritarian societies) believe strongly that the ITU as a formal, public and international SDO should govern the Internet instead.79

In specific ICT markets, either conventional SDOs or consortia may play the role of focal institutions. The Institute of Electrical and Electronics Engineers (IEEE) is a conventional SDO, the modern successor to electrical industry SDOs going back to the nineteenth century. The IEEE is accredited by the American National Standards Institute (ANSI), which means that it complies with the due process requirements contained in ANSI Essential Requirements.80 The IEEE developed the IEEE 802 family of local area network standards for wireless communications that includes technologies marketed to the public as Wi-Fi. After the IEEE 802.11 standard was developed, however, promotion of the Wi-Fi concept was turned over to the Wi-Fi Alliance, a consortium which is not ANSI accredited. The Wi-Fi Alliance manages the use of the Wi-Fi trademark and logo, and certifies that products are compliant with the standard, in addition to developing new standards in response to changing market conditions. The Wi-Fi Alliance has two classes of voting members: a small group of “sponsor members” with more authority over decision making, and “regular members.” It also has affiliate members with limited voting rights

and adopter members without voting rights. The Bluetooth Special Interest Group (SIG) develops standards for short-range, low-cost wireless communication technology for use with mobile devices and also promotes the adoption of the technology. Even though the Bluetooth SIG generally maintains open, transparent processes, it also maintains different classes of membership, and restricts admission: individuals are not allowed to join at all, and control over the most important management decisions is retained by seven “promoter” companies (Ericsson, Intel, Lenovo, Microsoft, Motorola, Nokia, and Toshiba). GS1 is the most important international radio frequency identification (RFID) SDO, and is considered to be a consortium. It is the successor to the Uniform Code Council and EAN International, the organizations that promoted the use of barcode technology since the 1970s. It has affiliated organizations in over 100 countries, and participation in GS1 activities is managed through the local affiliates. The GSM Association (GSMA), the main SDO and industry association for mobile telephone services around the world, is also a consortium. Full membership in the GSMA is limited to wireless network operators, and other businesses in one


of four categories are eligible to join as associate members, but individuals cannot join.\footnote{Types of Membership, GSMA, http://www.gsma.com/membership/types-of-membership/ (last visited Jan. 5, 2013).}

The whole idea of an ICT standards consortium originated in the United States, so it is not surprising that the official U.S. Standard Strategy treats the work of ICT consortia as equivalent to the work of formal SDOs.\footnote{AM. NAT’L STANDARDS INST., UNITED STATES STANDARD STRATEGY 3 (3d ed. 2010), available at http://www.ansi.org/standards_activities/nss/usss.aspx (“Global standardization goals are achieved in the United States through sector-specific activities and through alliances and processes provided by companies, associations, standards developing organizations, consortia, and collaborative projects.”).} This openness to treating consortia and formal public SDOs as equivalent is generally limited to LMEs, however. Until very recently, European regulators have been hostile to the idea of recognizing standards developed by consortia in legislation or public procurement, preferring instead to rely on international standards issued by formal public SDOs such as ISO or ITU, or standards developed by formal European SDOs.\footnote{European formal SDOs are very similar in structure to international formal SDOs: the European Committee for Standardisation (CEN), which corresponds to ISO, the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI) which correspond to the ITU; cooperation between CEN and ISO is governed by the Vienna Agreement and cooperation between CENELEC and IEC is governed by the Dresden agreement. \textit{See generally Winn, supra note 20.}} European regulators have justified their reluctance to embrace consortia standards by noting the success of the European CME approach to ICT standardization in the case of GSM technology.\footnote{Jacques Pelkmans, \textit{The GSM Standard: Explaining a Success Story}, 8 J. EUR. PUB. POL’Y 432 (2001).} Since the success of GSM, however, there have not been many major successes for the European CME model of ICT standardization in global markets, making it more difficult for EU regulators to avoid working with consortia standards. In 2011, the Commission announced its intention to permit reference to consortia standards in EU regulations and public procurement, provided that the processes by which those standards were
developed meet European due process standards:

The selected ICT standards will complement European standards and must comply with quality criteria. Those criteria, which address both the standards developing processes and the standards themselves, cover matters such as openness, transparency and neutrality as well as imposing the same minimum requirements as applied by the ESOs for the treatment of intellectual property (IP) rights.89

The EU quality criteria for consortia due process come from the Code of Good Practice for the Preparation, Adoption and Application of Standards, Annex 3 to the WTO Agreement on Technical Barriers to Trade.90

The European Union is clearly engaged in a “race to the top” regulatory competition strategy with regard to recognition of consortia ICT standards. While critics of its standards strategy might view the United States as engaged in a “race to the bottom” by permitting ICT consortia to pursue market opportunities unencumbered by social regulations, supporters of the U.S. approach would characterize it as “bottom up” (i.e., populist rather than “top down” or bureaucratic) and market-driven.91 European regulators are calculating they can use access to the European Internal Market for leverage in their regulatory competition with the United States to influence the character of the global information economy. If this strategy is not successful, then the

---


91 See generally Winn, supra note 73.
architecture of the global information economy will continue to be dominated by U.S. standards policy.

If the emerging global mobile remittance architecture becomes a platform market as well as a network supported by strong network effects, then regulators in developed and developing CMEs may find it difficult to exercise regulatory authority over its operation within their borders. This is because the private operator of a successful ICT-based platform has considerable discretion with regard to the terms and conditions of access to the platform market, and the prices of services offered through the platform.92 Once a platform based on global ICT networks takes root within a domestic economy, regulators may find it difficult (although not impossible) to mandate changes in the way the platform operates.93

A market-driven globally interoperable mobile remittance network is already emerging. Visa and GSMA are partnering with financial institutions, mobile network operators, handset manufacturers, technology service providers, and industry associations around the world to build that global architecture.94 Because this effort is being spearheaded by the private company that administers the largest proprietary payment card network in the world,95 and a private ICT consortium, its roots are clearly in the LME environment. This is not the only source of standards for mobile remittances, however. For example, the Government of India is actively promoting the development of a domestic Indian mobile payments architecture based on open standards.96 If the

92 See generally Evans et al., supra note 74.
93 David S. Evans, Interchange Fees: The Economics and Regulation of What Merchants Pay for Cards vi (2011), available at http://origin.library.constantcontact.com/download/get/file/1102767390831-1382/Interchange-Fees-web-2.pdf (noting that the United States, European Union, and Australia have all taken action in recent years to force credit card networks to change their pricing policies).
95 Panel Report, supra note 75, at § 7.39 (“[I]t is the [Electronic Payment Service] provider’s intellectual property that enables the switching of the transaction and supports the electronic payment process, the transaction is governed by the EPS provider’s rules and procedures . . . .”).
96 Indian Banks Collaborate on Merchant Payments Platform, GTNews
Indian CME approach to standardizing mobile payments is successful within the Indian domestic market, it might appeal to regulators in other developing countries.97

V. INTEGRITY BY DESIGN

For national regulators in developing countries who are working to promote financial inclusion, significant challenges arise in two broad areas of AML/CTF compliance: establishing identity under agreed “know your customer” (KYC) or “customer due diligence” (CDD) rules; and “suspicious transaction reporting” under agreed protocols to detect suspect patterns of financial transfers.98 For developing countries such as China and Kenya that had strong national identity systems in place long before AML/CTF norms were even invented, it might be possible to use ICT standards to rationalize KYC processes and make them more efficient. For countries such as India that have never had a strong national identity system, the Risk-Based Assessment approach in the 2012 FATF Guidelines now permits national regulators and mobile payment service providers to develop alternative KYC protocols for which ICT standards may have little relevance.99


98 Dittus & Klein, supra note 58.

99 For example, Reserve Bank of India KYC regulations permit someone without any other identity documents to use a letter from a recognized public authority or public servant verifying the identity and residence of the customer in order to open a bank account. Master Circular – 'Know Your Customer' (KYC) Guidelines – Anti Money Laundering Standards, RESERVE BANK OF INDIA (July 1, 2009), http://rbi.org.in/scripts/BS_CircularIndexDisplay.aspx?id=5083. India is currently building a national digital identity system. See generally Planning Comm’n, Unique Identification Authority of India, UIDAI, http://uidai.gov.in/ (last visited Jan. 5, 2013); see also Louis de Koker, Will RICA’s Customer Identification Data Meet Anti-Money Laundering Requirements and Facilitate the Development of Transformational Mobile Banking in South Africa?: An Exploratory Note, CTR. FOR FIN. REGULATION & INCLUSION (Oct. 7, 2010), http://www.cenfri.org/documents/...
Because national endowments with regard to identifying citizens vary so widely across developing countries, ICT standards may be more useful in lowering AML/CTF compliance costs if they focus on “suspicious activity reporting.” Financial institutions in developed countries already use sophisticated analytics on large databases of transactional information to detect patterns of behavior that might indicate money laundering. 100

Historically, advanced analytics have been used, among other things, to analyze large data sets in order to find patterns that can help isolate key variables to build predictive models for decision-making. Companies use advanced analytics with data mining to optimize their customer relationships; law enforcement agencies use advanced analytics to combat criminal activity from terrorism to tax evasion to identify theft. Naturally, these methods have their limits; for example, data mining in search of new patterns in counter-terrorism may yield little value. 101

If data formats and analytics for suspicious activity reporting related to mobile payments could be standardized, that might reduce barriers to the use of those same technologies in developing countries. Just as falling prices of telephone switching equipment and handsets helped spark the mobile telephony revolution in developing countries, falling prices for servers, processors, open source database software designed to work with very large databases, high bandwidth networks, cloud computing and other flexible resource allocation arrangements might make it possible

100 John Beck & John Morton, How Banks Can Make the Most of Data, THE BANKER (June 1, 2012), http://www.thebanker.com/Tech-Trading/Technology/How-banks-can-make-the-most-of-data?ct=true (“Today, most banks are using analytics very much on a departmental or a business unit basis, such as in their credit risk, market risk or anti-money laundering capabilities.”).

for managers and regulators in developing countries to enjoy at least some of the benefits of “Big Data.” Increasing the use of data analytics among mobile money service providers might be one strategy to help regulators and service providers in developing countries take full advantage of the flexibility offered with the Risk-Based Approach in the 2012 FATF Guidelines. However, because even sophisticated business enterprises in developed countries find it difficult to extract the full value of “Big Data,” it is clear that regulators and service providers in developing countries would require not just ICT standards but also considerable technical assistance in order to deploy similar technologies effectively under more difficult circumstances.

Current best practices in the development of information technology indicate that factors like privacy and security, or by analogy, financial integrity, should be treated as requirements from the beginning of the design process in order to be effective. Ann Cavoukian, Privacy Commissioner of Ontario, Canada, coined the term “Privacy by Design” to describe a rigorous, proactive approach to information privacy. The concept includes early mitigation of privacy concerns when developing information technologies and systems, as well as continued focus on privacy concerns throughout the entire information life cycle. The notion of Privacy by Design was always consistent with EU data protection law principles, and has now been embraced by EU regulators as a key element of their approach to thinking about the design of information technology and privacy. The U.S. Federal Trade Commission has now incorporated the idea into its

---

103 Andrew McAfee & Erik Brynjolfsson, Big Data: The Management Revolution, HARV. BUS. REV., Oct. 2012, at 60 (to reap the rewards of big data analytics will require changes in leadership, talent management, technology, decision-making processes, and company culture).
104 Cavoukian, supra note 27.
information privacy strategy as well.\textsuperscript{106} Alan Paller, of the SANS Institute, makes a similar point about computer security generally when he argues that security only works if it is “baked in,” rather than being “bolted on” after a product has been completed.\textsuperscript{107} Support for this “end-to-end” approach to privacy and security is growing among some leading information technology companies, and has been incorporated into their product development processes, although this change in attitude in the private sector is far from universal.\textsuperscript{108}

Recent attempts by the global payment card industry to upgrade security on its existing network provide a cautionary tale of how difficult and controversial the process of retrofitting privacy and security technologies can be. In 2004, the global credit card industry launched the Payment Card Industry Data Security Standard (PCI DSS) as a joint industry effort to respond to pressure from regulators in countries with strong data protection laws about the security of personal information in their systems, and to reduce the costs associated with large data breaches involving the loss of consumer payment card information by retail merchants. The PCI DSS standards are intended to establish a mandatory minimum level of security for retail merchants processing consumer card data, and range from basic common sense (do not use vendor-supplied default passwords) and modern risk management best practices (maintain a written security policy and regularly test security), to very specific requirements (use a firewall, issue a unique ID to each person accessing the system). Early versions of the PCI DSS standard were widely criticized by retail merchants as expensive and ineffective, and for having been developed by the credit card networks and banks without adequate consultation with the retail merchants expected to implement them.\textsuperscript{109} Even after the PCI DSS standard-setting process was


\textsuperscript{108} Rubinstein, supra note 27.

\textsuperscript{109} Michael Garry, PCI Seeks Retailer Feedback, Supermarket News (July
opened up to greater participation by all stakeholders, and the investment of many years of effort in implementation, independent surveys suggest widespread non-compliance with PCI DSS standards persists even in developed countries. Litigation in the United States has even called the legality of the scheme into question: when an American bank exercised its right under the scheme to fine a merchant for its alleged failure to comply with the standard, the merchant filed suit against the bank, highlighting the lack of accountability and transparency in the administration of the PCI DSS standards, and the bank’s failure to prove that the security breach had originated with the merchant in the first place.

While embracing the notion of “Integrity by Design” for the development of a global mobile remittance architecture might reduce the risks associated with trying to “bolt on” financial integrity functions after the network is already operational, such an effort would also introduce new risks. Whenever the requirements for standards are expressed too broadly, or incorporate too many politically contested factors, then the odds that the resulting standards will be widely adopted usually decline unless adoption is mandated by a regulator. At present, there is no global regulator capable of mandating compliance with ICT technical standards for mobile remittances that incorporate financial integrity requirements. If the adoption of ICT technical standards for global

110 Mathew J. Schwartz, 67% Of Companies Fail Credit Card Security Compliance, INFORMATIONWEEK (April 20, 2011), http://www.informationweek.com/security/management/67-of-companies-fail-credit-card-security/229401946 (“PCI may have an image problem. According to the study, 50% of security professionals view PCI as a burden, and 59% don’t think it helps them improve security. Furthermore, comparing this study with the inaugural one conducted in 2009, the number of respondents who said they had sufficient resources to comply with PCI dropped from 40% to 38.”); John Leyden, Firms Are RUBBISH at Payment Security: One in Five Bothered to Meet Standards, THE REGISTER (Sept. 29, 2011), http://www.theregister.co.uk/2011/09/29/pci_compliance_survey/.
mobile remittances is left up to the market and individual national regulators, then the more narrowly such technical standards focus on market demand, the greater their chance of widespread adoption.

Developed countries are only now starting to try to incorporate social requirements like privacy and security into the design of ICT networks from the beginning.\footnote{For example, the EU General Data Protection Regulation proposed in 2012 would mandate “data protection by design and by default” in the processing of personal information, which has been controversial. Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), COM (2012) 11 final (Jan. 25, 2012), available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.} Trying to incorporate social requirements like financial inclusion and financial integrity into ICT technical standards for global mobile remittances in order to achieve “Integrity by Design” in developing countries might be an even more challenging task than trying to achieve “Privacy by Design” in developed countries, and would be undertaken with even fewer resources. Because market conditions in developing countries may be more diverse and complex than market conditions in developed countries, merely developing ICT technical standards for interoperability may prove difficult, and adding AML/CFT compliance obligations to the scope of the standard-setting activity might doom it to failure.

VI. CO-REGULATION FOR GLOBAL MARKETS

In Europe, when the work of legislatures and standard-setting organizations is formally and explicitly coordinated, the resulting process is known as “co-regulation.” In the United States, similar processes are more likely to be referred to as “self-regulation.”\footnote{The delegation of U.S. federal securities regulation authority to “self-regulatory organizations” such as the New York Stock Exchange or National Association of Securities Dealers (NASD) is a clear example of this. Joel Seligman, The Transformation of Wall Street 185-86 (3d ed. 2003) (1939 decision to delegate regulatory powers to NASD because of skepticism about government competence to regulate many aspects of the securities market).}
However, because economic “self-regulation” even in LMEs takes place in the context of continuous dialogue between the state and private-sector actors, and involves at least some degree of implicit or explicit delegation of state authority, the term “co-regulation” could apply to what is referred to as “self-regulation” in the United States, but would often be more accurate. For this reason, the term “co-regulation” as used in this Article should be understood as including most of what is referred to as self-regulation in LMEs.

Since the rise of the modern industrial standards movement in Western nations in the late nineteenth century, governments of economically developed countries have developed some kind of administrative “interface” between the institutions that develop technical standards and the formal, public legal order, including courts and legislatures. As in other areas of economic regulation, the LME countries tend to favor an ad hoc piecemeal approach to coordinating legislation with relevant technical standards, while CME countries tend to favor a formal, systematic approach. The diversity of co-regulation approaches in the United States is a reflection of the diversity of standard-setting organizations that are recognized under U.S. law. For example, although the official U.S. Standards Strategy largely consists of letting the private sector lead, some standards are issued as mandatory government regulations, such as the U.S. Department of Agriculture’s standard for what constitutes “milk.” Private-sector standards normally

---


115 See Tate, supra note 64.


118 7 C.F.R. § 1000.15 (2012) (“[F]luid milk product means any milk products containing less than 9 percent butterfat intended to be used as
function only as voluntary guidelines for compliance with government regulations, but may be converted into mandatory regulations by government action.\textsuperscript{119} For example, when the Consumer Product Safety Commission decided to set mandatory minimum safety standards for children’s markers, it simply re-issued the voluntary, consensus standard already adopted by industry as a mandatory regulation.\textsuperscript{120} The National Technology Transfer and Advancement Act of 1995 directs U.S. government agencies to use standards developed by voluntary consensus bodies whenever available in lieu of government-developed standards to accomplish its regulatory and administrative objectives. For example, the U.S. Food and Drug Administration has a program that permits private-sector parties to request “safe harbor” status for voluntary private regulations, permitting them to be cited in applications for pre-market approval for medical devices in lieu of government standards.\textsuperscript{121}

The situation in most European countries, by contrast, is much simpler because most national technical standards are set by a national standards body that works closely with government economic planning departments, as well as with the European

\textsuperscript{119}See, e.g., Veeck v. S. Bldg. Codes Cong. Int’l, 293 F.3d 791 (5th Cir. 2002).

\textsuperscript{120}A private industry association, the Arts & Creative Materials Institute, began developing voluntary safety standards for the children’s art market in the 1940s; one of their standards was later taken up by the D01.57 Subcommittee of the D01 Technical Committee of the American Society for Testing and Materials (an ANSI accredited SDO) and issued as ASTM D-4236 in 1983, before being adopted by the U.S. Consumer Product Safety Commission under the 1988 Labeling of Hazardous Art Materials Act as a mandatory safety regulation for markers in the U.S. market and codified at 16 C.F.R. § 1500.14(b) (2012).

\textsuperscript{121}The U.S. Food and Drug Administration maintains a database of all voluntary, consensus standards that it has designated as equivalent to government standards; private parties are free to reference them in market approval applications but are not required to do so. \textit{Guidance for Industry and FDA Staff – Recognition and Use of Consensus Standards}, FED. TRADE COMM’N (Sept. 17, 2007). http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077274.htm.
standards organizations: CEN, CENELEC and ETSI. At the European Union level, a very successful co-regulatory framework known as the “New Approach” to standardization was developed in the 1980s to promote the Internal Market by reducing technical barriers to trade among member states. The New Approach was devised to end the gridlock that had characterized efforts to harmonize technical standards in the Internal Market in the 1970s. That old approach favored mandatory harmonization to a single standard, maximizing the problems of transition from many existing national standards to a single new European standard, thus fueling opposition from almost all stakeholders every step of the way. The New Approach required one of the European standards bodies to develop a standard that created a voluntary “safe harbor” for products that were certified compliant with it, permitting any producer who wanted to continue using national standards without the presumption of compliance to do so. The scope of the reference standard also only covered “essential requirements.” Each New Approach standard was developed to support a Directive, and the link between the technical standard and the legislation was established by publishing notices in the Official Journal rather than re-issuing the technical standard itself as legislation. The result was a loose coupling of traditional legislative processes with voluntary, consensus technical standard-setting processes that made it easier to accommodate technological innovation and also reduced statutory obsolescence caused by mandatory regulations based on standards that had become outdated.

The economies in countries where mobile money as a financial inclusion strategy is likely to have the most impact in terms of economic development are predominantly rural and agricultural so links between the state and modern technical standard-setting

institutions will normally be weak or simply non-existent. Some developing countries have developed an interface between government and technical standard-developing institutions, however, and in those countries, there is some evidence that the familiar LME versus CME distinction can be observed. In the case of M-Pesa, Kenya (a developing LME) pursued a more flexible, ad hoc market-oriented approach. 125 By contrast, in India (a developing CME) the central government has set a national open standards strategy in addition to financial inclusion and financial integrity strategies, and is working on a national mobile payment interoperability standard as part of its strategy of modernizing its payment systems generally.

More recently, another “co-regulatory” framework emerged in the European Union within which technical standards and legislation are even more loosely coupled. 126 The “Single Euro Payment Area” (SEPA) is the name applied to a public-private initiative in Europe to make the market for cross-border Euro transfers more efficient. When the Euro was launched in 1999, the bank clearing and settlement systems of different Eurozone member states were not interoperable because each country relied on separate legacy computer systems. Before the launch of the Euro, the banks had used the lack of technical interoperability as a justification to charge high fees for cross-border electronic funds transfers (EFTs). After the launch of the Euro, the Commission tried unsuccessfully to persuade the banks to lower their cross-border fees for Euro transfers. The banks resisted because merely adopting a new currency would not suddenly make their computer systems interoperable, so their actual costs for processing cross-border Euro transfers remained high. The Commission responded by issuing Regulation 2560/2001 prohibiting banks in the Eurozone from charging higher fees for cross-border Euro EFTs than for domestic Euro EFTs. 127 As a result, because domestic EFT

125 Buku & Meredith, supra note 6.
fees were generally very low, or in some countries had even been set at zero to encourage customers to stop paying by check, banks in the Eurozone began losing money on all cross-border Euro transfers.

In 2002, the major Eurozone banks responded by forming the European Payment Council, an industry trade association and standard-setting organization. Its membership structure is similar to that of an ICT consortium: membership is voluntary, but restricted to banks and European banking industry associations.\(^{128}\) The EPC’s mission is to promote and support SEPA,\(^ {129}\) and so it maintains a close dialogue not only with its member banks, but also with EU regulators. To solve the cross-border interoperability problem, the EPC develops “schemes” that combine technical engineering specifications with harmonized business processes.\(^ {130}\)

The SEPA Credit Transfer and Direct Debit schemes include ICT interoperability standards within the ISO 20022 framework as well as business process rules. In addition, EU banks are required to provide their customers with bank account numbers in the “International Bank Account Number” format for use with cross-border Euro transfers.\(^ {131}\)

The EPC originally set up informal “councils” to solicit input from non-bank stakeholder groups such as end users, but they produced mixed results. While the SEPA Credit Transfer scheme

---


\(^{129}\) Id. at § 2.


proved to be relatively uncontroversial, harmonizing business practices for direct debits from customer accounts proved to be very controversial. Users who felt excluded from EPC processes for drafting schemes and dissatisfied with the design of the SEPA direct debit scheme complained to the Commission that the EPC was not open and transparent. In 2009, the Commission summarized the governance challenges facing the EPC in the following terms:

The EPC has made progress in balancing the interests of different stakeholders, but it must operate in a more open manner to avoid possible foreclosure effects and take into account the interests of all stakeholders, including non-banking stakeholders, payment institutions and users. Greater transparency, adequate time for consultation and early involvement of all stakeholders, in particular users, in the planning and design of future initiatives need to be ensured.

The SEPA Council was launched in 2010 with the mandate of promoting the implementation of the SEPA system and also ensuring accountability and transparency in SEPA governance process. It meets twice a year, and is co-chaired by representatives of the European Commission and European Central Bank. The SEPA Council members include five representatives from the user side of the market (consumers, retailers, businesses, and national authorities); five representatives from the supplier side (European Payments Council, cooperative banks, savings banks, commercial banks, and payment institutions); and four national central bank board members (representing the Eurosystem). The EPC now engages in extensive consultation with external stakeholder groups

---


before finalizing or amending schemes.135

At the same time that the Commission and external stakeholders were growing frustrated with the EPC’s governance system, the EPC was growing frustrated with the Commission’s reluctance to support the work of the EPC with the full weight of EU legislation. The original vision for SEPA was that use of legacy national EFT systems would end and that all Euro transfers, domestic or cross-border, would be based on EPC standards; but without any statutory mandate, domestic Euro transfers were not being converted to the new formats. For example, the SEPA Credit Transfer Scheme was launched in 2007 with great fanfare, but by 2011, only 22.6 percent of all Euro transfers were made using it.136 Recognizing that progress in building SEPA had stalled, the EU Council and Parliament declared the need for a legislated “SEPA end date” to accelerate the migration process.137 The Commission responded, however, with a proposal to open up to competition the process of setting SEPA standards, without a firm commitment to an end date.138 Although the Commission tried to characterize the

---

135 See, e.g., Javier Santamaría, EPC Plenary Meeting Update, EPC NEWSL. (Eur. Payments Council), July 2012, at 47, available at http://www.europeanpaymentscouncil.eu/pdf/EPC_Newsletter_300712_15.pdf (At the EPC Member Plenary Meeting in June 2012, “It was decided that prior to continuing work to finalise the new optional SDD Fixed Amount Scheme, the following bodies would be consulted: the Payment Systems End User Committee (EUC) – in particular the BEUC (Bureau Européen des Unions de Consommateurs), the European Consumer’s Organisation – and the SEPA Council chaired by the European Commission (the Commission) and the European Central Bank (ECB) to ensure that the work is supported by the end users as well as the ECB and the Commission.”).


138 Internal Market and Services DG, Working Paper on SEPA Migration End-Date EUR. COMM’N (June 2, 2010), http://ec.europa.eu/internal_market/payments/docs/sepa/end-date_migration_en.pdf. (If Commission remains “neutral” with regard to specific standards, and only mandates “essential
development of EPC standards as a “market-driven” process that should be subject to competition, EPC members understood that SEPA schemes were public goods constructed by private enterprises at their own expense in furtherance of the Commission’s goal of building the Internal Market:

SEPA was not started as a demand-driven process, but as a policy-maker-driven EU integration initiative. The political SEPA vision aims to generate macro-economic benefits, strengthen the euro currency, drive forward the integration of the internal market and accelerate technological innovation in payments and beyond. In other words, SEPA is supposed to promote the public interest of European citizens at large. The current [low] rate of SEPA market uptake therefore, is perfectly in line with the progress of any other major EU integration initiative promoting a good that is not assumed to produce immediate benefits, requires initial investment to be realised and lacks clear regulatory direction. The European Commission itself recognises that full migration to SEPA would take some thirty years if projected based on market uptake to date. Consequently, the majority of stakeholders recognise that deadlines for SEPA migration must be set through EU legislation.139

The low voluntary adoption rates for SEPA schemes clearly demonstrated that the SEPA project was not market-driven, and without decisive intervention by a regulator, it would simply fail to achieve its original goals. In 2012, the Commission issued the SEPA End-Date Regulation, setting February 1, 2014 as the deadline for phasing out the use of old national Euro transfer requirements” for SEPA migration, then it might be possible for a new SEPA standard setting process to be organized to compete with EPC).

schemes and full migration to the new EPC SEPA Credit Transfer and Direct Debit Schemes.\textsuperscript{140}

Between market pressure for reform created by the original Regulation 2560/2001 and a statutory end-date established in 2012, together with the creation of the SEPA Council, the EPC and the Commission ended up in something close to the “New Approach” co-regulatory framework. The process looked more like LME informality than CME organization, however. With regard to the possibility of combining harmonized AML/CFT compliance business processes with ICT technical interoperability standards into something like “schemes” for a global mobile remittance network, the SEPA experience suggests that some degree of coercion by a central regulator would be necessary, and that the process of building and fine-tuning the “interface” between political institutions, markets and SDOs would be complex.

A global mobile remittance network will require some kind of co-regulatory interface, and the competition has already begun among developed and developing countries with both LME and CME orientations to take a leadership role in building that interface. Developed and developing countries that already have standards strategies in place are most likely to emerge as leaders in that process, while developing countries without national standards strategies will be unable to contribute much without a great deal of technical assistance. From the perspective of legitimacy, however, regulators and consumers in less developed countries may be essential stakeholders even though they currently lack the capacity to participate actively or directly in the creation of governance institutions. The inability of billions of global mobile remittance network stakeholders in developing countries to participate in the early stages of standard setting should give rise to concern about possible “foreclosure effects.”

What would a co-regulatory framework that promotes dialogue between FATF and private ICT SDOs, and minimizes the risk of foreclosure effects for the least developed countries look like? It might include some of the following elements:

Representatives of each standard-setting organization might be sent to observe each other’s meetings.

Technical assistance might be provided to representatives of less developed countries to permit them to participate as observers in private ICT SDO activities relevant to global mobile remittance standards.

A procedure might be established to determine whether private standard-setting organizations developing global mobile remittance standards relevant to AML/CTF compliance processes meet the due process requirements set out in the Code of Good Practice in Annex 3 to the WTO Technical Barriers to Trade Agreement.

Recognition of effective use of ICT standards to enhance compliance might be highlighted in FATF Mutual Evaluation Reports, building up a kind of precedent system.141

The FATF might issue guidance establishing a presumption of compliance with regard to specific issues when compliance with certain “schemes” (incorporating both business practice and ICT standards) has been certified by an accredited independent third party.

CONCLUSION

Mobile money offers much greater promise than almost any other development strategy to emerge since the modern study of development began after World War II.142 An operational global mobile remittance network would have an impact on the payment systems in any country that is either a source of poor economic

---

141 The U.S. Federal Trade Commission has created an informal system of precedent in the area of information security law through settlement agreements with companies it claims have engaged in unfair and deceptive trade practices as a result of bad security practices. JANE K. WINN & BENJAMIN WRIGHT, THE LAW OF ELECTRONIC COMMERCE §§ 14.03[O][1], 17.06[E] (2001 & Supp. 2012).

142 On the post-World War II origins of the modern study of development, see generally GERALD M. MEIER & DUDLEY SEERS, PIONEERS IN DEVELOPMENT (1984).
migrants or a target destination for them. No such network exists today, but, spearheaded by Visa and the GSM Association, a technical standards architecture for one is already emerging. The development of such a global architecture could promote financial inclusion without regard to national boundaries. The challenges facing EU regulators in creating a “Single Euro Payment Area” illustrate clearly the problems that might arise if developing countries each build their own mobile money systems and, only after they are complete, attempt to make them interoperable.

A global mobile remittance architecture might also provide an opportunity to integrate financial integrity functions into the operation of the network. If developing country regulatory requirements could be addressed in the same ICT standards that constitute the network, then the real cost to developing countries of AML/CFT compliance might fall with the growth of global mobile money networks. In such a case, expansion of the network would simultaneously enhance both financial inclusion and financial integrity goals. The challenges facing the card networks trying to increase security at the retail point-of-sale with the Payment Card Industry Data Security Standard illustrate clearly the risks of trying to “bolt on” compliance functions rather than “baking them in” from the beginning.

In recent decades, regulatory competition in many global ICT markets has been intense as countries try to push the development of technical standards in a direction that is compatible with their existing institutions. So it should not be surprising if regulatory competition emerges to set standards for a global mobile remittance market. The standard-setting activities that are already underway are within the “liberal market economy” tradition, and without external pressure from national regulators or international regulators with market clout, are unlikely to internalize any costs of AML/CTF compliance. They are also more likely to be dominated by private parties and to rely on proprietary technologies. By contrast, “coordinated market economy” regulators are more likely to embrace open standards. They are also more likely adopt policies like “privacy by design” that require private parties to internalize significant social regulation costs in the development of products and standards. If developed and developing CME countries supported an “integrity by design”
approach in standard setting, then AML/CTF compliance costs in developing countries pursuing mobile money financial inclusion strategies might fall.

A common reason that technical standard-setting efforts fail, however, is that the problems the standard-setting process tried to address were “over-constrained” or became too political.\textsuperscript{143} Within the LME approach to ICT standard setting, it is often possible to keep a tight focus on meeting market demand as quickly and effectively as possible. Because financial integrity is a regulatory obligation imposed on financial service providers, it is unlikely that financial integrity functions would be incorporated into LME market-driven standards in the absence of a clear regulatory mandate. The FATF, as the focal institution for global AML/CTF regulations, does not yet appear to have focused on ICT standards as a mechanism for reducing compliance burdens, let alone to have considered issuing such a mandate. Should it choose to focus on ICT schemes that combine technical interoperability standards and harmonized business process standards as a policy mechanism, then ICT governance issues would immediately surface. At that point, careful analysis of some of the co-regulatory mechanisms already in use in the United States and European Union might help frame governance issues related to regulatory effectiveness and legitimacy for global mobile money networks.

\begin{footnotesize}
\begin{footnote}
\textsuperscript{143} The IETF addresses both problems simultaneously with its “rough consensus and running code” standard. If rough consensus is not possible, i.e., the problem is too political, it is not undertaken. If there is not more than one successful implementation of the standard, i.e., running code, then the standard is not issued. More political organizations such as ISO and the ITU do not have the luxury of simply refusing to work on projects or failing to complete them. As a result, their portfolios are replete with standards with no known adoptions.
\end{footnote}
\end{footnotesize}
PRIVACY AND SECURITY CONCERNS ASSOCIATED WITH MOBILE MONEY APPLICATIONS IN AFRICA

Andrew Harris, Seymour Goodman, and Patrick Traynor*
© Andrew Harris, Seymour Goodman, and Patrick Traynor

Cite as: 8 WASH. J.L. TECH. & ARTS 245 (2013)
http://digital.law.washington.edu/dspace-law/handle/1773.1/1198

ABSTRACT

The rapid adoption of mobile money use in Africa raises concerns regarding the privacy and security of users, particularly in light of Financial Action Task Force recommendations requiring user transparency and the collection of transaction data. The transparency required of the now-financially-included—particularly in nations with weak adherence to the rule of law and limited privacy protections—leaves users vulnerable to abuse. Further, the increasing complexity of mobile phone use that is indicative of mobile money applications raises concerns regarding Africa’s preparedness for heightened security threats that come hand in hand with increased use. To address these problems, the authors of this Article recommend specific policy actions by African nations to improve consumer privacy and cybersecurity, supported by policies of

* Andrew Harris is a Foreign Affairs Officer at the U.S. Department of State. The views expressed in this paper are his own, and do not necessarily reflect those of the U.S. Department of State or the U.S. Government.
Seymour Goodman is a Professor in the Sam Nunn School of International Affairs and the College of Computing at the Georgia Institute of Technology.
Patrick Traynor is an Assistant Professor in the College of Computing at the Georgia Institute of Technology.
This Article was presented at the Mobile Money in Developing Countries: Financial Inclusion and Financial Integrity Conference held in April 2012 at the University of Washington School of Law with the support of the Linden Rhoads Dean’s Innovation Fund.
industrialized nations like the United States and responsible corporate behavior.

TABLE OF CONTENTS

Introduction ..................................................................................246
I. Privacy Concerns: Transparent Use Without Privacy
   Protection ..................................................................................248
   A. Limited Privacy Protections .............................................248
   B. Potential for Abuse ...........................................................249
II. Security ..................................................................................252
   A. Cybersecurity Limitations ................................................253
   B. Examples of Specific Mobile Money Threats ..................255
III. What Should be Done? ..........................................................257
   A. African Solutions .............................................................257
   B. United States Policy .........................................................260
   C. Public Advocacy and Corporate Responsibility ..............262
Conclusion ...................................................................................263

INTRODUCTION

Over the last decade, mobile telephony has enjoyed phenomenal adoption rates across most of Africa. Since 2005, there has been a five-fold increase in the number of African mobile phone subscriptions resulting in 53.1 mobile phone subscriptions per 100 inhabitants in 2011. While other areas of the world have adopted mobile phones to an even greater degree, the relative impact in Africa, where fixed telephone lines are available to less than 2 percent of the population, is perhaps greater than anywhere else. As the primary means of communication for most Africans, mobile phones have become a source of significant economic growth and a platform for innovation. One of the most dynamic of these innovations has been mobile money, the use of mobile phones to purchase goods or services through funds connected to the user’s account. With a broad base of mobile phone users

---

already in place, the widespread adoption of mobile money could have enormous positive impacts across Africa. On a continent with too few banking options necessary for a dynamic and modern economy, mobile money has the potential to address long-existing gaps in African economies.\(^2\) Unfortunately, the rapid growth of mobile telephony in Africa has not been accompanied by appropriate consideration for privacy and security concerns, opening the door for abuse and erosion of the application’s utility.

In light of limited privacy protections and a vulnerable cyber environment, the requirements of the Financial Action Task Force (FATF) raise a number of concerns associated with mobile money in Africa. As a financial service, the FATF Recommendations apply to mobile money just as with traditional banking services. The global effort to combat money laundering and terrorism is as applicable to mobile money services as to traditional banking. From a general security perspective, the identification, verification, and reporting requirements of the FATF Recommendations are a positive effort to ensure that mobile money applications do not become tools for money laundering. The requirements for user transparency, however, introduce a potential problem. FATF Recommendation 10 states that financial institutions must perform Customer Due Diligence, which includes confirming the identity of clients and scrutinizing client transactions.\(^3\) Further, Recommendation 11 requires financial institutions to maintain records of all transactions for five years, “to enable them to comply swiftly with information requests from the competent authorities.”\(^4\) These requirements for transparency and record keeping pose a number of user privacy concerns for mobile money applications in Africa, particularly in those nations with weak adherence to the


\(^4\) Id. at 15.
rule of law and limited privacy protections. Further, the increasing complexity of mobile phone use that is indicative of mobile money applications raises concerns regarding Africa’s preparedness for heightened security threats that come hand in hand with increased use.

I. PRIVACY CONCERNS: TRANSPARENT USE WITHOUT PRIVACY PROTECTION

According to FATF Recommendations 10 and 11, financial institutions should not allow customers to conduct business anonymously; and they must maintain user transaction records for five years. In most traditional banking settings, this requirement is both sensible and non-controversial. It does, however, raise significant questions for African users of mobile money services, particularly considering the limitations of privacy protections in Africa. For instance, a recent UN report noted that amongst the members of the East African Community—Burundi, Kenya, Rwanda, Tanzania, and Uganda—there is no legislation “that clearly defines who can get access to a mobile money trail, and how, when or under what conditions such access may be obtained.” Inadequate privacy protections can lead to abuse by governments and data brokers as well as leave personal information susceptible to theft or leakage, ultimately damaging user trust and limiting adoption and use.

A. Limited Privacy Protections

There are a number of reasons to explain the limits of privacy protection in Africa. First, a strong communitarian strain exists throughout much of Africa. This mindset de-emphasizes the rights of individuals in favor of those of community. In such a context, the privacy of individuals is given little consideration. Second,
traditional economies with limited electronic communication and commerce have less need for individual privacy protection as there are few means to collect, use, and exploit sensitive information. Until very recently, the vast majority of Africans did not engage in data compiling transactions. For both of the reasons above, there are few established legal protections in African nations. Most nations do not formally recognize a right to personal privacy, and most do not have laws or regulators in place to monitor abuse. Compounding the lack of legal protections is the relative absence of public interest groups to monitor government behavior, propose public policy, and promote awareness. This all leads to situations where serious abuses can occur with little impediment. Even in South Africa, where some legal protections are in place, illegal interception and abuse of electronic communications by intelligence agencies is routine. While a limited privacy protection regime may have caused little concern just a short time ago, the African boom in mobile telephony significantly heightens the risk to consumers operating in an ecosystem without protection.

B. Potential for Abuse

In the context of limited privacy protections and because FATF requires identity verification and data collection, African mobile money users may find their privacy threatened by governmental and corporate abuse. In cash-based economies, the spending and savings activities of individuals are known to an interested third party only with great effort. This is the environment that most Africans have come to understand, developing social behaviors reflective of spending that is anonymous to government and corporate entities. Despite a lack of privacy protections, the

---


inherent anonymity of cash prevents any other entity from knowing the extent of an individual’s transactions. Due to FATF requirements, however, the service provider can and must record every detail of a user’s transactions in a mobile money environment. It is also important to note that the initial wave of mobile phone adoption was anonymous, as the vast majority of users purchased and used unregistered pre-paid phones. Many African nations are now reversing this initial trend by requiring SIM-card registration, further reducing anonymity and potentially limiting private use. The availability of transaction data opens the door for abuse by an unscrupulous government, which could gain access to transaction records with little effort. This information could then be used in a number of ways to harass, intimidate, or manipulate the violated citizen.

Corporate abuse of personal information can have similarly insidious effects in a mobile money environment without legal safeguards. Mobile money services necessarily operate in a data-rich environment that creates incentives for the commoditization of personal information and targeted advertising. A fully employed mobile money ecosystem can include a mobile network operator, financial institution, trusted service manager, marketer, retailer, and the customer. Each of these entities (other than the customer) has a growing interest in collecting personal information tied to mobile money transactions. With so many interested parties and little consumer protection, the opportunities for data leakage and subsequent abuse are abundant. Liberal collecting and sharing policies result in electronic dossiers useful not only for providing targeted advertising, but also for making decisions regarding

---


11 See Andrew Harris et al., Emerging Privacy and Security Concerns for Digital Wallet Deployment, in PRIVACY IN AMERICA: INTERDISCIPLINARY PERSPECTIVES 185 (William Aspray & Philip Doty eds., 2011).
employment or credit worthiness as well as for committing fraud.

It is important to note that the threats of data leakage are amplified in a mobile money environment because how we spend is a valuable predictor of who we are and how we will spend or possibly otherwise behave in the future. Since FATF requires financial institutions to record user transactions, this information is necessarily compiled and available for use. The ability to connect basic personal information to spending records obtained through mobile phones has great commercial use—and potentially misuse. In places where mobile money is not yet extensively used, like North America and Europe, a spending record connected to the user’s mobile phone is less accessible or not available at all, so nations in these regions have not yet needed to wrestle fully with the implications of mobile money data. But in Africa, mobile money data sets are quickly growing. As Africans also begin to use their phones to access the Internet, the incentives to commoditize this data will grow and present challenges yet unseen in Western nations.

The potential for abuse of private information can harm not only the violated citizens, but also the overall economy. If governments and businesses abuse users’ trust, they will restrain adoption and limit the utility of mobile money, thus limiting the application’s utility and holding back their countries. Two of the authors witnessed a good illustration of this at a cybersecurity conference for East African government officials in Kenya.12 During a discussion of African broadband adoption, a law enforcement official from one of the participating countries stood up to proclaim the virtues of Facebook for monitoring and catching criminals. Such behavior can have a chilling effect on technology adoption, and the brazenness of the statement in a room full of government lawyers and officials demonstrates the lack of regard for privacy that some in government demonstrate. Calls to monitor social media are certainly not confined to Africa, but when proposed in industrialized nations, monitoring is suggested only within tight restrictions and a devotion to the rule of law.13 In most

---

13 See Sir David Omand et al., # Intelligence (2012), available at
African nations, there is little to stop governments or corporations from pushing the boundaries of acceptable use with regards to revealing mobile money data. If widespread abuse becomes commonplace, users may walk away from mobile money and all its enormous benefits.

II. SECURITY

The growth of mobile money is indicative of a larger trend of greater and more sophisticated mobile telephony use—a trend that many African nations are ill prepared for, for a host of reasons. As user experiences grow richer and smart phone adoption increases—a trend well underway—mobile phones will become a more appealing target to a wide range of cyber threats. The FATF requirements contribute to this trend by requiring user identification and transaction recording, meaning that mobile phones become directly linked to financial accounts and rich data sets, increasing the desirability for hackers. Smart phones are just as susceptible—if not more so—to the same viruses, worms, and botnets that plague PCs. In this environment, the user might lose more than just personal information, but notably money, and be susceptible to other forms of crime through exposure via his mobile device. The FATF requirements are generally beneficial for security issues considering their focus on the serious threats associated with terrorism, money laundering, and weapons proliferation. Further, FATF may generate constructive pressure by forcing regulators to more deeply consider the range of risks associated with mobile money. The extent of African cybersecurity deficiencies is significant enough, however, that FATF requirements alone—which do not address cybersecurity—are unlikely to compel improvements. Without proper attention to


security on the devices that enable mobile money, the user may be vulnerable to criminal activity.

A. Cybersecurity Limitations

This vulnerability is particularly pronounced in the African context due to a set of unique challenges that amplify the growing insecurity threat. First, most African nations have inadequate laws and institutions to confront serious cyber threats. While various efforts are underway to encourage the adoption of national legal frameworks, even these steps have limited effects without institutions in place to monitor networks and remediate threats. Computer Emergency Response Teams (CERTs) have become valuable assets for performing these necessary functions, but they are either lacking or in nascent stages across much of Africa. Beyond the institutional and legal inadequacy, African nations suffer from a shortage of trained public-sector professionals needed in both the policy and operational spaces. This is a common problem for all nations, but one that is exacerbated in Africa where the number of individuals with advanced information security knowledge is relatively lower than elsewhere. Those with such knowledge tend to be drawn to the higher paying private sector, leaving little expertise for governments. Without capable CERTs in place with the commensurate technical expertise to operate them, African networks are more vulnerable to cyber threats, leaving mobile money users vulnerable to attack and fraud.

Awareness is another crucial piece of the security equation. The rapid adoption of mobile phones and applications like mobile money has placed these useful tools in the hands of users with little prior experience with technology. Users with limited digital literacy are more likely to be unaware of cyber threats, placing

---

themselves and the networks at greater risk.\textsuperscript{17} Lack of cyber awareness is certainly a leading cause of infection across the globe, but African nations have a higher proportion of low-capacity users, and thus more users unfamiliar with the best practices that can limit vulnerability.\textsuperscript{18} Awareness issues extend beyond the average user into the corporate setting as well. Because most African companies have evolved in an environment of limited interconnectivity, they have had little reason to focus on cybersecurity measures and best practices. But now that broadband connectivity is growing, it is essential that measures such as software standardization and network monitoring be implemented. With lax operating procedures in place, corporate behavior can open threat vectors, infecting networks and endangering users. It is important to remember that a user of a mobile money application connected to an infected network is far more vulnerable than a user engaging in basic web browsing and email. It is therefore essential that heavy network users such as corporations are actively protecting the network.

Because the Internet knows few political boundaries, international cooperation on cybersecurity issues is a necessity, but few African nations are engaged in cross border law enforcement efforts. Only South Africa and Senegal have joined the Council of Europe’s Convention on Cybercrime, the most significant international law enforcement effort to address cybercrime.\textsuperscript{19} Further, there are limitations to the assistance developed nations are able and willing to provide. First, it is uncommon for developed nations to devote significant resources to cyber assistance. Most assistance funds are directed at more traditional development projects such as health or education. Second, details

\begin{itemize}
  \item \textsuperscript{17} See Steven Furnell et al., \textit{Security Beliefs and Barriers for Novice Internet Users}, 27 \textit{Computers & Security} 235 (2008).
  \item \textsuperscript{19} See the Council of Europe Convention on Cybercrime, available at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG.
\end{itemize}
of cybersecurity efforts and methodologies are often considered classified or restricted information in western nations. These nations are reluctant or completely unable to cooperate with nations they regard as having lax information security standards. All too often this is the case in the African context, making western governments unlikely to meaningfully share information and cooperate with African states.

Finally, the state of cybersecurity in Africa is hindered by the low prioritization from national leaders. This is of course understandable in the African context where limited resources must first be allocated to address society’s most fundamental problems. The low priority for cybersecurity in the face of other pressing issues means that solutions requiring strong governmental direction are absent from most African states, further endangering vulnerable networks and their applications. For this reason, and for the reasons described above, the African continent is likely the least safe place to operate a sensitive application like mobile money. Further, as mobile money grows more popular, it will inevitably become a greater target for criminal activity. If Africa’s cybersecurity deficiencies are not addressed in a timely manner, the widespread adoption of mobile money may be accompanied by widespread mobile money abuse.

B. Examples of Specific Mobile Money Threats

Without proper attention to basic security features, mobile money users introduce themselves to numerous threats, the most damaging being the loss of money should an assailant gain physical control of the mobile device. Given that nearly 5 percent of smartphones issued to or used by employees are lost annually and that only 30 percent of users protect their devices with passwords and data encryption, the possibility of someone other

---

than a device’s owner using it to gain access to mobile money is significant. It should also be noted that such mechanisms only offer protection against unsophisticated attackers. In particular, prior work has demonstrated that a technically adept adversary may be able to take advantage of poor security design within mobile money apps\textsuperscript{22} or simply bypass poorly implemented encryption.\textsuperscript{23} Accordingly, it is critical that both users and financial institutions consider a range of risk models.

More subtle digital attacks against users are also possible. For instance, mobile money applications could also be used to isolate or burden a potential target. Malicious applications within the phones themselves could easily target unsuspecting users. For instance, a “trojaned” application could simply fail to allow transactions from a target’s phone to clear, dramatically limiting the target’s ability to make purchases or move funds. Alternatively, the application could illegally track all the purchases made by the target, potentially giving the adversary information about the target’s strategies and physical location. Finally, such an application could make arbitrary purchases on behalf of the target. Given that the avenues to contest the legitimacy of such purchases are generally lacking (e.g., the presence of the correct PIN made with a purchase virtually ensures that liability is held by the target and not their financial institution), such an application could slowly drain funds from the target’s account. Performed in an inconspicuous fashion, such purchases would be unlikely to raise alarms in traditional fraud detection systems. With an increasingly appealing target for criminals and an environment of cyber insecurity, African mobile money uses face an uncertain future.


III. WHAT SHOULD BE DONE?

Mobile money has enormous potential for the people and economies of Africa, yet users must ultimately trust the technology if its greatest impact is to be realized. Lurking issues associated with personal privacy and cybersecurity currently threaten that user trust. Both are global problems requiring global solutions with cooperation from all stakeholders.

A. African Solutions

First and foremost, African nations must recognize the importance of digital technologies to the future of their economies. While perhaps one of the most dynamic and compelling, mobile money is just one of many technologies with the power to help transform African economies. With financial resources understandably limited, national leaders should take policy actions that will increase user trust without requiring exceptional monetary and other resource allocations.

Primary amongst these steps is instituting comprehensive but flexible privacy regimes. In reviewing the lack of privacy regulation in East Africa, the United Nations Conference on Trade and Development (UNCTAD) declares that “simple and transparent mechanisms are needed through which users can authorize an entity to access” data associated with mobile money.\(^{24}\) Individuals should be empowered through national legislation to control their personal information and corporations should be required to use that information only in contextually appropriate ways. Licensing for mobile money services should include explicit rules for the collection and sharing of personal information. Crucially, it is imperative that lawmakers implement comprehensive regulations rather than taking a sectoral approach, as has unfolded in the United States. Sector-specific laws may prove inadequate for converged technologies like mobile money, leaving banks, telecommunications companies, and data brokers

\(^{24}\) UNCTAD, *supra* note 5, at 20.
with differing requirements leading to inconsistent treatment of user data.\textsuperscript{25}

There have been some recent positive steps regarding privacy legislation in Africa. In February 2012, Ghana passed a comprehensive data protection bill establishing users’ rights of data access, control, and consent of use.\textsuperscript{26} The bill also creates a Data Protection Commission to enforce and regulate the new law.\textsuperscript{27} Further, a draft bill in Kenya specific to electronic retail requires user consent for any information sharing.\textsuperscript{28} Both are positive steps and serve as recognition from these two nations of the necessity to protect users and promote trust in order to maximize utility of new technologies like mobile money. Further these efforts may serve to encourage other African nations to explore privacy legislation. While protecting citizens should be a primary concern for policymakers, they must also seek balance in any law, working to ensure that new legislation is not overly prescriptive or burdensome for corporations bringing innovative tools to the marketplace. For instance, while many international businesses welcome the European’s new privacy plans to streamline privacy rules in a more centralized manner, these same companies also protest the regulation’s more stringent guidelines such as the proposal for an individual’s “right to be forgotten.”\textsuperscript{29} While the proper balance between adequate protection and flexible business operations is certainly delicate, African leaders must act in order to ensure the ultimate success of mobile money.

To address the lack of technical capacity, policy makers should stress the study of security, privacy, computer science and information programs in universities. There is a growing demand for African app developers, and universities will train many of

\textsuperscript{25}See Harris et al., \textit{supra} note 11.


\textsuperscript{27}Data Protection Act 843 of 2010 (Ghana), \textit{available at} http://www.parliament.gh/assets/file/Bills/Data%20Protection%20Act,%202010.pdf.

\textsuperscript{28}UNCTAD, \textit{supra} note 5, at 20.

them. These universities should insist on strong privacy and security backgrounds. These courses of study should be promoted as holding particular import for future development with incentives created to draw in prospective students. To help facilitate a greater emphasis on privacy and security at the university level, policymakers should encourage empowering partnerships with international institutions that excel in the field. For instance, the Rwandan government recently sponsored a Carnegie Mellon University campus in Kigali with the government committing to offer substantial scholarships to qualifying applicants. Carnegie Mellon’s Rwanda campus offers Masters of Science in Information Technology with the option to focus on cybersecurity and began classes in the fall of 2012. This action by the Rwandan government demonstrates a clear understanding from national leaders that technological advances must be accompanied with sufficient human capacity. Similar partnerships coupled with the promotion of security and privacy studies can help African nations make strides in addressing human capacity issues.

African application developers and service providers can of course begin to place a greater emphasis on personal privacy and security by designing solutions to protect networks and data and providing users tools to protect themselves and their devices. In considering the problems of transparency in mobile money applications in the African context, developers could explore some of the benefits of e-cash, a primarily conceptual digital currency in which transactions are anonymous and funds cannot be double spent. Bitcoin is the most prominent manifestation of e-cash, although numerous technical and regulatory problems exist with this particular implementation. With proper research, mobile money applications may find some of the principles and features of e-cash useful in introducing layers of anonymity and protection for users. Finally, African nations should commission public awareness campaigns focused on cybersecurity and personal data. With relatively little money, public awareness campaigns can

increase digital literacy, informing consumers of basic dos and don’ts to protect themselves and others.

B. United States Policy

Developed nations should pursue policy solutions as well. The safe and effective employment of mobile money across Africa is clearly in the interest of countries like the United States. Indeed, the United States has a number of applicable policies in place. Joining these policies with specific action to assist African nations can serve to address some of the potential problems. One of the most vocal proponents for a free and open Internet has been Secretary of State Hillary Clinton: “The United States will continue to promote an Internet where people’s rights are protected and that it is open to innovation, interoperable all over the world, secure enough to hold people’s trust, and reliable enough to support their work.” These words have provided leadership for the United States to increase diplomatic pressure on offending governments and raise the costs of bad behavior. Because of her initiative, American embassies are poised to monitor for and respond to governmental abuse of digital technologies like mobile money.

The forward leaning posture of Secretary Clinton should be matched with a clear policy on dual-use technology controls. The U.S. government needs to put careful thought into the export of technologies that can be used to block, monitor, or filter digital content as well as performing more benign and easily marketable tasks. Rebecca MacKinnon points out this fact and criticizes the U.S. government’s complicity: “American corporations are major suppliers of software and hardware used by all sorts of governments to carry out censorship and surveillance—and not just dictatorships.” Therefore, a policy is needed to sufficiently deter

---

33 Rebecca MacKinnon, Internet Freedom Starts at Home, FOREIGN POLICY (Apr. 3, 2012), http://www.foreignpolicy.com/articles/2012/04/03/The_Worlds_
repressive regimes from obtaining these tools and encouraging
democratic governments not to abuse the capabilities of dual use
technologies. While the United States has taken direct action in
some of the most extreme cases, such as President Obama’s
Executive Order banning the transfer of certain technologies to
Iran and Syria, uniform guidance and consistent enforcement
would offer more effective protection.

The United States can and should also make efforts to assist
African nations protecting individual privacy. The recently
released White House Blueprint on Consumer Privacy protection
identifies the needs for both consumer control of personal
information and for the free flow of international data: “The United
States is committed to engaging with its international partners to
increase interoperability in privacy laws by pursuing mutual
recognition, the development of codes of conduct through multi-
stakeholder processes, and enforcement cooperation.” If pursued
with African partners, this policy can help ensure that African
consumers are protected and African economies are equipped to
engage in the global digital marketplace.

Finally, the United States—and indeed other developed
countries—must begin to prioritize cybersecurity cooperation with
Africa. Appropriate high-level U.S. policies are in place, but
significant implementation of those policies is yet to occur. The
President’s International Strategy for Cyberspace commits the
United States to working with developing countries to build
cybersecurity capacity, develop and share best practices, offer
cybercrime training, and to develop and deepen governmental ties

---


with counterparts and subject matter experts. To adequately achieve these commitments, Congress must first acknowledge and address the global nature of cyber insecurity in Africa. Then, significant additional resources are needed to allow U.S. experts to provide technical assistance to partner nations. Finally, there is a need to reconcile conflicts between the value of information sharing and the necessity of ensuring the integrity of classified material. American action alone cannot address the potential problems facing Africa, but the United States has adopted promising policies in the last few years that can serve to guide both American and global action in providing needed assistance.

C. Public Advocacy and Corporate Responsibility

As new technologies proliferate, particularly in African settings with large populations of users less accustomed to these technologies, it is essential that public advocacy groups focus their attention on possible governmental or corporate abuse. Under the banner of Internet Freedom, human rights groups can monitor for abuse and apply international pressure to those most egregious abusers. Freedom House’s “Freedom of the Net” report is an excellent example of such an effort. By reporting broadly on the state of government Internet restrictions, Freedom House is providing an essential tool in helping to hold governments accountable. As African users adopt sophisticated and specific applications like mobile money, similar monitoring of governmental interference in these spaces should be established as well.

Corporate responsibility is another vital piece in ensuring user safety and privacy. Service providers and banks have a responsibility to protect users’ data and finances through technical means as well through appropriate behavior and policies that do not expose users to abuse at the hands of repressive governments or unscrupulous third parties. Beyond a moral issue, widespread

adoption of mobile money requires user trust. The necessity of trust should provide sufficient incentive for responsible corporate behavior. A positive example of companies proactively committing to responsible behavior is the Global Network Initiative (GNI), a multi-stakeholder group that includes Google, Microsoft, and Yahoo!. GNI attempts to assist technology companies in protecting privacy and free expression in the face of repressive regimes and can serve as a model for self-organized corporate commitment making. Where corporations are complicit in abuse, other institutions or legal mechanisms, as mentioned above, are appropriate.

CONCLUSION

There can be no doubt about the enormous potential for mobile money in Africa. For a continent plagued by limited banking options, mobile money has in just a short time brought millions to the ranks of financial inclusion. As part of the global effort to counter money laundering and terrorism, FATF requirements demand transparency of all financial services customers, including mobile money. The increased data collection associated with this transparency renders mobile money users in Africa particularly vulnerable to governmental or corporate abuse of the data generated by mobile transactions. Equally troubling are cybersecurity concerns, leaving African mobile money users in a doubly precarious position. Should mobile money platforms come to be inundated with privacy breaches and malware, users will lose trust in the application, reversing adoption trends and eliminating potential gains. It is therefore incumbent for all to act—government, human rights watchdogs, corporations, and individual citizens—to address existing deficiencies and ensure that the power of mobile money will be enjoyed across Africa.

---

THE ROLE OF UNCITRAL TEXTS IN PROMOTING A HARMONIZED LEGAL FRAMEWORK FOR CROSS-BORDER MOBILE PAYMENTS

Luca G. Castellani*
© Luca G. Castellani

Cite as: 8 WASH. J.L. TECH. & ARTS 265 (2013)
http://digital.law.washington.edu/dspace-law/handle/1773.1/1199

ABSTRACT

The establishment of a regulatory environment is a condition necessary, but not sufficient, for setting up a legal environment supportive of mobile payment and banking services. Equally important is the creation of an enabling legislative environment on the legal status of electronic communications and on other relevant rules such as those on payments. In fact, existing legal frameworks, be they of statutory or contractual origin, are often insufficient to address all legal issues, especially in developing countries. Therefore, guidance in the form of international standards, such as those prepared by the United Nations Commission on International Trade Law (UNCITRAL), is desirable. In particular, existing UNCITRAL texts on payments could be reviewed in order to align them with UNCITRAL texts on electronic commerce as well as current practices in the use of electronic communications. This work should take into consideration the needs of small and medium-sized...
enterprises, which are likely to particularly benefit from broader access to mobile services.

TABLE OF CONTENTS

Introduction ..................................................................................266
I.  UNCITRAL Texts on Electronic Transactions ....................269
II. The UNCITRAL Model Law on International Credit Transfer..........................................................................................272
III. The EU Payment Services Directive: Another Example of Supranational Legal Text Applicable to Mobile Payments..........................................................................................277
IV. The Current Status of Mobile Payments Legislation in Developing Countries: The Cases of Kenya and Tanzania..........................................................................................279
Conclusion ...................................................................................281

INTRODUCTION

Electronic communications have significantly and irreversibly changed the manner of conducting business. One of the early fields where electronic communications have found application is payments; indeed, large inter-bank payment systems have been at the forefront of the digital revolution. Access to those systems has been gradually extended to major clients, and eventually to the public at large. Today, the use of electronic means is so pervasive that it is simply impossible to think of renouncing it. Payment services represent the core of electronic banking.

The increasing mobility of electronic devices has created new opportunities. Mobile payments as well as mobile banking services are available.¹ Mobile payments, however, have not received equal attention or interest in all countries.

¹ For the purpose of this Article, the term “mobile payments” refers to payments where the payment order is sent and/or received using mobile devices, such as mobile telephones, and the term “mobile banking” refers to access to credit services via mobile devices. In general, however, the term “mobile banking” is often used to refer to all transactions with banks, and not necessarily only to those involving access to credit.
The possibility of having access to electronic services, including via mobile devices, depends on the information and communication technology (ICT) infrastructure. Mobile services need a network capable of supporting them in a reliable and secure manner. At the same time, in certain regions ICT infrastructures, including mobile networks, though not yet fully developed, are already more ubiquitous than the physical banking network. This explains the asymmetry in the offering of mobile payments. On the one hand, in some very ICT advanced countries, such as Japan and the Republic of Korea, mobile devices are commonly used for micropayments. In those cases, the broad availability of mobile networks allows for frequent transactions of small value. On the other hand, in many developing countries, especially in Africa, the reach of mobile networks, though more limited than in the previous case, is sufficient to permit the exchange of payment orders with simple technologies. Given the dearth of physical banks and other payment systems in these countries, mobile payments have become a fundamental element of conducting business, and a promising vehicle to promote financial inclusion.

The current status does not, of course, preclude future developments. In particular, if appealing services are developed or if mobile networks are further expanded, it is possible that the use of mobile devices for micropayments will also become prevalent in other countries. However, countries currently situated between the two groups mentioned above see mobile payments as a niche market, for instance, for remittances.

---

2 A definition of micropayments is necessarily elusive as the notion of “very small payments” may vary with purchasing power. These are transactions relating, for example, to a single ride on a public transportation system. PayPal, a leader in electronic payments, defines micropayments as transactions of value below US$12. Micropayments, PayPal, https://www.paypalobjects.com/IntegrationCenter/ic_micropayments.html. This definition is used for the purpose of fee charges.


4 For a brief description of the status of mobile payments in the United
Significant attention has already been given to the law applicable to mobile payments, especially given its possible contribution to financial inclusion. However, commentators tend to focus on the regulatory aspects of those payments: issues such as which entities may offer mobile payment services, and at what conditions. So-called enabling aspects—i.e., legislative provisions aimed at facilitating trade and, in this case, mobile payments—seem less discussed. Those provisions are found at the intersection of two separate fields of international trade law: the law of electronic transactions and the law of payment. The first set of rules deals with the technological aspects of mobile payments, while the second addresses issues arising from the transfer of money and, possibly, underlying transactions.

The United Nations Commission on International Trade Law (UNCITRAL, or the Commission) was established in 1966 by the United Nations General Assembly to further the progressive harmonization and unification of international trade law.\(^5\) In doing so, the Commission has prepared texts that have been enacted to regulate not only international but also domestic trade. The work of UNCITRAL is particularly interesting for mobile payments because the Commission has prepared texts both in the field of electronic communications (of which mobile communications are a subset) and in the field of (international) payments. Those texts will be discussed in order to ascertain the usefulness of their adoption to enable mobile payments. A short review of some relevant texts, including of a contractual nature, will follow in order to establish a benchmark and ascertain the need for future work. In conclusion, suggestions for establishing a modern enabling framework for mobile payments will be formulated.

---

I. UNCITRAL TEXTS ON ELECTRONIC TRANSACTIONS

UNCITRAL has dealt with the law of “electronic commerce” since the 1980s and has prepared uniform legislative texts that have been adopted in numerous jurisdictions. Not only are UNCITRAL texts widely considered as global standards, the fundamental principles underpinning them are universally accepted as the core elements of modern electronic commerce law. These principles include non-discrimination, functional equivalence, and technological neutrality. The principle of non-discrimination requires that electronic transactions shall not be discriminated against solely because of their nature; the principle of functional equivalence establishes that, when certain conditions are met, the legal value of electronic transactions shall be equivalent to that of other forms of communication, such as those in writing; the principle of technological neutrality mandates that the law shall not demand the use of any specific technology but shall accommodate all existing and future technologies by using generic terms.

Not surprisingly, in light of what was said above with respect to the early interaction between electronic communications and payments, in 1987 UNCITRAL had already prepared a Legal Guide on Electronic Funds Transfers. As a result, UNCITRAL has prepared three legislative texts applicable to both domestic and cross-border electronic transactions: the UNCITRAL Model Law on Electronic Commerce, the UNCITRAL Model Law on Electronic Signatures, and the United Nations Convention on the Use of Electronic Communications in International Contracts

---

The UNCITRAL texts on electronic communications provide a comprehensive set of rules. The definitions of “data message” and “electronic communication” contained therein encompass communications exchanged via mobile devices (“mobile communications”). Therefore, mobile communications normally fall under the scope of general legislation on electronic transactions enacting UNCITRAL model laws, and of the Electronic Communications Convention. This conclusion is supported also by case law.11

However, mobile communications sometimes pose special challenges and thus require additional specific provisions. These particular issues arose at a dedicated session of the UNCITRAL Colloquium on Electronic Commerce.12 The conclusion at that colloquium was that certain features of mobile communications could indeed pose peculiar difficulties, particularly in relation to: the ability to gain access to large documents, both in terms of readability and of cost of download; the ability to archive information on the user side, given the comparatively short average usage period of mobile devices, and their limited storage capability, especially for lower-end models prevalent in developing countries; and the ability to sign documents with advanced signature technologies, such as those based on public-key

---


11 Interestingly, such case law comes from South Africa, possibly the Sub-Saharan country with the most developed ICT infrastructure. The decisions are available in the CLOUT (Case Law on UNCITRAL Texts) system, managed by the UNCITRAL secretariat: Jafta v. Ezemvelo KZN Wildlife, CLOUT case no. 964, and Sihlali Mafka v. South African Broadcasting Corporation Ltd., CLOUT Case No. forthcoming. They can be accessed online at: http://www.uncitral.org/uncitral/en/case_law.html. See also Z. Ntozintle Jobodwana, E-Commerce and Mobile Commerce in South Africa: Regulatory Challenges, 4 J. INT’L COM. LAW & TECH. 287 (2009).

12 The colloquium was held in New York on February 14-16, 2011.
infrastructures, particularly in light of the simpler technology prevalent in developing countries.\textsuperscript{13}

Those discussions highlight interesting elements that deserve accurate consideration. However, appropriate solutions seem available for technological issues. Rather, the limited awareness of legislators and other stakeholders with respect to the applicable legislative framework seems to be the real challenge to the legal predictability of mobile communications, including mobile payments. Indeed, the very notion that mobile communications are a subset of electronic transactions is not yet fully consolidated. More generally, the need for an enabling environment seems underestimated by decision-makers, while their legislative efforts are concentrated on the regulatory side. In particular, a discussion on how to enable such exchanges across borders has yet to take place, despite existing regional economic integration.

For example, member states of the East African Community are adopting enabling legislation based on a regional model law inspired by UNCITRAL texts, thanks to a dedicated capacity building project managed by the East African Community and the United Nations Conference on Trade and Development (UNCTAD). Mobile payments are prevalent and used massively on a daily basis in East Africa. Thanks to the uniform model legislation, the adoption of the Electronic Communications Convention, the fundamental text to enable cross-border electronic transactions, would require very limited additional legislative work by East African states. However, none of those states has yet adopted the Convention. Similar considerations may be made with respect to Association of Southeast Asian Nations (ASEAN) member States.

II. THE UNCITRAL MODEL LAW ON INTERNATIONAL CREDIT TRANSFER

UNCITRAL adopted its Model Law on International Credit Transfer (MLICT)\(^4\) in 1992 in response to two major changes: the increasing use of electronic means in payment orders, and the shift from a prevalence of debit transfers to a prevalence of credit transfers.\(^5\) In this respect, it should be noted that credit transfers are considered simpler, less prone to error and fraud, and therefore better suited for electronic transposition than debit transfers.\(^6\) The MLICT is compatible with paper-based payment orders, but was actually designed with particular reference to “high speed electronic credit transfers.”\(^7\)

While mobile payments are more similar in structure to debit transfers than to credit transfers, the distinction between the two categories is being reduced.\(^8\) Hence, while the adaptation of rules in the MLICT to mobile payments could require keeping in mind the possible need to adapt them to a debit transfer environment, fundamental issues remain similar.

The MLICT was drafted with banks in mind as handlers of payment orders. The issue of the text’s applicability to non-banking institutions was raised with respect to European postal and telephone authorities.\(^9\) Moreover, concerns were expressed in regard to the possibility that purely transmitters of information, i.e., entities involved in the movement of funds only on a technical


\(\text{\textsuperscript{5}}\) A debit transfer is initiated by the beneficiary of the funds, while a credit transfer is initiated by the originator of the payment order.


\(\text{\textsuperscript{8}}\) Ronald Mann, Making Sense of Payments Policy in the Information Age, 93 GEO. L.J. 633, 652 (2005).

level such as message systems, would fall under the scope of the MLICT. As a result, Article 1(2) of the MLICT specifies that “this law applies to other entities that as an ordinary part of their business engage in executing payment orders in the same manner as it applies to banks.” Legislation based on the MLICT would therefore cover mobile payments effected through a mobile network operator.

The MLICT does not exclude payments to consumers from its scope of application, but, at the same time, does not deal with consumer protection, an issue that may give rise to challenges. In fact, small and medium-sized enterprises represent a significant share of the users of mobile payments in developing countries, while consumers are prevalent in the case of micropayments. Therefore, the need to choose between conflicting rules may arise if opposite goals are at stake.

However, it seems important to distinguish between provisions beneficial to all users in light of the technical features of the device used for the transaction, and provisions specifically aimed at consumer protection. An example of the former may be a rule akin to that contained in Article 14 of the Electronic Communications Convention, encouraging the implementation of mechanisms under which automated systems provide a summary of the information input by human beings, thus giving an opportunity to review and eliminate input errors before final submission. At the same time, provisions designed for consumer protection should be strictly technology neutral, and the imposition of special rules for mobile payments vis-à-vis paper-based, or even other electronic payment methods, would violate that fundamental principle. This approach is in line with the general recommendations made for electronic contracting.

With respect to the general architecture of the payment, it should be noted that the majority of mobile payments may currently take place under the simplest scheme: the mobile network operator transfers a sum from the account of the payer to the account of the payee, and both accounts are maintained with that operator. This scheme does not pose significant issues from the perspective of the payment, while it still calls for basic provisions relating to the use of electronic transactions. However, when the payment takes place in favor of a beneficiary holding an
account with another mobile network operator, in the same country or in another country, the role in the transaction of that second mobile network operator will also need to be taken into consideration. These are also cases that need to be enabled by the law, since they promote competition among mobile network operators, including across borders. The MLICT contains the rules necessary to enable such scenarios. In fact, while the MLICT only refers explicitly to international credit transfers, its provisions also apply to domestic transfers. The limitation to international transfers in the language used by the MLICT seems mostly due to the terms of references given to that Working Group by the Commission, and not to the content of the MLICT itself. The importance of the adoption of rules on the relation between mobile network operators (in the language of the MLICT, they would be referred to as “sending bank” and “receiving bank”) cannot be over-emphasized. Those rules will, in fact, determine when the payment takes place, in what currency, and other similar critical elements.

Under the MLICT, the payment “is completed when the beneficiary’s bank accepts a payment order for the benefit of the beneficiary.” This rule was chosen to place the risk that the payment could not be completed due to insolvency of the beneficiary’s bank on the beneficiary. This rule could be adequate for a market where several large professional operators compete in offering payment services, but the different nature of the clients of most mobile payments (consumers, or small and medium-sized enterprises) and the limited choice of mobile network operators, due to the oligopolistic nature of that market, might recommend a different choice. For instance, mobile payments could be considered completed when the sum is credited on the account of the beneficiary. It should be noted that this moment might have important consequences with respect to the time of performance of the underlying obligation, such as, for instance, the payment of the price for a good or service sold.

20 Different again would be the case where the beneficiary holds no account.
21 Bergsten, supra note 17, at 437-38.
22 MLICT, supra note 14, at 13 (art. 19(1)).
23 Bergsten, supra note 17, at 489.
validity of the payment and the validity of the underlying obligation should, however, remain distinct matters.

A rule particularly relevant for mobile payments relates to the so-called “money-back guarantee,” which imposes liability on the originator’s bank for return of the money if the payment is not completed as instructed.\(^{24}\) The rationale is that the originator has no say in the choice of the intermediary banks, which are chosen by the originator’s bank.\(^{25}\) In the case of money transfer via mobile network operators, that choice is limited by the location of the account of the beneficiary. It seems therefore useful to introduce a distinction between liability for technical failures, which could remain on the operator of the failing network, and liability for other reasons, which might need more detailed treatment. The liability of the payment service provider could be limited to avoid consequential damages.\(^{26}\)

In light of the needs of clients, a general duty to assist those clients, including a duty to send certain notices, may be imposed on the payment service provider. Such duties may not be excessive given the technology available. For instance, duties such as those imposed by Article 8(4) and Article 19(2) of the MLICT, relating to the bank notifying the sender (when identified) if the payment order contains insufficient data, may now be easily discharged in an automated manner. In that respect, it should be noted that the sender, under normal circumstances, opts to be reached for communications at the mobile telephone number used to initiate the payment. That telephone number, to which a Short Message Service (SMS) may be sent, is therefore a valid designated electronic address.

The provision contained in Article 5(2) of the MLICT is also of great interest. It sets forth that a payment order authenticated with a procedure other than mere comparison of signature binds the purported sender if “the authentication is in the circumstances a commercially reasonable method of security against unauthorized

\(^{24}\)MLICT, supra note 14, at 10 (art. 14).

\(^{25}\)Bergsten, supra note 17, at 463.

\(^{26}\)See the discussion on consequential damages and the MLICT in Bergsten, supra note 17, at 487-88.
payment orders" and the receiving bank has complied with the authentication.

The current prevailing global standard for banking operations calls for at least a double level of authentication. The “commercially reasonable method” standard for security procedures used for payments (also contained in U.C.C. § 4A-202) has recently been better explained, possibly by placing a heavier burden on banks that cannot be easily contracted out. However, mobile telephones already provide for multiple levels of authentication: physical possession of the mobile device is one authentication factor; the ability to turn it on by entering a personal identification number (PIN), when present as is often the case, is a second factor; and the submission of the payment order by entering a separate PIN is a third factor. At the same time, the common statutory choice to limit the liability for credit and debit cards (though to different extents) should not be overlooked as mobile payments may present significant similarities with those cases. Therefore, the policy issue on liability allocation in case the sender is not the person purported to be remains open. The prevailing use, and therefore the amounts in play, may be relevant in finding a solution: while strict liability on consumers may be harsh, stricter rules for professionals transferring higher amounts might be more appropriate.

Equally interesting is the fact that traditionally the risk for payment of an unauthorized order lies with the receiving bank. Here the Working Group made an assumption that the receiving bank could determine the authentication procedure. This cannot be the case with mobile network operators, where the operator equivalent to the “sending bank” determines the authentication procedure.

The MLICT does not allow for revocation of payment orders, except in cases where the receiving bank receives the revocation before the payment is executed (or the credit transfer is

---

29 Bergsten, supra note 17, at 443.
completed). Given the speed of electronic transactions, it is unlikely that this mechanism could find application in mobile payments. However, there might be cases where the payment must indeed be revoked, similar, for instance, to reasons for credit and debit card chargebacks.

III. The EU Payment Services Directive: Another Example of Supranational Legal Text Applicable to Mobile Payments

The European Union has dealt extensively with provisions relating to payments, in an effort to build an efficient Single European Payment Area (SEPA). The EU Payment Services Directive (PSD) seems to apply to mobile payments, including mobile remittances.

---

30 MLICT, supra note 14, at 9 (art. 12(1)-(2)).
Put simply, where a telecom operator makes a payment on behalf of a payment service user to a third party, the payment transaction will fall within the scope of the Directive when operator acts solely as an intermediary making the payment. On the other hand, payments relating to the purchase of digital services such as ring tones, music or digital newspapers which are sent to a mobile phone (or some other digital device e.g. a computer) are not normally covered by this Directive.

However, it should also be noted that Recital 6 of the Regulation 260/2012 of the European Parliament and of the Council of 14 March 2012 Establishing Technical and Business Requirements for Credit Transfers and Direct Debits in Euro and Amending Regulation (EC) No 924/2009, 2012 O.J. (L 94) 22, 23 (implementing the SEPA), indicates that:
Money remittance, internally processed payments, large-value payment transactions, payments between payment service providers (PSPs) for their own account and payments via mobile phone or any other means of telecommunication or
While the PSD has significant regulatory content, it also contains enabling rules. In particular, its Title IV sets the rights and obligations in relation to the provision and use of payment services, and Chapter 2 of that title deals with authorization of payment transactions. Among those topics treated both in the MLICT and the PSD, it should be noted that the PSD contains a rule on evidence on authentication and execution of payments,\textsuperscript{33} according to which the burden of proof is on the payment service provider. This could be particularly useful in light of the technical limits in archiving capacity of mobile telephone sets, especially those at the lower price range. The PSD also sets limits of €150 (or at the lower limit set by the Member State) on the payer’s liability for unauthorized payments occurring before the notification of the loss, theft or misappropriation of the payment instrument or of its unauthorized use.\textsuperscript{34} However, those limits do not apply in case of low-value payment instruments (and electronic money).\textsuperscript{35}

Chapter 3 of Title IV of the PSD deals with payment orders, providing rules for their receipt, refusal and for determining the amounts transferred and received. Payment orders are usually irrevocable, unless agreed otherwise, and with the exception of direct debit payments revoked at least the business day prior to the date agreed for the payment.\textsuperscript{36}

The same chapter also provides rules for the time of execution of the payment and the value date, as well as liability issues. With regard to the latter, as a general rule the payment service provider

\textsuperscript{33} PSD, \textit{supra} note 31, at 28 (art. 59).
\textsuperscript{34} \textit{Id.} at 28 (art. 61(1)).
\textsuperscript{35} \textit{Id.} at 26-27 (art. 53). These are payment instruments whose individual transactions may not exceed €30 and with a spending limit of €150.
\textsuperscript{36} \textit{Id.} at 30 (art. 66).
is liable for non-execution or defective execution of the payment order. A number of detailed duties are listed. Moreover, the payment service provider is not liable if the unique identifier of the beneficiary provided by the payer is incorrect. However, the payment service provider shall make reasonable efforts to recover the wrongly transferred funds. In mobile payments, the telephone number of the beneficiary may be used as a unique identifier. A similar rule might therefore be particularly useful.

In conclusion, the PSD is a rather complex text and contains a number of provisions directly relevant to mobile payments. Some of them overlap with those of the MLICT.

IV. THE CURRENT STATUS OF MOBILE PAYMENTS LEGISLATION IN DEVELOPING COUNTRIES: THE CASES OF KENYA AND TANZANIA

Before advocating new work in the field, possibly on the basis of the MLICT and of the PSD, it is advisable to verify actual needs of the potential recipients. Kenya and Tanzania, two developing countries with significant mobile payments markets, may provide useful information.

At the statutory level, Kenya has adopted electronic transactions legislation. However, this is not considered sufficient for the needs of all commercial operators, including the needs of mobile payments providers. In 2011, Kenya adopted the National Payment System Bill, which mostly contains regulatory content, but explicitly allows the use of electronic means when providing payment services in its Article 2, sub-definition of “payment service provider.”

Tanzania does not have an electronic transactions act or a national payment system act. Currently, the Bank of Tanzania is preparing draft mobile payments regulations. Mobile payments

37 Id. at 31-32 (art. 75).
38 Id. at 31 (art. 74(2)).
39 In turn, the MLICT had influenced the predecessor of the PSD, i.e., Directive 97/5 of the European Parliament and of the Council of 27 January 1997 on Cross-Border Credit Transfers 1997 O.J. (L 43) 25.
40 Alawi Masare, BoT to Check Mobile Payments in Tanzania, THE CITIZEN
have nevertheless been offered in the country since 2007.

Useful elements for the assessment may be found in the contractual provisions of two major mobile network operators offering payment services: Safaricom’s M-PESA in Kenya and Vodacom’s M-PESA in Tanzania. Those provisions deal with several issues discussed in the MLICT and the PSD.

Vodacom indicates that the user shall be responsible for all losses incurred in case of damage, loss, or theft of the SIM card, prior to notification of such loss. Transactions are effected and sums debited or credited when the sum is actually credited to, withdrawn, or transferred from the user’s account. However, the rules for the exact determination of the time when the credit, withdrawal, or transfer is considered completed remain unclear. The user may not reverse or chargeback payments. The liability of the mobile network operator is limited in several ways, including for losses arising from “particular circumstances,” even if known to the operator. The mobile network operator is also not liable for technical malfunctions resulting “from circumstances beyond . . . reasonable control.” These two rules depart significantly from the principle that risk should be allocated where it could be best prevented.

Safaricom specifies that the use of the PIN represents the authentication method and that operations entered under the legitimate PIN will be considered as validly performed by the user. Safaricom also offers, for instance, a rather comprehensive system of notification both for complete and incomplete


41 Customer Terms & Conditions, SAFARICOM (on file with author) [hereinafter SAFARICOM Customer Terms & Conditions]; Terms & Conditions, VODACOM available at http://www.vodacom.co.tz/vodacom-m-pesa/terms--conditions (July 20, 2012) [hereinafter VODACOM Terms & Conditions].

42 VODACOM Terms & Conditions, supra note 41, at r. 4.

43 Id. at r. 8.

44 Id.

45 Id. at r. 13.

46 Id. at r. 16.

47 SAFARICOM Customer Terms & Conditions, supra note 41, at 4.
payments. Payments may not be reversed; however, Safaricom may determine, at its sole discretion, the reversal of a payment in case of fraud or error, if the recipient has not yet redeemed the e-money and the claim is made within one month of the transaction date. Safaricom limits its liability to the maximum account balance limit for a single event or series of events; however, it accepts liability for failure in the M-PESA transmission system (though not in other systems).

**CONCLUSION**

A quick survey of the provisions available in developing countries shows significant differences, despite the fact that those provisions are prepared unilaterally by mobile network operators and accordingly reflect policy choices. Moreover, those rules are not comprehensive and may unduly penalize users. Nevertheless, contractual rules are the preferred solution given the gaps in the national legislation.

In light of these findings, it seems that the preparation of uniform enabling legislative or contractual provisions for mobile payments could be useful and timely. The argument against uniformity in payment laws, based on the fact that users, including consumers, may prefer to have a menu of options to choose from, and to bargain conditions individually, may not apply in a market where service providers are necessarily few due to the licensing system of mobile networks.

A uniform reference text could help in overcoming national

---

48 Id. at 5.
49 Id. at 5.
50 Id. at 7.
51 Id. at 7.
52 It is doubtful that existing rules in Kenya and Tanzania would address exhaustively all four fundamental questions that “at its heart, payments law must resolve”: who bears the risk of unauthorized payments; what must be done about claims of errors; when payments are completed and when they can be reversed. Mann, *supra* note 18, at 638. Of course, differences in the level of detail provided are significant between those two jurisdictions.
differences and would be particularly useful in addressing legal challenges arising from cross-border transactions. In particular, it could address a matter that was left open by the MLICT, i.e., the possibility of having a unique legal regime applicable to cross-border payments. The option of choosing only one applicable law was not accepted in the MLICT in order to avoid the possible application of a law unfavorable to non-bank entities involved in the payment.54

Specialists who discussed the topic at the previously mentioned UNCITRAL Colloquium on Electronic Commerce reached similar conclusions. In discussing the suitability of the MLICT as a basis for legislation for mobile payments, Professor Benjamin Geva concluded that:

Low-value credit transfers were envisaged as covered by the Model Law and yet were not central in the work leading to it. From this perspective, it is encouraging to find that, overall, the Model Law is appropriate to cover them. Consumer aspects, primarily as to disclosures are nevertheless to be added; consumer’s liability for unauthorized transfers is to be rethought and redrafted.55

At the same colloquium, Professor Maria Chiara Malaguti also concluded that an updated and revised text, more focused on non-traditional payments instruments and, dealing specifically with legal aspects of the activities of mobile network operators, “would be of enormous benefit at this point in time.”56

One manner of dealing with the issue could be to prepare standard contractual rules, to be enacted voluntarily by mobile

54 Bergsten, supra note 17, at 496.
network operators. This solution would be consistent with the favor for co-regulation in the ICT sector.

UNCITRAL could be an appropriate forum for this discussion, especially if this task is seen, as it should be, in the broader framework of the need for modern rules for all forms of electronic payments. Departures from general principles in the field of electronic payments to accommodate special needs of mobile payments should be kept to a bare minimum.

One major practical obstacle to having UNCITRAL work on the law of mobile payments is the fact that the matter is not seen as urgent or relevant by several countries active in defining UNCITRAL’s work agenda. Developing countries interested in the topic should express their needs and aspirations in a coordinated manner if they wish to see mobile payments on that agenda. The importance of a modern uniform legislative framework for mobile payments for the achievement of fundamental policy goals, such as the promotion of small and medium-sized enterprises, should also be stressed in order to get adequate attention from stakeholders.
MOBILE MONEY AS AN ENGINE OF FINANCIAL INCLUSION AND LYNCHPIN OF FINANCIAL INTEGRITY

Claire Alexandre and Lynn Chang Eisenhart

© Claire Alexandre and Lynn Chang Eisenhart

Cite as: 8 WASH. J.L. TECH. & ARTS 285 (2013)
http://digital.law.washington.edu/dspace-law/handle/1773.1/1200

ABSTRACT

Few people would dispute that mobile money can be an engine of financial inclusion and has the potential to reach millions of customers, including those at the bottom of the socio-economic pyramid. Fewer though would characterize mobile money as the lynchpin of financial integrity. But financial inclusion and financial integrity have at least three tangential points to mobile money: (1) mobile money will help reduce dependency on cash, which is the common enemy of both financial inclusion and financial integrity, (2) mobile money generates data which is instrumental to the health and growth of both financial inclusion and financial integrity, and (3) mobile money accelerates the development of accounts, which are the backbone of financial inclusion and financial integrity. In any case, if mobile money is to deliver on its promises for both financial inclusion and financial integrity, three regulatory barriers need to be removed.

* Claire Alexandre is a public policy expert in mobile and financial services and until recently, Senior Program Officer – Financial Services for the Poor at the Bill and Melinda Gates Foundation. Lynn Chang Eisenhart is a Program Officer – Financial Services for the Poor at the Bill and Melinda Gates Foundation. We thank Jane K. Winn, Louis de Koker, and Laura Powell for their contributions.

This Article was presented at the Mobile Money in Developing Countries: Financial Inclusion and Financial Integrity Conference held in April 2012 at the University of Washington School of Law with the support of the Linden Rhoads Dean’s Innovation Fund.
INTRODUCTION

In its Monetary Policy Statement of February 2012, the Bank of Tanzania highlights how “mobile financial services have contributed significantly towards broadening access to financial services in Tanzania given the high level of mobile phone usage.”\(^1\) Despite a high poverty rate, 78 percent of Tanzanian households and 63 percent of Tanzanians own a mobile phone. Simply walking through a market in Arusha shows ample evidence of the widespread availability of mobile devices and communication networks. By contrast, only 12 percent of the population in Tanzania was banked in 2009, leaving the remaining 88 percent to meet their financial needs through informal instruments and mechanisms outside the banking sector.

If people use mobile services to transmit voice and text messages, why should they not also use their mobile phones to transmit and store value? It may not be an obvious question for affluent customers who have several options with which to manage their financial needs, but for the 88 percent mentioned above, it is an important one. Leveraging existing infrastructure and services must be part of a solution that reduces costs low enough to reach down market and improve access to financial services in developing countries. In Tanzania, providers such as Tigo, Vodacom, Airtel, and Zantel are doing just that when they offer

---

mobile money services. When customers sign up for one of these services, they get an account from which they can send, receive, and store money using their mobile phone. This is in large part what Bank of Tanzania refers to in its Policy Statement.

Mobile money is at the crossroads of mobile communications and financial services, its power in distribution and marketing disguised under a technology facade. It is without a doubt disruptive to the business of incumbent financial services providers and has the potential to foster broad transformation through improved efficiency and simplified access. It is still a very young “industry” however; the first services were only launched commercially in the Philippines less than ten years ago and mobile money is becoming a reality at scale so far only in East Africa. So the potential is there, but it still needs to be realized.

Among the stakeholders interested in mobile money, policymakers and regulators are in a good position to drive change. When it comes to financial inclusion, mobile money appears very promising as it addresses the problems of cost and proximity, both of which contribute to the staggering figures of financial exclusion. When it comes to financial integrity however, mobile money seems less appreciated. Some worry that mobile money can be damaging to financial integrity as it increases the velocity of transactions. Some even have the perception that mobile money, when issued by mobile operators in particular, might be unregulated. This creates the impression of greater risk and seems to reinforce views that financial inclusion and financial integrity are in opposition with each other.

Rather than being the apple of discord between financial inclusion and financial integrity, mobile money actually serves both objectives by (1) helping to reduce dependency on cash, which is the common enemy of both financial inclusion and financial integrity, (2) generating data which is instrumental to the health and growth of both financial inclusion and financial integrity, and (3) accelerating the development of accounts, which are the backbone of financial inclusion and financial integrity. If mobile money is to deliver on its promises for both financial inclusion and financial integrity, three regulatory barriers need to be removed.
I. MOBILE MONEY REDUCES THE DEPENDENCY ON CASH

The role of cash, its costs, and its benefits are usually approached from a convenience point of view, and when cost is addressed, it is from the issuer perspective and how much it costs the State to mint. Canada is waving farewell to its one penny coins; they cost more to mint than they are worth.2 The use of cash also has other indirect costs and policy ramifications.

Living on the equivalent of a couple of dollars a day does not only entail a more precarious life due to little means. It also implies spending a great amount of energy and resources to manage cash, keep it safe, and transport it. While wealthier people live their financial lives using electronic financial instruments, poorer customers often have no choice but getting by with cash and physical assets. From a regional perspective, the difference is staggering: any single individual performs on average one hundred or more cashless transactions per year in developed countries, but less than one in Africa.3 Financial inclusion advocates could be tempted to limit their remittances to protect poor people using cash. A more ambitious goal to improve access to financial services, however, should actually start with finding ways to move away from a total dependence on cash and instead promote the use of electronic means to store value and transfer it. Make no mistake—this is not about going “cashless”; this is about providing consumers with an option to use electronic money or cash. As Mas and Porteous put it, “[i]t’s freedom from cash, not absence of cash.”4 And this is where mobile money can help.

Simply put, mobile money is essentially electronic money. It contributes to the development of an electronic ecosystem of

---


4 Ignacio Mas & David Porteous, A LiFi World, CONSULTATIVE GRP. TO ASSIST THE POOR BLOG (Jan. 11, 2012), http://technology.cgap.org/2012/01/11/a-lifi-world/.
financial services due to three key attributes. First, it enables the conversion, both ways, between cash and electronic money through a network of retailers. This may sound benign but it is actually the part of the value chain that is most critically lacking and the most difficult to design and execute well. Second, mobile money provides a storage facility for electronic value in the form of an account. For many customers, it will be their first account ever. Finally, mobile money offers a mechanism for transactions to take place electronically, which is particularly useful for non-proximity scenarios.

Of course, the ability to make mobile payments is not enough from a financial inclusion perspective. People need more than payment or storage functionalities to manage their financial lives—insurance, credit, and different types of saving options are also important, if not essential. However, repaying a loan when you only have cash is not always convenient. If you save a dollar a week, you might not feel like walking to the bank for that dollar every week. Paying someone close by is easy with cash, but still assumes you are going to carry cash with you, which is not always safe. Although mobile money is not a panacea, it can facilitate access to financial services in a manner that cash simply cannot.

The impact of mobile money on reducing the use of cash has less to do with the underlying technology and more with its convenience. Mobile money customers can use their own mobile devices to initiate transactions or check the status of their account wherever they have mobile coverage. If they need to deposit or withdraw cash, they know there is a store next door where they can make the conversion. If the experience is consistent over time and across different outlets, it will contribute to the creation of trust that is necessary to increase the use of electronic instruments and mobile money. Essentially, mobile money is more about distribution and accessibility than technology.

If mobile money helps the case of financial inclusion, it can also help another public good that is not available with cash:

---

financing integrity. Criminal and fraudulent activities are often more difficult to spot and disrupt if their proceeds are in cash, which is anonymous, fungible, and largely invisible. In contrast, electronic transactions leave traces, which can be used to recognize patterns and identify who is party to them. This is true even in cases where the identity of the sender or receiver cannot be authenticated. Some have argued that when accumulated in large amounts, cash becomes effectively very visible and rather unpractical to handle discretely. While this argument is logical, a large amount of cash could be even more visible if everyone else was using electronic means.

Overall, financial exclusion and its cash corollary are increasingly recognized as an impediment to financial integrity. The recent guidance paper of the Financial Action Task Force (FATF) on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion states that “informal, unregulated and undocumented financial services and a pervasive cash economy can generate significant money laundering and terrorist financing risks and negatively affect AML/CFT preventive, detection and investigation/prosecution efforts.” As mobile money shifts a large portion of cash-based transactions to electronic-based transactions, it magnifies the sheer volume of financial movements that can be monitored.

Some may believe that mobile money has an impact on financial integrity risk. The velocity of mobile money transactions could be considered by some as increasing financial integrity risks because they are faster than cash transactions in most cases since mobile money transactions are instant or near-instant. However, mobile money transactions are generally not more rapid than other electronic transactions. So as long as mobile money transactions

---


are regulated as electronic transactions, there is little reason to be concerned by their velocity. Also, their speed can be met by real-time analysis, providing an opportunity for observation that cash cannot provide.

In fact, mobile money services have the potential to be lower-risk products with respect to financial integrity. Let us not forget that mobile money builds on a mobile operator’s core business model of high volumes and low denominations. MTN Uganda allows its customers to send or receive as little as €1.5. Few electronic payment platforms would be able to match that. In its revised recommendations, FATF provides guidance on its risk-based approach and refers to lower-risk circumstances, which include “financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.” This does not mean that mobile money services per se are lower risk, but they could be designed in such a way. To qualify as lower risk, mobile money accounts are generally capped with limits in terms of transactions (number of transactions and amounts transacted) as well as balances. MTN Uganda for instance has set a maximum account balance equivalent to €300. Of course, fraudsters and criminals may very well try to use mobile money services if they have no better alternative, but such use would cause their reprehensible activities to become quite visible and traceable.

II. MOBILE MONEY GENERATES DATA

While reducing the dependency on cash and contributing to the increase in the number of electronic transactions, mobile money also produces a very strong asset for both financial inclusion and financial integrity: data.

Key to the fight against money laundering or terrorism

---

financing is data, which comprises the entire AML/CFT value chain. Financial institutions are charged, among other things, to generate information about their transactions, to store and monitor that generated data, and to report on the suspicious transactions they identify. This is the purpose of most of the so-called “preventive measures” contained in the FATF recommendations.\(^9\) Public authorities are then responsible for following up on reported suspicious transactions. Recommendation 29 specifies the role of a Financial Intelligence Unit (FIU), which is to serve “as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other [relevant] information.”\(^{10}\) FIUs are dependent on the data produced by the financial services industry. The regulatory debate around new services such as mobile money often focuses on the ability of the industry to meet these demands and on whether or not non-bank issuers or providers have to comply with preventive measures. Clearly, if an entity provides a financial service such as mobile money, it should comply with those rules. The challenge is to ensure the rules are applied in a proportional manner.

The introduction of mobile money services also raises other questions: as it considerably increases the amount of electronic transactions and the overall quantity of data produced, what is the capacity of the overall value chain to handle that data? In countries where FIUs are formally in place and actually operational, they manage today, with different degrees of success, data representing the financial services operations of a minority of the population (12 percent in the case of Tanzania, for example). Can they handle the volume of data representing the transactions of 50 percent of the population? And later 75 percent?

If capacity can be an issue, the question of the efficiency of the AML/CFT controls becomes even more important. Mobile money services can be used for all types of transactions, but many of the schemes launched in developing countries are designed to capture low-value transactions. Should AML/CFT controls apply to small value transactions in the same way as they apply to larger value

\(^9\) Id. at 62-66 (Recs. 9-23).

\(^{10}\) Id. at 24.
transactions? The answer is likely to revolve around the application of the risk-based approach.

New data and more data—thanks to the introduction of mobile money services—should prove very helpful on the financial inclusion front. Understanding how poor customers transact might start to shed some light on the behaviors and the needs of a segment of the market that has largely been ignored by many financial services providers. Although little has been done in that area, and a payment behavior does not necessarily reflect the same behavior for other services, there could be interesting applications in the areas of credit and insurance. Insurance services in particular are a great example of a highly data-dependent business that has had very little success in reaching down-market. Without consumer behavior data, the business case for providing insurance to the poor becomes very difficult to build. If insurance providers had access to payment data of poor customers, they could begin to build the business case to serve a new, diverse portfolio of customers. This concept of data’s ability to better illustrate a segment of potential customers and allow providers to selectively market to them is of course not specific to the insurance industry; in general, one can imagine how a bank might utilize payment behavior data to develop opportunities to cross-sell additional products, such as credit or long-term savings accounts, that improve the business case for a low-value bank account.

The opportunities discussed above—while providing significant advantages to financial services institutions bold enough to innovate—also place the mobile operators that generate this data in a very sweet spot. This data creates potential new revenue streams that improve the business case for mobile operators. They can now selectively sell data to parties that can utilize it to market products and services that are not in direct competition with mobile money, but rather help to broaden the services that can keep customers loyal to their existing mobile money scheme.
III. MOBILE MONEY ACCELERATES THE DEVELOPMENT OF ACCOUNTS

If financial inclusion and financial integrity have a common enemy in the form of cash, they may have a common ally in the form of an account, which is an important element of the backbone for financial services. The development of mobile money services increases the number of accounts and sheds a new light on their role for financial inclusion and financial integrity.

Mobile money is often seen through the prism of transactions and presented as a money transfer service and/or a payment platform. Airtel money services in India may “not [be] just about money”; its use cases are centered on sending, transferring, and paying. The need to move money around in an efficient and convenient way is certainly a strong explanation behind the demand for mobile money, but it could not be met without an account. For wealthier users, a mobile money account will be an additional account that likely complements a primary bank account. Conversely, for poorer customers, a mobile money account is often the first one they have and has the potential to integrate them further into the formal financial services ecosystem by providing access to other accounts that cover the range of their financial services needs.

While mobile money is the gateway to an account, accounts are a gateway12 to using a variety of financial services. They can take different forms to allow more straightforward or sophisticated operations but in all cases, an account remains an essential tool. It provides its user with a financial identity through an account number, which may equate in some cases with a phone number or another legacy identifier. The mobile money account introduces an interesting dimension as it is effectively a transactional account,

---


whereby the main function of the account is to enable transactions and not to solely hold float.

The change in emphasis and its focus on transactions enables an important shift in how to think about the economics of the account. It is no longer solely based on float but now also includes transactions. It is not surprising therefore that the concept was first devised by entities whose business model is primarily transactional: mobile operators. They are accustomed to handling a large number of transactions that are completed in very small denominations. There is no reason why banks could not also start thinking in the same terms and design transactional accounts as well. One of the reasons behind the high rate of financial exclusion lies in the design of accounts, which traditionally has required a minimum account balance at all times and fixed fees which are unrelated to the actual usage of the account. These attributes have placed standard financial accounts out of the reach of poor people.

Beyond their purpose of enabling transactions, mobile money accounts are also often low-value accounts. There are limits on how much one can transact or hold. These limits can be designed by the provider to meet the needs of a specific customer base but control its costs and exposure. They are often also set to reduce \textit{ex ante} the money laundering and terrorism financing risks, and to benefit from lighter Know Your Customer (KYC) controls. In both cases, low-value accounts are attractive for poor customers, meeting some of their financial services needs while not presenting high barriers to entry.

From a financial inclusion perspective, a low-value account is much more interesting than a no-frills account because it is more likely to drive usage rather than simply access. The former is designed to be in some way or form profitable and does charge fees to customers using it; it is based on the analysis that poor customers can and will pay for services which meet their needs but need variable rather than fixed fees. The latter cannot earn revenue directly from the customers (there are usually “free” accounts, which by stipulation cannot incur any fees) as it is often mandated by governments upon service providers. To minimize their loss, these providers are likely to seek to limit the availability of such products and unlikely to market them actively. As expected, no-frills accounts have met limited success; once opened, they remain
dormant and are seldom used. This is the case in India and South Africa.

From a financial integrity perspective, the main benefit of accounts is to establish stable “business relationships” through which transactions can occur rather than witnessing stand-alone transfers on an occasional basis or the use of prepaid cards. This is an equally important point on the financial inclusion side: some services are mere money-transfer services, or over-the-counter solutions, for instance Easypaisa when it started in Pakistan or Tigo Cash in Paraguay. That way, it is relatively similar to Western Union, although for domestic remittances. It is also a popular method of paying bills. The account goes one step further. Overall it is a more recurrent proposition, which makes it easier to move towards a cash-light ecosystem. The account also helps correlate payments across the payment network and makes it easier to collect and analyze data.

IV. REMOVING REGULATORY BARRIERS

Mobile money can deliver on promises for financial inclusion and financial integrity provided it has the means to develop. While this may sound obvious, the basic supply-side regulatory conditions for mobile money to be issued and used—and therefore begin to develop—are not yet in place in most geographies. Debates are numerous and passionate about the complexity of the issue, the uncertainty, and the risks. Due to the novelty of mobile money businesses, it is not surprising that many are quick to raise issues around consumer protection; the emphasis on the data digitization component of mobile money especially contributes to concerns regarding consumers.

There is very little question regarding the importance of consumer protection, and there are a number of regulatory issues to address on the demand side. For example, ensuring that terms and conditions as well as retail tariffs are published and available seems very sensible. Requiring mechanisms for customers to complain and even a redress mechanism is common sense. Generating and processing and/or storing electronic data require some level of protection on behalf of the consumer. However, sequencing of these regulations is critical to the development of
mobile money. Focusing on these types of regulatory requirements before having even addressed the basic enabling regulatory framework is shortsighted and can impede the initial stages of development. If mobile money services cannot develop, there is no mobile money consumer or data subject to protect. So while not undermining the importance of having the right regulation on the demand side, the priority of any regulator today should be to create an enabling environment for mobile money and to address the supply-side barriers.

A way forward is to move away from a one-size-fits-all regulatory model tailored around one product—credit—and one set of financial service providers—credit-issuing institutions. This way forward implies creating more classes of licenses, allowing tiered controls for account opening, and enabling distribution beyond bank branches through agents and retailers. Ironically by doing so, regulators—although they may disturb the established operating and business models of incumbent banks—may actually contribute to helping them become more efficient and better positioned to serve more customers.

In fact, mobile money is much simpler than it seems at first sight, even from a regulatory perspective. Take the “mobile” element first. It essentially refers to the distribution method the electronic money issuer has decided to use. So the regulatory risks associated with the “mobile” part in mobile money should be dealt with as part of the management of any technology and of the operational risks inherent to any financial service. Presently all financial services have important technology components; technology is not specific to mobile money. There are singularities around mobile technologies, whether at the level of the communication protocols or on the device side, but again they are not unique to mobile money and should be considered within the context of all technology and operational risks. They are present in mobile banking\textsuperscript{13} for instance, when a bank allows its customers to access their bank account using a mobile device. Regulatory frameworks are generally more useful and efficient when they

\textsuperscript{13} In this case, the bank is offering a mobile-based service, but does not issue electronic money, so it is not mobile money.
remains neutral from a technology perspective. So there is no need for specific “mobile money” regulation *per se* but instead for rules on electronic money that also apply to mobile money services. Unsurprisingly the “money” element is the most important. From a regulatory perspective, mobile money is not an alternative currency, it is essentially the same currency in electronic form: mobile money is already included as a monetary aggregate through the pooled accounts at the banks. It can be offered by a mobile operator but not exclusively: a bank can also offer a mobile money service, or even a retailer or a technology provider.

The confusion around mobile money usually stems from the question on the licensing of the issuing entity, in particular when it is not a bank. There should be no doubt that any issuer of electronic money must be regulated and therefore licensed to offer the service. This principle is also valid for mobile operators or any third-party technology provider or retailer. The issuing entity should, however, be regulated as an e-money issuer and not as a credit issuer (i.e., a bank). Financial services regulators are mostly accustomed to dealing with banks and tend to associate any funds received from the public as deposit-taking, an activity over which credit-issuing entities have a monopoly. However, electronic money is not a deposit, so electronic money transactions cannot be intermediated by the issuer if it is not a bank. Both the European legislation\(^\text{14}\) and the Philippines’ circular on electronic money\(^\text{15}\)—which were precursors in mobile money regulation—are very clear on that point. An e-money issuer that is not a bank is usually required by legislation to safeguard those funds and place them within a commercial bank, which is the regulated entity from a prudential perspective. So electronic money should be regulated, but there is no need to regulate the same funds twice.


In many countries today, there is still no option to issue electronic money without being a bank, buying a bank, or applying for a banking license. There must be more efficient ways to increase the amounts of electronic sources of funds and contribute to improving the efficiency of the payment systems and thereby of the overall financial services sector. Creating new classes of licenses for electronic money issuers is an important step to progress mobile money.

Another regulatory hurdle that mobile money faces relates to account opening. Mobile money issuers are unlikely to invest in mobile money if opening a mobile money account, which is the first step toward using the service, is made impossible or difficult. In many cases today, the same requirements are imposed for customer due diligence (also referred to as Know Your Customer) for any type of account, no matter what amounts they hold or are enabled to transfer. This is unfortunate for two reasons: (1) it defeats the purpose of the controls; and (2) it makes the overall system inefficient.

A uniform KYC\textsuperscript{16} means that some customers will not be able to open accounts: they simply do not have the necessary identification documents. As a result, they will continue to manage their financial lives using informal instruments on which no AML/CFT controls are imposed. By placing too high a threshold, the controls are only applied to a very small proportion of the overall transactions and accounts. The total amount of transactions conducted by a given population remains the same; there is simply a greater proportion which happens informally and is therefore not controlled.

A one-size-fits-all approach is not proportionate to the risks of the different accounts. A low-value account ought to have less scrutiny than an account that can be used to transfer or hold more. The type of customer (poor or not) matters relatively little here: a customer is not low risk because he is poor; rather he is low risk when he uses a low-value product.\textsuperscript{17} Applying a disproportionately

\textsuperscript{16} The FATF has allowed some flexibility on KYC since 2003, but country-level regulation has often not implemented that option.

\textsuperscript{17} As also noted in FATF GUIDANCE, supra note 5.
high level of KYC to some accounts and/or transactions does not make them safer in any way but simply more expensive. Putting on a helmet, gloves, and a padded jacket before heading out for a stroll on a walkway similarly does not add much to one’s security. It mostly adds cost and inconvenience. Finding the right level of KYC is a matter of efficiency for the service providers and for the whole system.

The solution is to apply a tiered approach whereby different KYC treatments apply to different types of accounts. Mexico has recently adopted legislation along those lines, starting with a very low level anonymous account with limited functionality and then progressively increasing financial and usage limits as the level of KYC increases. This principle of a gradual approach can also be found in the new FATF Recommendation 10 on Customer Due Diligence. The revised sets of international standards are most notable though for including this risk-based approach in the very first Recommendation. It reflects the significant shift exhibited by the intergovernmental organization in the last decade.

The restriction on distribution is the third regulatory hurdle and often an underestimated obstacle. Having mobile money issuers is one good thing, and being able to open an account is another. Having the option to open that account close to home or to work is even better. It excludes the use of bank branches that are relatively few compared to the size of the population.\(^\text{18}\) It requires instead the adoption of a broad distribution network, which can be composed of agents and third-party retailers or merchants. This model is not usual in the banking industry, where vertical integration has been the dominant approach. Such a model is expensive to deploy and operate. The solution is once more a tiered one, whereby different locations are available to manage different types of operations. If you only need to open a low-value account or to exchange cash against electronic money, you can go to the “mom and pop shop around the corner” (a small-scale, owner-operated nearby business), reasoning that they sell rice, soap, and pens, why not

\(^{18}\) In 2010, there were less than 11 commercial bank branches per 100,000 adults in India and Serbia for instance. There were 35 in the U.S., 33 in Japan and 23 in the Netherlands. Financial Access Survey, INT’L MONETARY FUND, http://fas.imf.org (last visited Aug. 28, 2012).
also electronic money? If you need to complete paperwork to apply for a loan, you might find it convenient to hand your forms over to an agent. If however you needed to actually discuss a loan with a credit officer or buy a more complex financial product, at that point it might make sense to visit a bank branch.

In most industries, this tiered approach is very common. It is adapted to customers’ needs and streamlines the costs of operations. To date, it has not permeated the banking industry, potentially in part due to frequent regulatory restrictions on the overall use of agents or third parties, the type of entities which can play that role, the type of services they can render or also the conditions they must meet to do so. In that case too, agents and merchants should be regulated but in a way that makes sense for the type of service they are providing and for the actual risks generated.

CONCLUSION

When not portrayed as contradictory policy objectives, financial integrity and financial inclusion have often been presented as incompatible. Financial inclusion was said to put financial integrity efforts at risk by promoting the use of financial services by the majority if not the entirety of the population. For some expanding access in such a way remains a scary thought. Financial inclusion advocates were blaming financial integrity guardians for undermining their efforts by erecting strict KYC controls. In truth, there is no tradeoff between financial inclusion and financial integrity—on the contrary, they reinforce each other. And mobile money is strengthening that relationship.
The Role of Anti-Money Laundering Law in Mobile Money Systems in Developing Countries

Emery S. Kobor*
© Emery S. Kobor

This Article explains that the application of anti-money laundering (AML) regulation, supervision, and enforcement is relevant to financial inclusion, but is not, in itself, necessarily determinative of the success or failure of financial inclusion initiatives or their impact on economic growth. Successful payments system innovation, particularly payment tools targeting underserved markets, requires effective entrepreneurship operating in an environment of good governance and rational economic policies. AML safeguards help to deter corruption and other forms of financial crime, which helps to establish and maintain economic stability and preserve the rule of law, creating a supportive environment for innovation and

* Emery S. Kobor is the assistant director for strategic policy in the Office of Terrorist Financing and Financial Crimes at the U.S. Department of the Treasury and is a member of the U.S. delegation to the Financial Action Task Force. Prior to joining the Department of the Treasury, he worked as a consultant advising corporate treasurers on payment and risk management strategies and was a senior research analyst for the Federal Reserve Bank of Chicago’s Payments Studies Group. Kobor earned an MBA degree in finance from George Washington University and an undergraduate degree from Vanderbilt University.

I would like to thank my colleagues Anne Larson, Mark Poncy, and Anne Wallwork for reviewing my remarks and providing helpful comments.

This Article was presented as the keynote speech at the Mobile Money in Developing Countries: Financial Inclusion and Financial Integrity Conference held in 2012 at the University of Washington School of Law with the support of the Linden Rhoads Dean’s Innovation Fund.
financial inclusion. This Article explains that the revised Financial Action Task Force (FATF) Recommendations, the international standard for AML practices, promote a risk-based approach to implementation, allowing countries flexibility in order to encourage the widest possible participation in the regulated and supervised financial system.

TABLE OF CONTENTS

Introduction ..................................................................................304
I. Payment Systems Innovation................................................306
II. Financial Inclusion.................................................................308
III. Economic Development.......................................................309
IV. Regulation and Supervision..................................................310
Conclusion ...................................................................................315

INTRODUCTION

I am delighted to be here today and for that honor, I want to thank Louis de Koker, whom I met several years ago when we were both speaking at a conference in Kuala Lumpur. I remember that event vividly because we gave multiple presentations over several days – something like a repertory company. I recalled that experience in preparing for today’s remarks. It occurred to me that, in order to discuss how anti-money laundering (AML) regulations apply to new payment methods that are used to spur financial inclusion and boost economic development, one must, in effect, give four presentations. Not only do payments innovation, financial inclusion, economic development, and AML regulation each deserve special attention, but how each influences and is influenced by the public and private sectors is also relevant.

Consider:

- The engine of innovation is private-sector ingenuity and the pursuit of profit. The public sector’s role in supporting payments system innovation, at the most basic level, is to allow for the accumulation of private property; protect property rights, including intellectual property, by upholding the rule of law; facilitate access to capital; and
permit competition to take place, while maintaining an open and stable economy.

- Entrepreneurs will reach out to the unbanked where it makes economic sense to do so. The unbanked will be responsive, provided their use of cash and unlicensed financial services are not a reaction to poor governance and inadequate economic policies. But any firm willing to invest in developing an untapped market is going to want as big a share of the potential profits as possible, which means a firm willing to move first will seek to erect barriers to competition. The public sector and non-governmental organizations (NGOs) fostering financial inclusion may seek to remove those barriers in the belief that more competition right away means greater financial access. Failure to coordinate public and private sector goals will ultimately impede financial inclusion.

- The pillars of economic development include macroeconomic stability, infrastructure development, and good governance, including promoting the rule of law. An unfriendly business environment—including endemic corruption and counterproductive monetary and fiscal policies—impedes growth and drives economic activity underground, which erodes the tax base worsening public-sector budget constraints and restricting government programs and policies intended to foster the basic conditions for further growth.

- Excessive regulation, including AML regulation, is a burden to business and a barrier to economic growth. But the rule of law and proportional regulation, particularly as it pertains to AML safeguards, deters corruption, enhances transparency, and facilitates international cooperation, which creates a supportive business environment.

That is a very quick overview of how payment systems innovation, financial inclusion, economic development, and financial regulation interact. Now I would like to look at each in a little more depth.
I. PAYMENT SYSTEMS INNOVATION

Almost ten years ago, I co-authored a paper at the Federal Reserve Bank of Chicago titled Why Invest in Payment Innovations? The title was not intended to be ironic. The paper was written to help financial services providers identify the appropriate strategy when investing in new payment methods. At the time, the focus was on how to leverage the Internet to extend payment options. Today, the focus is on mobile payments. But it is still a challenge for the private sector to know when to pursue customer acquisition versus customer retention, or to emphasize cutting costs versus boosting revenues.

The right private-sector strategy is based in part on where a company wants to be on what I refer to as the “innovation timeline.” To be the first to introduce a new payment method to the market involves taking a big risk, but opens up the possibility of big returns and locking in new customers if the strategy is successful. Taking the opposite approach and moving slowly can also be a big risk, but if fast-moving competitors stumble, their costly mistakes offer valuable lessons to the rest of the market. Even when the firm that acts first to establish a market is successful, other firms still have important strategic decisions to make as to how fast or how slowly they choose to follow, and how or whether they differentiate their services.

The innovation timeline starts when a company introduces a new payment method, ideally tapping into latent demand and a new source of profits. For taking the risk and making the investment to establish the market, a first mover will seek a high profit margin and will attempt to hold back competitors for as long as possible, often using proprietary technology and intellectual property protections. As competitors eventually enter the market, competition will gradually erode the advantage the first mover enjoyed, lowering prices and broadening market access over time.

But that scenario, in which a single company blazes a bold trail to a successful new market, is rare. More often many companies

---

attempt a number of strategies and more-or-less manage to find their way to a viable market. There is always uncertainty. The mobile payments initiatives currently struggling throughout the developing world demonstrate that the need for financial inclusion and the ubiquity of cell phones do not, by themselves, easily translate into profitable demand for mobile payments.

Safaricom’s M-PESA mobile payment service in Kenya stands out precisely because of the rarity of its success. There have been a number of studies comparing M-PESA with similar services elsewhere, including M-PESA in Tanzania;\(^2\) various mobile money providers in Ghana;\(^3\) and in the Philippines.\(^4\) The common deficiencies cited by these studies include ineffective marketing, inadequate distribution channels, and a failure to address country-specific demand characteristics.

Harvard Business School recently introduced a case study comparing M-PESA in Kenya with the mobile payments company WIZZIT in South Africa.\(^5\) The case study emphasizes that profits are earned by delivering what the customer wants, not what the service provider thinks the customer needs. More broadly, the case study illustrates that each component of a successful strategy is important, including how the company is capitalized, the marketing plan, and the distribution network. M-PESA is successful in part because the company focused narrowly on


providing a convenient and cost-effective way for Kenyans to send money domestically from urban areas to family members in rural communities. WIZZIT saw its role as providing a full suite of banking services to the unbanked in South Africa without regard for market demand. The Harvard case study concludes that WIZZIT, in addition to overreaching strategically, made less than optimal decisions regarding capitalization, marketing, and distribution.

II. FINANCIAL INCLUSION

For a mobile payments initiative to be a successful financial inclusion tool, it has to be a viable business. But government and civil society may be able to help influence the market’s rate of adopting a new payment method by changing how they pay salaries and conduct transactions. NGOs, development banks, and bilateral development partners may be able to introduce mobile payments or other electronic payment methods as part of relief initiatives. If coordinated with private-sector participants, these initiatives can promote financial inclusion.

More important than fostering the adoption of a product, however, is helping to develop a receptive market. Potential barriers to financial inclusion include market disruptions caused by armed conflict, extreme poverty, and natural disasters. Inadequate government infrastructure—including a lack of government-issued identification—as well as illiteracy, lawlessness, and well-established networks of unlicensed payment service providers also handicap financial inclusion initiatives.

Market demand for an alternative payment method is a function of need and experience. Need is influenced by the extent to which there is a supply of financial service providers, whether or not they operate legally. Experience is influenced by price volatility, opportunities for tax evasion, foreign exchange restrictions, corruption, and financial illiteracy, all of which can drive consumers and businesses to prefer cash.

In addition to promoting good governance and economic stability, government can help ease the cost to the private sector of marketing new payment initiatives by promoting literacy and
financial education, and providing incentives to help foster the transition to electronic payments.

III. ECONOMIC DEVELOPMENT

Financial inclusion is one facet of economic development, and financial inclusion itself has many facets beyond facilitating transactions. For example, giving the poor an alternative to cash that allows them to hold what money they have with a service provider for safekeeping has the effect of mobilizing capital. In Kibera, a slum in Nairobi that is home to hundreds of thousands of people who, remarkably, have electricity but very little else, I saw a surprising number of M-PESA agents. For the residents of Kibera, using M-PESA can reduce crime and help facilitate the accumulation of savings. My observations are consistent with the results of a recent study of the effects of M-PESA in Kenya, which concluded that M-PESA is helping to expand local economies, enhance security, help people to accumulate capital, and make transactions easier.6

There is a limit, however, to what can be accomplished without financial transparency, effective governance, and the rule of law. Serious development challenges remain in Africa, where, according to the World Bank, almost half the population lives on US$1.25 a day, and governance and transparency remain weak.7 There is an understanding in Kenya of the importance of good governance and transparency to economic development. The country’s development plan, Kenya Vision 2030, states: “One of the most urgent steps towards creating a competitive financial environment in Kenya is introducing legal and institutional reforms that will enhance transparency in all transactions, build trust and make enforcement of justice more efficient.”8 However, Kenya’s

8 GOV’T OF THE REPUBLIC OF KENYA, KENYA VISION 2030 – THE POPULAR
slow progress on financial transparency, combating corruption, and affirming the rule of law may jeopardize the gains M-PESA has achieved.

Corruption is most prevalent and damaging where it compounds other forms of institutional inefficiency, such as political instability, bureaucratic red tape, and weak legislative and judicial systems. Research by the International Monetary Fund shows corruption reduces economic growth primarily by discouraging private investment. Poor monetary and fiscal policies also hurt economic growth by inadvertently encouraging consumers and entrepreneurs to use cash and transact in the underground economy. The Council of Europe estimates the underground economy accounts for as much as two-thirds of gross domestic product in some Central and East European countries where, as they put it, “the rule of law is still fragile.” Zimbabwe gave up on monetary policy in 2009, adopting the U.S. dollar instead. But the memory of crushing inflation is keeping people away from banks and alternatives to cash, putting a brake on economic growth. Argentina, Greece, Italy, Nigeria, Russia, and Tanzania are struggling to reduce the use of cash through regulation in order to mitigate capital flight, financial crime, and tax evasion. However, in countries with inadequate regulation, supervision, and enforcement, electronic transactions are more efficient for both licit and illicit transactions.

IV. REGULATION AND SUPERVISION

The ease with which money moves around the world today

---


makes it seem that every major financial crime now is an international crime. The U.S. Department of the Treasury was reconfigured in 2004 to better deal with the challenges of money laundering and terrorist financing, which have become increasingly more complicated. The creation of the Office of Terrorism and Financial Intelligence (TFI), where I work, signaled a new era for finance ministries globally. TFI includes an intelligence component and has enforcement, policy, and regulatory authorities. TFI works to establish, support, and enforce best practices against money laundering and terrorist financing domestically, bilaterally, and through multilateral bodies, including the Financial Action Task Force (FATF).

Established by the G-7 Economic Summit in 1989, the FATF is acknowledged by the G-20, International Monetary Fund, World Bank, and United Nations to be the global standard-setter for anti-money laundering and counter terrorist financing policies and procedures (AML/CFT). The FATF includes 36\(^{12}\) members, representing most major financial centers in all parts of the globe. In addition to setting AML/CFT standards, the FATF promotes and assesses compliance and, when necessary, coordinates diplomatic pressure and countermeasures through its member governments. Through a combination of technical expertise and political and economic strength, the FATF has been unique among international bodies in its ability to take strong, effective multilateral action to prompt positive change in strengthening jurisdictional AML/CFT regimes worldwide.

The FATF recently revised its Recommendations. Originally there were 40 AML Recommendations. After September 11, the FATF adopted nine special recommendations to address terrorist financing. As part of the revision this year, some recommendations were combined or dropped, some added, resulting once again in 40

\(^{12}\) The FATF members include: Argentina; Australia, Austria, Belgium, Brazil, Canada, Denmark, European Commission, Finland, France, Germany, Greece, Gulf Cooperation Council, Hong Kong, China, Iceland, India, Ireland, Italy, Japan, Luxembourg, Mexico, Kingdom of the Netherlands, New Zealand, Norway, People’s Republic of China, Portugal, Republic of Korea, Russian Federation, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom, and the United States.
Recommendations, with no special recommendations. The FATF 40 Recommendations now cover money laundering, terrorist financing, and the financing of proliferation of weapons of mass destruction (WMD).

The Recommendations are clustered into seven categories, with the first two Recommendations making up the first category. The new Recommendation 1 calls on countries to undertake a national risk assessment to understand the money laundering and terrorist financing risks in the country. A guidance paper is being prepared to help countries conduct their first risk assessment. Recommendation 2 calls for national risk-based AML/CFT policies, responsive to the risk assessment.

Recommendations 3 and 4 address criminalizing money laundering and facilitating the forfeiture of illicit assets. The next group, Recommendations 5-8, addresses the financing of terrorism and WMD proliferation, including the implementation of relevant sanctions in United Nations Security Council resolutions.

The preventative measures, Recommendations 9-23, are the standards most closely associated with the FATF and most directly tied to discussions of regulatory costs, economic growth, and financial inclusion. These Recommendations include the customer identification and recordkeeping obligations, as well as requirements for filing suspicious transaction reports and conducting enhanced due diligence when opening an account for a foreign political figure or their family members.

Recommendations 24 and 25 concern the registration of legal entities and opening an account for a legal entity at a financial institution, and the requirement in both processes to understand who owns or controls the entity—so-called beneficial ownership. Recommendations 26-35 address supervision of financial institutions, the role and responsibilities of law enforcement, and the role of financial intelligence units.

The final category, Recommendations 36-40, addresses international cooperation, including requirements to implement four international conventions. These Recommendations include

---

13 "The Vienna Convention, 1988; the Palermo Convention, 2000; the United Nations Convention against Corruption, 2003; and the Terrorist Financing Convention, 1999." FIN. ACTION TASK FORCE, INTERNATIONAL
criteria addressing cross-border cooperation for civil and criminal investigations, the freezing and confiscation of assets, extradition, and cooperation among supervisory authorities.

The FATF is working on a new methodology for the mutual evaluation process to assess compliance with the Recommendations. Previously, the assessment process was detailed, technical, and lengthy, and produced detailed, technical, and lengthy reports. The goal of the new methodology is to assess the effectiveness of the implementation of the standards rather than rate technical compliance, and in doing so, hopefully, the next round of mutual evaluation reports will be less technical and much shorter.

Exactly what criteria the FATF will use to measure effective implementation is the subject of ongoing lengthy discussions. It is hoped that emphasizing effective compliance with the FATF Recommendations will help to provide the financial transparency necessary to deter corruption, assist law enforcement, and maintain the rule of law not only at home, but globally through international cooperation. Poor laws and inadequate enforcement provide little capacity to support neighbors seeking help in conducting criminal investigations, identifying stolen assets, or deterring terrorist financing. A country that demonstrates an unwillingness to address significant gaps in its AML/CFT regime opens its borders to a cross-flow of illicit assets, weakening the anti-corruption and AML/CFT efforts of other countries.

Flexibility is built into many of the Recommendations, allowing countries to take a risk-based approach to implementation. The FATF has published guidance papers that illustrate how to apply a risk-based approach. But a review of the FATF mutual evaluations that were completed between 2005 and 2011 indicates that few countries attempted to assess the risks they were trying to address and apply the FATF Recommendations.

accordingly. Most countries took a uniform approach, mandating the same obligations of all financial institutions, regardless of product or customer. This strategy can hamper financial inclusion efforts involving small-scale, low-risk financial services providers.

One reason why the risk-based approach has not yet been widely embraced is because it is not well understood. Most countries have not attempted a systematic risk assessment, and many will find it challenging. Where governance is weak, there will be few civil or criminal enforcement actions or suspicious transaction reports filed by financial institutions to help policy makers understand the underlying threats. However, a risk assessment does not have to be retrospective, especially regarding new payments initiatives fostering financial inclusion. Establishing usage limits such as a balance, deposit, or withdrawal cap and transaction limits, with effective ongoing transaction monitoring, is one way to limit risk by design.

I often hear that the FATF customer identification and recordkeeping obligations can be too burdensome for developing countries, especially those exploring financial inclusion initiatives using mobile payments or other new payments methods. But in fact, customer identification and transaction recordkeeping are essential to the private sector to inform marketing decisions, help prevent fraud, and protect consumers. An important benefit M-PESA has enjoyed in Kenya is the availability of government-issued identification for citizens over the age of eighteen.

Accommodating non-traditional financial service providers, particularly non-banks offering account-based services, within the regulated financial system can be difficult for many countries. The traditional regulatory framework divides financial services providers into those that offer account-based or transaction-based services, with banks on one side and money or value transfer services on the other. Allowing account-based financial services to be offered by businesses that are not regulated as banks can extend the physical reach of the formal financial system, but requires a new approach to regulation that applies safeguards on the basis of potential risk. One way to reduce risk and allow for a reduced regulatory burden is for non-traditional financial services providers to cap account and transaction value or deposit and withdrawal value and frequency.
A different challenge for many countries is limited resources for supervision, examination, and enforcement. If a country has only a small cadre of trained bank examiners and the central bank can barely account for the depository institutions in the country, it is daunting and potentially dangerous to open the financial system to additional service providers without adequate oversight or without limiting the potential risk. Defining the parameters of what is acceptable for businesses operating as financial services providers can help to reduce the risk and help countries become comfortable with allowing nontraditional service providers into the market.

The tools to foster economic development are not at odds with AML/CFT policies and procedures, and in fact are mutually reinforcing. The challenge for developing countries is to ensure that financial inclusion efforts involving new payment methods include appropriate risk-based AML/CFT safeguards, rather than assuming these efforts can be sequenced. It is misguided to start implementing new financial services now and follow with regulation and supervision at some point in the future. A better approach is to apply appropriate safeguards, given the potential risks. A mobile payments initiative offered through a mobile network operator that provides the unbanked a limited purpose account arguably could present a lower money laundering and terrorist financing risk than the status quo, if the status quo means a large unbanked population, transacting in cash, using unlicensed money transmitters.

**CONCLUSION**

In an increasingly interconnected world, our interests are inextricably bound to the interests of those beyond our borders. A few years ago, when Gordon Brown was still Chancellor of the Exchequer in the United Kingdom before becoming Prime Minister, he said: “There is a paradox about globalization: the very opportunities it offers—the free movement of money, people, goods and information—are harnessed by terrorists and organised
criminals.”

Brown’s observation is a good reminder that as we seek to channel the benefits of technological and geopolitical change to increase access to economic opportunity, we must also work to limit opportunities for corruption, financial crime, and terrorism. The FATF Recommendations are above all intended to establish a common defense against financial crime, and encouraging financial inclusion supports that effort.

---

The usage of mobile banking and in particular, payments by means of mobile phones, has increased in recent years in South Africa, with consequent impacts from a legal and regulatory point of view. South Africa is a developing economy with a large “unbanked” sector. That is, a large segment of the population does not have bank accounts and “banking” happens through informal means. This Article deals with the legal and regulatory framework pertaining to mobile money and examines issues relating to financial integrity and financial inclusion as they present themselves in South Africa. The author states that the regulatory framework in South Africa is not entirely conducive to greater financial inclusion and argues for a better balance between the regulation of risk and access to the payment system through an enhanced implementation of a risk-based approach.
INTRODUCTION

Mobile banking, and consequently, mobile payments and mobile money are the latest in a myriad of emerging technological innovations in the banking industry. The usage of mobile banking and in particular, payments by means of mobile phones, have increased in recent years in South Africa, with consequent impacts from a legal and regulatory point of view.

South Africa is a developing economy with a large “unbanked” sector. That is, a large segment of the population does not have bank accounts and “banking” happens through informal means. It also appears from latest figures that the penetration level of South Africans with mobile phones is increasing, yet the regulatory framework is not entirely conducive to greater financial inclusion. This Article seeks to examine the legal and regulatory framework pertaining to mobile money and examines issues relating to financial integrity and financial inclusion as they present themselves in South Africa. Regulatory gaps and areas for
improvement are highlighted. The author argues for a more flexible approach to regulation in South Africa to enhance financial inclusion through the use of mobile money there.

I. DEFINITION OF MOBILE MONEY

Before one could understand the term “mobile money,” it is necessary to understand associated terms that may have bearing on the definition of mobile money. As a form of e-banking,1 “m-banking” is defined as “financial services delivered via mobile networks and performed on a mobile phone. These services may or may not be defined as banking services by the regulator, depending on the legislation of the country in question, as well as on which services are offered.”2

“Mobile money” or “m-money” is a form of electronic money and refers to services that connect consumers financially through mobile phones. Mobile money allows for any mobile phone subscriber—whether banked or unbanked—to deposit value into their mobile account, send value via a simple handset to another mobile subscriber, and allow the recipient to turn that value back into cash easily and cheaply.3 In this way, m-money can be used for both mobile money transfers4 and mobile payments.5 Mobile

---

1 E-banking is the use of electronic delivery channels for banking products and services. See BANK FOR INT’L SETTLEMENTS [BIS], RISK MANAGEMENT PRINCIPLES FOR ELECTRONIC BANK 5 (2001), available at http://www.bis.org/publ/bcbs82.pdf.


4 “Mobile money transfers” are international remittances using mobile phones. For more detail, see CPSS & THE WORLD BANK, GENERAL PRINCIPLES FOR INTERNATIONAL REMITTANCE SERVICES 2 (2007), available at http://siteresources.worldbank.org/INTPAYMENTREMMITTANCE/Resources
money transfers are thus included in the definition of mobile money for the purposes of this Article.

II. MOBILE MONEY IN SOUTH AFRICA

Mobile banking has been increasing in South Africa. Several initiatives have emerged for initiating payments from mobile phones by using short messaging services (SMS) or phone calls. Some products use the phone as an access channel through existing bank accounts or payment cards. Meanwhile, other products allow customers to pay using prepaid value stored on their mobile phone or to pay afterwards, where payment for goods or services are additional items on the customer’s phone bill or through the use of Near Field Communication (NFC) technology. However, this system was only piloted once within a closed system during a music festival called “Oppikoppi” and on a trial basis by ABSA employees.6

Initially the four major banks in South Africa were given a wake-up call with the emergence of then-new kid on the block, WIZZIT.7 However, it is apparent that it is now the four biggest


5 “Mobile payments” refer to the provision of payment services through the use of mobile phones, mostly electronic funds transfer between a customer’s own accounts, transfers to a third party (beneficiary), or would be mobile money. A mobile payment may also refer to the process of two parties exchanging financial value using a mobile device in return for goods and services. See Elham Ramezani, Mobile Payment 4 (June 17, 2008) (term paper, Hochschule Furtwangen Univ.), available at http://webuser.hs-furtwangen.de/~heindl/ebte-08-ss-mobile-payment-Ramezani.pdf.


7 WIZZIT is the brain-child of Brian Richardson. It has a strategy of getting into South African townships using “whizz kids” to sign up users to open bank accounts. MTN Banking is a joint venture between MTN and Standard
commercial banks (Nedbank, First National Bank, Standard Bank, and ABSA) that are the providers of mobile banking services in South Africa through joint ventures with mobile technology companies and retailers. For example, Nedbank and mobile operator Vodacom teamed up to launch M-PESA, a solution that enables person-to-person money transfers via mobile phone, even between persons without bank accounts. This followed the Standard Bank’s launch of a similar product, called “Instant Money,” a joint venture between the bank and local retailer Spar. Standard Bank also has a joint venture company called “Oltio” between itself and pan-African mobile network operator MTN, which, through its “payD” platform enables customers to purchase products and services online and use their debit cards to pay for the purchase while making use of their mobile phones to enter their personal identification numbers (PINs). First National Bank also entered the fray, launching its “e-Wallet” mobile money transfer solution, which allows customers to send money to anyone in South Africa with a valid mobile phone number. Finally, as stated previously, ABSA Bank conducted South Africa’s first live user trial of NFC technology on mobile phones, in a partnership with MasterCard, to embed the “Paypass Tap and Go” payment chip on mobile handsets for the trial. This enabled customers to load funds onto their phones through the ABSA website or ATMs and then to pay for goods or services by merely holding their phones in front of NFC-enabled pay points. The value of their transactions is then immediately debited from their stored value.8

Bank of South Africa. MTN simply requires a SMS that the user provides an ID number and make a follow-up call to start an account-opening procedure that includes voice recognition technology. FNB Mobile at one stage in 2005 signed up 130,000 customers in six months. WIZZIT was developed to operate even in older phones and is not confined to any mobile telecommunications network. It “piggybacks” on the banking license of Bank of Athens, a registered branch of a foreign banking institution. See Maya Fisher-French, *Talking ’Bout a Revolution*, MAVERICK MAGAZINE, Nov. 3, 2005, at 34, available at http://www.wizzit.co.za/media/revolution.pdf.

Mobile devices are well positioned for making payments because the penetration level of digital mobile phones is higher in South Africa than that of computers. Latest figures from Wide World Worx suggest that in 2009 South Africa had a mobile penetration level of about 10.8 percent, which amounted to 5,300,000 users out of a population of 49,052,489.9

It is interesting that, even though the use of Internet services has exploded in South Africa, less than half of urban mobile phone users who have Internet-enabled phones use the Internet. As many as 9,500,000 South Africans are able to browse the Internet on their phones.10 If they use the Internet, the figure of World Wide Worx would almost double to 9,600,000.11 The potential thus clearly exists for a higher penetration level with respect to Internet-enabled payments through the use of a mobile phone.

It is also interesting to note the inroads that have been made to increase the level of banked South Africans. Between 1993 and 2009, the number of banked South Africans increased remarkably, especially in the black ethnic group. This increase has largely been due to easier access to banking services being provided to people living in informal urban areas and to those earning less than ZAR2,000 a month. The driving force behind the substantial increase was the South African government policy on economic empowerment and the inclusion of targets in the Financial Sector Charter, which led to a proliferation of products and services offered, such as “Mzansi accounts,” ATM cards, debit/check cards, credit cards, savings and transaction accounts, as well as mobile banking.12 Nonetheless, a significant portion of the black population is still unbanked.13

11 Id.
13 For more detail, see FINMARK TRUST, FINSCOPE SOUTH AFRICA (2009),
III. FINANCIAL INCLUSION AND THE SOUTH AFRICAN LEGAL AND REGULATORY FRAMEWORK FOR MOBILE MONEY

The regulatory stance in South Africa has mostly been with reference to electronic money, a subset of e-banking. The legal and regulatory framework with regards to e-banking would apply to mobile banking. In South Africa the legal framework is comprised of the following:

- South African Reserve Bank Act (Act 89 of 1990);
- National Payment System Act (Act 78 of 1998);
- Banks Act (Act 90 of 1994);
- Exchange Control Regulations (if cross-border);
- Financial Intelligence Centre Act (Act 38 of 2001); and
- South African Reserve Bank Position Paper on Electronic Money.14

A. The National Payment System (NPS)

Payment systems are critical to the effective functioning of financial systems in a country and globally.15 If a payment system is insufficiently protected against risks such as credit, liquidity, and

---


15 The payment system can also be described as the “essential oil that lubricates the economy.” Stefan Gannon, Weaving Nets to Catch the Wind: The Legal and Regulatory Issues Concerning the Development of Robust and Efficient International Electronic Financial Infrastructure, 33 COMM. L. WORLD REV. 352, 353 (2004).
settlement risks, disruption within the system could trigger or transmit further disruptions among its participants, or generate systemic disruptions in the financial markets or more widely across the economy. This phenomenon is referred to as “systemic risk.”

A fundamental requirement for a stable and secure payment system is that it should operate in a well-defined legal environment, setting out the rights and obligations of each party involved in effecting a payment through the system. It is for this very reason that Core Principle I of the Core Principles for Systemically Important Payment Systems published by the Committee on Payment and Settlement Systems of the BIS provides that the legal basis for payments should be well defined. The ambit of the South African NPS has been confirmed by the Reserve Bank in its recently released National Payment System Framework and Strategy Vision 2015.

---

16 The generally accepted terminology used to describe these risks are derived from CPSS, BIS, A GLOSSARY OF TERMS USED IN PAYMENTS AND SETTLEMENT SYSTEMS (2003), available at http://www.bis.org/publ/cpss00b.pdf.
17 This is to guard against “legal risk.” “Legal risk” is defined by the BIS as “the risk of loss because of the unexpected application of a law or regulation or because a contract cannot be enforced.” See id. at 29.
18 It states that “the system should have a well founded legal basis under all relevant jurisdictions.” CPSS, BIS, CORE PRINCIPLES FOR SYSTEMICALLY IMPORTANT PAYMENT SYSTEMS 6 (2001), available at http://www.bis.org/publ/cpss43.pdf.

The oversight domain of the NPS entails the entire process of making payment. In other words, it entails the process (including but not limited to) that enables the payer to make a payment . . . the payer to issue a payment instruction via a payment instrument or other infrastructure, the institution to receive the payment instruction via clearing or otherwise, the process of clearing and settlement (where applicable), the beneficiary to accept the payment instruction, the beneficiary
B. Oversight of the NPS

The Reserve Bank, as a neutral agent, is best suited to oversee and supervise the NPS. Section 10(1)(c) of the South African Reserve Bank Act enables the Reserve Bank to establish, operate, oversee, and regulate payment, clearing, and settlement systems. This power is reaffirmed in Section 2 of the National Payment System Act.20

Besides the general powers of oversight in terms of Section 10(1)(c) of the Reserve Bank Act as mentioned above, the Reserve Bank has the power to issue directives,21 in consultation with the

---

20 Nat’l Payment Sys. Act 78 of 1998 (S. Afr.), available at http://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/NPS%20Act.pdf [hereinafter NPS Act]. The National Payment System Department of the Reserve Bank performs the oversight of payments in South Africa. In terms of Section 3 of the Banks Act, the Registrar of Banks supervises the banking industry. The Registrar performs this function, in conjunction with the Bank Supervision Department of the Reserve Bank. Depending on the type of banking product that a bank wishes to offer, oversight would fall into the domain of either of these departments, sometimes into both. For example, there is no provision in the Banks Act that prevents a bank from setting up mobile banking. However, if mobile payments are offered, the matter would fall within the ambit of the National Payment System Department (NPSD), because the provision of these services may pose systemic or other risks which may threaten the stability of and confidence in, the National Payment System. For more detail on the South African NPS, see Vivienne Lawack-Davids, The Legal and Regulatory Framework of the National Payment System (NPS) – Peeling the Layers of the Onion, 29 OBITER 453 (2008).

21 Directives issued in consultation with the payment system management body terms of Subsection 1 are “general directives,” as opposed to the “remedial directives” which the Reserve Bank may issue in terms of Subsection 3. Provision is made for the cancellation of previously issued directives and an offense in Subsection 3. See NPS Act §§ 12(3), (5), (6), (8).
payment system management body and other stakeholders (Section 12(1)). The Reserve Bank has to date issued three directives, to wit, in respect of banks involved in the collection of payment instructions in the early debit order of Payment Clearing Houses (PCHs), in respect of system operators, and in respect of payments to third persons, but no directives dealing with m-money or m-payments.

Furthermore, the Reserve Bank sometimes issues Position Papers to clarify its regulatory stance. Although Position Papers do not have the same legal binding power as directives, they are usually followed because of the Reserve Bank’s moral persuasion powers. In addition, if the Reserve Bank is so inclined, it may issue a special directive aligned with its stance in the Position Paper that must be complied with, otherwise the Reserve Bank may apply to the High Court for an order to direct such person to comply with the directive issued.

“Mobile money” is defined in the 2009 Position Paper as:

[M]onetary value represented by a claim on the issuer. This money is stored electronically and issued on receipt of funds, is generally accepted as a means of payment by persons other than the issuer and is redeemable for physical cash or a deposit into a bank account on demand.26

---

22 It is an offense to fail, refuse, or neglect to comply with directives and a person who is found guilty of such an offense is liable to a fine of ZAR1 million or to imprisonment or to both a fine and imprisonment. No directives issued will have retroactive effect. Provision is also made for a grace period in respect of “general directives,” as opposed to “remedial directives” which will become effective immediately. See id. at § 12(9).


26 POSITION PAPER, supra note 14, at 3. The Reserve Bank initially issued a Position Paper on mobile money in 1999. This Position Paper was amended in 2006 and subsequently again in 2009.
Having “money” stored on a mobile phone could satisfy the definition of “mobile money” since it is monetary value represented by a claim on the issuer, it is stored electronically (on the mobile phone), it is issued on receipt of funds (to the issuer), and may be redeemed for physical cash or deposited into a bank account. However, one could argue that at this stage, mobile payments, while growing, would not be “generally accepted as a means of payment by persons other than the issuer.”

The definition of e-money in the 2009 Position Paper is different from previous definitions of mobile money in various respects. Most notably for purposes of this Article is that the Position Paper now states that only South African registered banks may issue mobile money, unlike the reference in the previous definitions of “making payments to undertakings other than the issuer, with or without involving bank accounts in the transaction.”

With the emergence of a few non-banks, such as mobile banking services providers and retailers, the effect is that the normal sponsorship arrangements for clearing and settlement will prevail. In other words, the retailer or technology company is not a settlement system participant and needs to be sponsored by a bank to enable clearing and settlement.27

Viewed from the Reserve Bank’s point of view, it could be argued that emerging e-money products may require regulatory adjustment or intervention, which may arise from the need to:

- Maintain the integrity, confidence and limit the risk in the NPS;
- Assist other regulatory authorities in providing consumers with adequate protection from unfair practices, fraud and financial loss; and
- Assist law enforcement agencies in the prevention of criminal activity.28

This view is affirmed by the new Reserve Bank Payment System Vision 2015, which explains that, in view of the global

---

27 See NPS Act §§ 4(2)(d)(i), 6 on clearing and sponsorship arrangements. See also POSITION PAPER, supra note 14, at 4.
28 POSITION PAPER, supra note 14, at 4.
crisis, a tightening of oversight is needed. Viewed from the perspective of non-banks wanting to enter this market, the Position Paper limits financial inclusion (access to the payment system) in that the non-bank would have to enter into a sponsoring arrangement with a bank, with consequent cost implications for such non-bank. Furthermore, the high growth and penetration rates of mobile telephony that is transforming cell phones into banks in pockets of Africa is providing opportunities for countries on the African continent to increase affordable and cost-effective means of bringing the “unbanked” into the formal financial system.29

With the requirement in the Position Paper that an issuer of e-money has to be a bank registered in South Africa, multiple regulators are involved, namely the South African Reserve Bank for regulation of banking and oversight of payments and the telecommunications regulator for the regulation of the telecommunications service provider.30 The problem with multiple regulators is that the possibility exists for regulatory arbitrage, that is, that players would take advantage of regulatory lacunae.

Whilst the above legal and regulatory environment seems for the most part sound, there are uncertainties as highlighted. It is submitted that instead of focusing on e-money, the South African Reserve Bank may want to consider issuing a Position Paper dealing with all forms of emerging payment technologies in which definitions can be stated clearly and any change in regulatory stance explained with reference to other regulatory instruments. It seems that due to the tightening of regulation, the trade-off is in favor of risk management over financial inclusion (access to the payment system). Klein and Mayer make a compelling argument that what mobile banking illustrates in a stark form is the way in

29 See for example the success of M-PESA in Kenya. For more information, see Carmen Nobel, Mobile Banking for the Unbanked, HARVARD BUS. SCH. (June 13, 2011), http://hbswk.hbs.edu/item/6729.html.
30 The Electronic Communications Act 36 of 2005 (S. Afr.) replaced the former Telecommunications Act 103 of 1996 (S. Afr.). This Act aims to converge broadcasting and telecommunications under one regulator. In South Africa, telecommunications are regulated in terms of the Electronic Communications Act. The main authority is the Independent Communications Authority of South Africa, established by Section 3 of the Independent Communications Authority of South Africa Act 13 of 2000 (S. Afr.).
which payment systems can be disaggregated into component services, namely exchange, storage, transfer and investment. In their words: “Regulation should mirror this and be structured by service rather than along traditional institutional lines, like a bank. The question then is what type of regulation is appropriate for each type of service.”

Okeahalam examines the NPS from an economic point of view and argues that there may be a trade-off between widening of access in the payment system and systemic risk. Whilst it is difficult to be specific as to the exact cost of widening access, there are financial, microeconomic, and actuarial methods for estimation of risk and relating risk to the welfare benefits of the payment system. It is submitted that Okeahalam is correct in his argument that different payment instruments present different sets of risk to the payment system. It is submitted that a “stratified” regulatory approach could be followed once an analysis has been done of the risks presented by individual instruments, as opposed to the individual institution, as is presently the case. This would mean that the regulatory approach would then be stratified based on the risks presented by the specific payment instrument. This is a challenge which is presently not well researched in South Africa, since the risks are determined based on the profile of the bank or institution. It is further submitted that with the increasing penetration level of mobile users in South Africa, research is needed into the impact on access to the unbanked given the change in regulatory stance of the South African Reserve Bank, lest a golden opportunity is missed to broaden access to financial services to the poor in South Africa.

---


IV. Financial Integrity

This section deals with anti-money laundering (AML) and combatting financing of terrorist (CFT) concerns as regulated in South Africa. Other policy issues such as seigniorage, operation of monetary policy, and consumer protection concerns fall outside of the ambit of this Article.

A. South Africa

South Africa has criminalized money laundering in three separate provisions of the 1998 Prevention of Organised Crime Act (POCA), which cover the conversion or transfer, concealment or disguise, possession, and acquisition of property in a manner that is largely consistent with the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention) and the 2000 U.N. Convention against Transnational Organised Crime (Palermo Convention). POCA provides for both criminal and civil forfeiture. The former is based on conviction of the offender whereas the latter is not dependent on conviction.

Terrorist financing is criminalized in South Africa in Section 4 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act (POCDATARA). The POCDATARA is comprehensive and criminalizes the collection or provision of property with the intention that it be used for the purpose of committing a terrorist act, or by a terrorist organization or individual terrorist for any purpose.

Comprehensive AML/CFT preventative measures have been

implemented in South Africa through the application of the 2001 Financial Intelligence Centre Act (FICA)\(^\text{36}\) and the Money Laundering and Terrorist Financing Control Regulations (MLTFC Regulations), read with various exemptions in terms of the Financial Intelligence Centre Act (Exemptions). The FICA has since been amended in 2008 by the Financial Intelligence Centre Amendment Act, which addressed, inter alia, some of the supervisory concerns raised in the FATF mutual evaluation of South Africa undertaken in 2008.\(^\text{37}\) While the POCA is the primary piece of legislation in terms of outlining activities that constitute money laundering offences, it does not outline the measures to be implemented to suppress and detect money laundering. Such is provided for in the FICA\(^\text{38}\) which is the principle piece of legislation in terms of outlining AML measures.

What follows is a more detailed exposition of the specific issues pertinent to this Article.

\section*{B. Analysis}

South African AML and CFT laws primarily affect mobile money via the customer due diligence (CDD) requirements that they place upon financial institutions. The CDD measures of the FICA and the POCDATARA are set out in the FICA, read with the MLTFC Regulations. The nature of these CDD requisites and their impact upon mobile money transactions are examined below.

1. Customer Identification and Verification

Section 21 of the FICA places an obligation upon “accountable institutions” to establish as well as verify the identity of their clients. The First Schedule of the Act outlines which institutions

\begin{itemize}
  \item \textsuperscript{38} FICA, supra note 36.
\end{itemize}
are accountable institutions in terms of the Act and amongst those listed are banks as well as money remitters. The FICA prohibits these institutions from establishing a business relationship or concluding a single transaction with a person unless they have taken steps to:

- Establish as well and verify the identity of the client; and
- If the client is acting on behalf of another person, or alternatively, if the person acts on behalf of the client, the institution must establish and verify the identity of the other person and their authority to act on behalf of the client, or as the case may be, the client’s authority to act on behalf of another person.

Should an accountable institution open an account or conclude a single transaction (once-off) transaction without duly identifying the client it commits an offence in terms of FICA.\(^3^9\) The penalty for such an offence is imprisonment for a maximum period of 15 years or a fine of ZAR100 million (US$12 million).\(^4^0\)

The MLTFC Regulations, which have to be read in conjunction with the FICA, give more intrinsic details in regard to how customer identification and verification of such is to be carried out (promulgated by GN No. R1595 in GG No. 24176). The Regulations state that, when establishing and verifying the identity of a client, the following information must be obtained:

- In the case of citizens, their full name, date of birth, identification number, residential address, and tax registration number.\(^4^1\)
- In the case of foreigners, in addition to the ordinary information that a citizen must provide, they are required to give details in regard to their nationality as well as passport number.\(^4^2\)

---

\(^{39}\) *Id.* at § 46.

\(^{40}\) *Id.* at § 68.


\(^{42}\) *Id.* at 5 (Reg. 5).
The FICA, in contrast to the Exchange Control Act and its Regulations, does not put a duty on financial institutions to determine whether their clients are legally present in South Africa. Hence non-citizens are not required to provide details in regard to their residence or work permit in order for financial institutions to comply with the FICA provisions.  

A person’s identity has to be verified by means of an identification document. In the case of South African citizens and residents, an official national identity document would need to be presented whereas foreigners have to present a passport. Residential addresses are to be verified using documents such as a utility bill. Records in regard to, amongst other information, a client’s identity, as well as transaction amounts, must be kept for a period of five years from the date that the business relationship is established or transaction is concluded.

The regulator was mindful of the fact that the need to present an identity document could prevent individuals without such a document from accessing formal financial services and hence created room for exclusion. The MLTFC Regulations therefore allow financial institutions, in circumstances where it is deemed to be reasonably acceptable for a person to be unable to provide an identity document, to rely on another document issued to that person that bears the following:

- A photograph of the person;
- The person’s full name or initials and surname;
- The person’s date of birth; and

---

44 MLTFC Regulations, supra note 41, at 4-5 (Reg. 4), 6 (Reg. 6).
45 An identity document is defined in Regulation 1. Id. at 3.
47 FICA §§ 22-23.
The person’s identity number.48

Examples of documents that can be accepted as an alternative form of verification in exceptional circumstances are a valid South African driver’s license or passport as well as a valid temporary identity document issued by the Department of Home Affairs.49 The latter documents should be valid in the sense that they must be current and unexpired.

This exemption is, however, not applicable to individuals who are not South African citizens or residents, as no mention of such is made within the Regulations. If the Regulations are strictly implemented, migrants who have neither a passport nor valid travel document in their possession would be unable to access formal remittance services. It is submitted, however, that even if the exception were applicable to foreigners it would likely be of little effect taking into account that studies show that financial institutions such as banks have been hesitant to exercise the discretion bestowed upon them by Regulation 6.50 The conservative approach has been attributed to the significant fines that are associated with money laundering offences.51

---

48 MLTFC Regulations, supra note 41, at 4-5 (Reg. 4(a)(ii)).
51 Bester et al., supra note 46, at 144.
Ideally the information gathered in identifying a client should enable a financial institution to form a client profile. According to de Koker, many South African institutions are unable to form an individual comprehensive client profile for general financial service customers that would support effective AML/CFT monitoring for unusual activity. This is due to the fact that under ordinary circumstances financial institutions are only obliged to obtain information that pertains to the personal identity of the client. Such particulars only play a small role in building a client profile and are insufficient to enable a financial institution to effectively detect suspicious financial activity by a client.

For a client profile to effectively be established, information such as the source of the client’s income would be needed. Financial institutions are only obliged to obtain such information in the case of business relationships or transactions that present a high risk of facilitating money-laundering activities.

In circumstances where a business relationship or once-off transaction presents a high risk of facilitating money laundering or where it is necessary for a financial institution to identify the proceeds of unlawful activity or money laundering, , the following must be ascertained:

- The source of the client’s income; and
- The source of the funds which the client intends to use to conclude the transaction or series of transactions in the course of a business relationship.

Professor de Koker states that the procedure prescribed by the current Regulation 21 is essentially a “Know Your Customer” or CDD procedure, in contrast to the ordinary procedure of identifying clients which is merely a “Client Identification and Verification” procedure.

---

53 MLTFC Regulations, supra note 41, at 15 (Reg. 21).
54 de Koker, supra note 52, at 724.
2. The Provision and Verification of a Residential Address

The obligation to provide an address and the need for such to be verified appears to have been the chosen safeguard against identity fraud. The value of providing a residential address for purposes of identifying a customer has been questioned. It is argued that such a requirement may be more useful in developed countries without a system of national identity numbers, but with rich sources of data on their residents.\(^\text{55}\) In such countries, addresses are helpful to distinguish between different people with similar names, but are less functional in countries with comprehensive national identification systems. Once an accountable institution obtains a client’s name, date of birth, and unique national identity number, there is no need for it to obtain a residential address. Requiring address verification under these conditions does not add significant identification value, but causes undue hardship for customers who often lack formal addresses.

Professor de Koker argues that the negative impact of residential address verification increases as a result of the high level of internal migration in South Africa.\(^\text{56}\) Such arguments become relevant when one considers the practical difficulties that have been experienced in South Africa in verifying the residential addresses of individuals.

In South Africa, the verification of a client’s address has presented certain difficulties, particularly with low-income individuals.\(^\text{57}\) The drafters of the FICA and its Regulations were aware of the fact that individuals who lived in informal settlements and rural areas could face problems in verifying their residential address in accordance with the regulatory requisites.\(^\text{58}\) As a consequence, room for exception from the need to provide a residential address was created by means of “Exemption 17.”

\(^{55}\) Id. at 742.

\(^{56}\) Id.

\(^{57}\) Bester et al., supra note 43, at 18.

latter is contained within the Schedule to the MLTFC Regulations.59

3. Enhancing Financial Inclusion: Exemption 17 and Mobile Money

Exemption 17 relieves certain financial institutions from the general obligation placed upon them by Section 21 of the FICA, which requires them to attain as well as verify their customer’s residential address. The exemption is only applicable if certain requirements are fulfilled. Exemption 17 was included in the original set of Exemptions, but it proved of little value in practice as the requirements were too rigid and could not be met by many unbanked persons. Exemption 17 was therefore revised in 2004.60

The amendments were informed by actual market research and take the needs of the financially excluded into account.61 According to Isern and de Koker, this framework allows “financial institutions to verify a person’s identity using the national ID document without having to verify the person’s residential address if the financial product meets a certain balance limit (US$3,000) and transaction restrictions (US$600 per day).”62

The amended Exemption 17 facilitated the launch of the Mzansi account63 that has reportedly brought over 6 million people into the formal financial sector.64

63 The Mzansi account is a savings account with basic transaction capability aimed at the low-income market.
64 See the data in BANKABLE FRONTIER ASSOC., THE MZANSI BANK
The Financial Intelligence Centre (FIC) has, in addition, issued guidance notes as contemplated in Section 4(c) of the FICA, which provide guidance to banks in regard to which documents qualify as acceptable verification documentation. In establishing and verifying customer identity, banks are encouraged to undertake a “risk based approach” as opposed to following a “one size fits all approach.”

Exemption 17 also enabled the creation of a simplified CDD framework for mobile money. The Banks Act Guidance Note of 2008 issued by the Registrar of Banks brought mobile banking products within the framework of Exemption 17. The product is offered to clients via a non-face-to-face process, which must be followed only on the basis of the minimum set of criteria being met. Importantly, however, a lower daily transaction limit of ZAR1,000 (US$120) per day is set. If a client wishes to exceed this limit, the normal verification procedures would have to be followed. Finally, the Guidance Note states that the “expansion of banking services should not happen to the detriment of control measures that are aimed at facilitating the detection and investigation, or even the prevention, of money laundering and terrorist financing through banks.”

It is submitted that the relief granted by Exemption 17, even in its amended form, is only partially effective in achieving the desired effect of increasing financial inclusion. This is taking into account that the exemption only provides room for exception in regard to the ascertainment of a client’s residential address; it does not absolve individuals from presenting an identity document. In addition to the latter, the exemption does not apply to cross-border...
transactions that go beyond the Common Monetary Area (CMA), comprised of South Africa, Lesotho, Namibia, and Swaziland.\textsuperscript{68} Transactions that go beyond the CMA are still subject to the stringent CDD requisites imposed by FICA. Furthermore, the exemption only applies to certain accountable institutions and not all of them. Mobile money transfer businesses, unlike banking institutions, have not been included within the scope of the exemption.

Asylum seekers have been dealt a major blow by the May 2010 FIC advisory issued to banks that banks are not allowed to transact with asylum seekers based on the official certificates and permits issued by the South African government. This means that an asylum seeker is barred from opening a bank account and conducting transactions until the application for asylum is processed, asylum was granted and the refugee was issued with a more formal maroon South African refugee document. Before the issuing of the interpretation, they were allowed to rely on the permits and licenses to open accounts. Since the interpretation was issued, asylum seekers have reported that banks have also refused them permission to withdraw their funds from the accounts that they have previously opened, causing severe personal hardship.\textsuperscript{69} Not only was the FIC advisory ineffective communication, it was also confrontational and upset a practice which banks have adopted as early as 2003.

A compromise has since been reached following litigation challenging the position of the FIC allowing banks to accept asylum documentation to verify identify only after verifying the authenticity of the document with the South African Department of Home Affairs.\textsuperscript{70}

\begin{itemize}
\item \textsuperscript{68} FICA Exemption 17, \textit{supra} note 60, at 6.
\item \textsuperscript{69} \textit{See} FATF, \textit{FATF GUIDANCE ON ANTI-MONEY LAUNDERING AND TERRORIST FINANCING MEASURES AND FINANCIAL INCLUSION} (2011), \textit{available at} http://www.fatf-gafi.org/media/fatf/content/images/AML%20CFT%20measures%20and%20financial%20inclusion.pdf.
\item \textsuperscript{70} For more information on the debacle, see Tatenda Gumbo, \textit{S. African Court Restores Access to Bank Accounts by Refugees and Asylum Seekers}, \textit{VOICE OF AMERICA ZIMBABWE} (June 8, 2012), http://www.voazimbabwe.com/content/south-african-court-restores-bank-access-for-refugees-107057558/1459047.html.
\end{itemize}
Despite the compromise, the hardship for undocumented migrants deepened when they lost their access to mobile communication in South Africa. The Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA)\(^{71}\) of 2002 introduced customer identification and verification measures that are very similar to the FICA CDD requirements. Users have to verify their identities using official documentation to access mobile communication services. Foreigners without passports are generally not able to legally gain normal access to South African-issued mobile phones. They are therefore faced with mobile money access barriers created by RICA as well as FICA. A recent report stated:

Refugees are vulnerable to the high levels of random crime that afflict South Africa, as well as sexual and gender-based violence, exploitation in the workplace and detention due to lack of proper documentation. Poor socio-economic conditions among host communities provide a breeding ground for xenophobia. Documents of limited validity compromise refugees’ efforts to become self-reliant by making it hard for them to hold long-term jobs, while at the same time a law allowing refugees and asylum-seekers to have bank accounts is not being fully implemented.\(^{72}\)

The fact that a passport must be presented effectively bars undocumented migrants who do not have valid travel documents from accessing formal remittance services. Migrants who live in informal settlements\(^{73}\) are also barred from accessing formal remittance channels as they are unable to fulfill the address


verification requisite imposed by FICA. In view of the above, it is submitted that regulators should give more thought in making policy that would align AML/CFT, financial inclusion, the regulation of telecommunications service providers who offer mobile money services, as well as South Africa’s international obligations to alleviate the plight of refugees.

In his Article on the 2012 FATF Standards, de Koker notes that the risk-based approach is now mandatory for countries and institutions and that the cornerstone of the risk-based approach is risk assessment. It is interesting to note that South Africa has to some extent followed a risk-based approach, but to date no formal risk assessment has taken place. The current CDD requirements, for example, were based on the previous FATF Recommendations. Regulation 21, for example, was based on the predecessor of 2003 Recommendation 5, which has now, in turn, been replaced by Recommendation 10. In effect this would mean that South Africa would have to conduct a formal risk assessment and in a sense conduct a “gap analysis” of the current CDD requirements as contained in the FICA and regulations thereto and match this against the new 2012 FATF Standards. Furthermore, lower-risk and higher-risk scenarios would have to be determined. Should the risk assessment show that mobile money is considered a “lower risk” product, the effect would be that the limits imposed would have to be commensurate with the risk identified, i.e. the lower the risk, the more simplified the measures should be. It would be interesting to see how this would be done in South Africa, where, as stated earlier, even though a “risk-based approach” was followed in the past, a formal risk assessment would now have to take place. It is hoped that in the formal risk assessment, a more equitable system would be employed as far as migrant workers who come from outside the CMA are concerned.74 This would

---

74 For example, mobile money could be regarded as “financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.” FATF, INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION: THE FATF RECOMMENDATIONS 64 (2012), available at http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%20(approved%20February
mean that regulators would have to show more faith in refugees and asylum seekers in amending Exemption 17, which remains to be seen.75

Even if the AML barriers are removed, refugees and asylum seekers are still faced with the barriers imposed by RICA.76 In effect this would mean that if a risk assessment is made for South Africa and a distinction is made between low-risk and high-risk scenarios, RICA would likewise have to be amended to allow for greater financial inclusion in line with the risk-based approach to be followed and formalised through the formal risk assessment.

4. Cross-Border Networking

If one is to take a look at the effects of AML measures upon the remittance industry from a wider perspective the FATF Standards become relevant. The 2012 FATF Standards deal with correspondent banking relationships in Regulation 13. Financial institutions that are involved in correspondent banking relationships must gather information about their counterparty’s business, which includes their AML and CFT supervision, investigation and regulatory action, and their AML/CFT controls. Furthermore, these financial institutions should obtain approvals from senior management before establishing new correspondent banking relationships; they must clearly understand the respective responsibilities of each institution and be satisfied that the respondent bank has conducted CDD on its customers who have direct access to accounts of the correspondent bank.

New Recommendation 14 provides that countries should take measures to ensure that natural or legal persons who provide

---

75 For more detail see de Koker, supra note 58, at 328.

money or money value transfer services are licensed or registered and subject to effective systems for monitoring and compliance with the relevant measures called for in the FATF Recommendations. South Africa would need to ensure that this is accommodated for in its legal framework.

V. RECOMMENDATIONS

Policy makers may need to consider some potentially new challenges posed by technological innovation and other changes in the payment system more generally as well as how these impact regulatory approaches with respect to AML/CFT. For instance, mobile money products in some countries may be offered by entities other than institutions subject to banking supervision, although many countries apply anti-money laundering laws to all institutions.

The extent of CFT/AML regulation should depend on the relative attractiveness for money launderers and risk posed by such a scheme. In other words, if a risk-based approached is followed, the level of regulation would be relative to the risk introduced by such system. It is recommended that a stratified approach to regulation of m-money be followed, viewed from a risk-based AML/CFT perspective.

The following factors could be taken into consideration to arrive at such a stratified approach based on the service rather than the institution:

- Semi-open systems – A limited form of regulation could be applicable. Issuers could be licensed as M-Money Issuers similar to the EU or U.K. position or Authorized Institutions similar to the Hong Kong position. One of the conditions could be to place a limit on the value on the card similar to the U.K. position.

- Open loop systems – In consultation with the SARB on oversight and supervisory issues, open loop systems would be regulated by the SARB in terms of its E-money Position Paper which restricts such systems to banks. However, from an AML/CFT perspective, the FIC could add provisions in the Regulations which would state that reporting on m-money products have to be done as part of
such bank’s obligations as an accountable institution in terms of FICA and the Regulations.

The relief granted by Exemption 17, as mentioned previously, is only partially effective in facilitating greater financial inclusion. The view is taken bearing into account that Exemption 17 is not applicable to certain mobile money transfers, namely remittance transactions that go beyond the CMA,77 nor does it apply to financial institutions that provide mobile money transfers (remittance services) as their only business.78 Hence, migrant laborers who live in informal settlements face a significant barrier in accessing formal remittance services as they are likely to face significant difficulty in verifying their residential address. An amendment of Exemption 17 is thus needed if the trade-off has to be in favor of financial inclusion. It is always difficult to balance financial integrity on one hand and the concern of financial inclusion on the other. South Africa would have to conduct a formal risk assessment in accordance with the mandatory risk-based approach advocated in the 2012 FATF Standards. This means that there is an opportunity to align the South African legal framework with the 2012 FATF Standards and hopefully, also amend Exemption 17 to be more inclusive, depending of course on the outcome of the formal risk assessment of course. This would also mean that the obstacles imposed by RICA be revisited in light of the formal risk assessment mandated by the 2012 FATF Recommendations.

CONCLUSION

This Article gives an overview of the legal and regulatory framework for mobile payments in South Africa. While the legal and regulatory framework is, for the most part, sound, the Article identifies risks, challenges, and uncertainties that regulators may take into account. The analysis also examines the significance of the South African Reserve Bank’s 2009 Position Paper on Electronic Money, the reasons for the change in regulatory stance,

77 FICA Exemption 17, supra note 60, at 6.
78 FICA Exemption 17, supra note 60.
and the effect that this may have on financial inclusion (access to the payment system) for non-bank mobile payment providers. Continued research in this area is needed to assess the impact of the change in regulatory stance on access to financial services for the poor, as a golden opportunity may be missed to increase financial inclusion to the payment system if it is found that there is over-regulation of mobile payments in South Africa. What may be needed is a stratified regulatory approach, that is, that regulation be structured by service rather than along traditional lines and that the focus should be on what type of regulation would be appropriate for which type of payment. The opportunity now arises to address this through a formal risk assessment, as mandated by the 2012 FATF Standards, as well as an amendment to RICA to remove the obstacles for refugees and asylum seekers. If this is not done properly, the clear benefits of mobile money as shown in Kenya may not be realized in South Africa.
M-PAYMENTS IN BRAZIL: NOTES ON HOW A COUNTRY’S BACKGROUND MAY DETERMINE TIMING AND DESIGN OF A REGULATORY MODEL

Gilberto Martins de Almeida *
© Gilberto Martins de Almeida

Cite as: 8 WASH. J.L. TECH. & ARTS 347 (2013)
http://digital.law.washington.edu/dspace-law/handle/1773.1/1203

ABSTRACT

Extended periods of high-inflation in Brazil have resulted in a sophisticated platform for payment methods and a vast network of banking correspondents all over the country. Social policies have encouraged increased access to telecommunications, with the number of mobile phones exceeding the nearly 200 million inhabitants. Governmental programs intend to combine such strengths to achieve massive financial inclusion and integrity, an effort that is expected to reach dozens of millions of new beneficiaries. In that endeavor, authorities wish to foster rapid popularization of mobile payments (m-payments) while keeping sound financial controls. Availability of current technological and legal platforms has allowed that a mature process develops in the selection of proper regulation. This Article discusses how Brazil’s background has determined the timing and design of a regulatory model, and points out a case of prudent approach by a developing country in the subject matter.

* Pontifical Catholic University of Rio de Janeiro (1983), LL.M. University of São Paulo (2000), currently attending Doctorate in Law at the University of Buenos Aires. Thank you to Adriana Mondolfo for extensive research and to Laura Powell for careful revision.

This Article was presented at the Mobile Money in Developing Countries: Financial Inclusion and Financial Integrity Conference held in April 2012 at the University of Washington School of Law with the support of the Linden Rhoads Dean’s Innovation Fund.
TABLE OF CONTENTS

Introduction ..................................................................................348
A. Background: Challenges Concerning E-Payments,
   Financial Inclusion, and Financial Integrity .................349
B. M-Payments: Nature, Modalities, and Characteristics....351
C. Legal and Regulatory Implications ...........................352
I. Financial Inclusion in Brazil .................................................354
   A. Concept and Outreach of Banking Correspondents ...354
   B. Payment Systems in Brazil .................................356
   C. Mobile Money Policy ........................................360
   D. Integration of Banks, MNOs, Retail, and  
ed-Government Interests ........................................ 361
II. Financial Integrity Concerns for Financial Inclusion .......362
   A. Money Laundering Concerns .............................362
   B. Tax Evasion Concerns ....................................367
   C. Foreign Exchange Concerns .............................367
   D. Mandatory Acceptance ....................................368
   E. Consumer Protection Issues .............................368
III. Perspectives and Possible Future Directions .................370
   A. Singular Local Environment .............................370
   B. The Bill of Law at the Congress .........................371
Conclusion ....................................................................................372

INTRODUCTION

“In short consumers only have confidence in cash tokens  
issued by, and/or guaranteed by either the central bank or  
government of the issuing state. This was the problem with  
cyberspace. There was no government, no central bank, and no  
pre-existing financial framework: only private organisations and  
competing technologies.” – Andrew Murray

1 Andrew Murray, Information Technology Law: The Law and  
Society 444 (2010).
A. Background: Challenges Concerning E-Payments, Financial Inclusion, and Financial Integrity

Mobile payments (m-payments) have been developed as a step forward in the process of dematerialization of money, following notarization, electronic fund transfer, automated teller machines, financial electronic data interchange, and Internet-based electronic payments.²

The introduction of m-payments³ is usually associated with expectations of enormous social outreach,⁴ assuming the number of mobile devices used in a given country far exceeds the number of local computers.⁵

However, the myriad of applications which may use m-payments—public services, transportation, convenience stores, payment of small amounts, and countless others—do not necessarily promote financial inclusion and financial integrity.

Depending on the regulatory model selected for a given environment, the social divide may deepen, e-government may become less effective, money laundering may become easier, and tax collection and foreign exchange control may become more difficult.⁶

³ “M-payments” may have different meanings (electronic fund transfers, payment for goods or services, or other financial services); given the absence of uniformity in research and data on the subject, this Article refers to m-payments as comprising mostly (though not only) mobile payments in exchange for acquisition of goods or services.
⁵ New mobile equipment technology rivals personal computers in the making of electronic payments, and has a greater portability advantage over them. See ÉTIENNE WERY, PAIEMENTS ET MONNAIE ÉLECTRONIQUES – DROITS EUROPEEN, FRANÇAIS ET BELGE 22 (2007).
⁶ There are different taxonomies of regulatory models. For instance, Marc Bourreau and Marianne Verdier identify five models: “light” model, bank-centric model, mobile-centric model, partial-integration model, and full-integration model. Marc Bourreau & Marianne Verdier, Cooperation for Innovation in Payment Systems: The Case of Mobile Payments 3 (Telecom
Experience\(^7\) has shown that the more a country emphasizes accelerated popularization of m-payments, the more likely it may lose financial controls, and vice-versa.\(^8\) The right balance between those opposing goals seems to hinge on specific public policies, designed on a country-by-country basis.

Notwithstanding, the phenomenon of global access to acquisition of goods or services in today’s society requires development of consistent, efficient international platforms. Technical and procedural standardization\(^9\) is key to building such common grounds.

In this regard, new harmonization of technological infrastructure must be struck between mobile network operators (MNOs) and banks, and between members of each category. Media convergence and m-payments’ exciting business prospects have turned this axis into an even more pivotal one.

The above aspects seem to indicate how the challenges posed by m-payments are both national and international, and how coordination will necessarily be the focus of associated legal and technical regulatory issues.

---

\(^7\) Reference is made here especially to the cases of Kenya and of European countries, as described, respectively, by Ignacio Mas & Daniel Radcliffe, Mobile Payments Go Viral: M-PESA in Kenya, 32 J. FIN. TRANSFORMATION 169 (2011), available at http://www.capco.com/sites/all/files/journal-32_article-16.pdf and by Murray, supra note 1, at 446.

\(^8\) In 2006, six years after the first specific Directives, there were only nine active electronic money issuers in Europe, while seventy-two institutions were in operation under the waiver set forth in the Electronic Money Directive for institutions that engaged in more limited financial operations. Murray, supra note 1, at 446.

\(^9\) Although most standards are formally qualified as technical, some are essentially procedural in nature, such as the Information Security standards developed by entities such as ISO, IEC, and ITU. See Int’l Telecomm. Union, Guidelines for Cybersecurity (2012), available at http://www.itu.int/itu-t/security/task_details.aspx?isn=4097&isnView=1&from=b1_-1!b2_-1!b3_-1!t1_-1!k_procedural.
B. M-Payments: Nature, Modalities, and Characteristics

M-payments are, fundamentally, technology-based payment methods comprising three basic modalities: (1) mobile phone as a wallet (storing money downloaded via Internet, or “reading” it from a smartcard); (2) payment ordered via short messaging service (SMS);\(^{10}\) and (3) payment effected by bringing mobile phone into contact or close proximity with some tagged device (using technologies such as Near Field Communication (NFC)).\(^{11}\)

Terminology surrounding m-payments varies considerably, however it seems fair to split m-payments into two categories: (1) a means of communicating payment orders, and (2) a means of storing and transmitting digital cash.\(^{13}\) The former may also be completed by computers, thus the latter appears to be the more unique category.

Mobile phones may have built-in features—such as a smartcard or credit or debit card reader, and NFC capabilities—or may work in conjunction with an attached device. The volume of equipment produced with built-in NFC capabilities has grown rapidly,\(^{14}\) and NFC capabilities are expected to become an industry standard.\(^{15}\)

Such payment methods usually include banks, Mobile Network Operators ("MNOs") (which provide the telecommunications infrastructure), accredited merchants (which accede to communication and security protocols), subscribing users (who perform the m-payment transactions), and may include some

\(^{10}\) Or via web-based Wireless Application Protocol (WAP).

\(^{11}\) NFC is based on radio communication making use of Radio Frequency Identification (RFID) standards.

\(^{12}\) Other modalities may be used, such as electronic checks or digital images of regular checks sent via e-mail.


intermediaries, such as electronic money\textsuperscript{16} issuers and electronic payment service providers.

The concern which inspires the safety to be added to m-payments—that is, two-way communication between the mobile equipment and the tagged end (either an object, or a network)—may turn the mobile phone into a device used for a wide range of applications, ranging from making payments to controlling household facilities to performing identity management.

Once mobile phones include all or most of those features, they may cause a paradigm shift in terms of convenience for their users, necessary for purposes of effectively changing cultural habits.\textsuperscript{17} In fact, credit cards have long been accepted as a payment method, and although m-payments have advantages over credit cards for ensuring a practical way to make small payments and for enabling peer-to-peer direct transactions,\textsuperscript{18} mobile phones are not expected to replace the possession of credit cards unless they convert into a multifunction wallet including a credit card application.

\textbf{C. Legal and Regulatory Implications}

Given that m-payments constitute a matter that pervades various areas of social, economic, and political repercussion, their legal and regulatory implications mirror this wide spectrum.

The relevant issues include privacy, consumer protection, money laundering, tax evasion, by-pass of foreign exchange controls, anti-trust, intellectual property, legal recognition of e-transactions, cybercrime,\textsuperscript{19} and several others.


\textsuperscript{17}Bourreau & Verdier, \textit{supra} note 6.


\textsuperscript{19}“With respect to the state of the regulatory environment, the modus
Most of these issues are intertwined (for instance, privacy and consumer protection, and money laundering and tax evasion), and may be dealt with by the same authorities. Other issues are more closely related to certain regulatory areas (as in the case of anti-trust or intellectual property).

The issues associated with telecommunications and those related to banking have been understood to form a couple of microcosms. The integrated view required by the phenomenon of technological convergence shall include joint consideration of both microcosms (as in the hypothesis of joint ventures between MNOs and banks, encouraged by commingling interests and practices).

Given the novel character of m-payments as a tool for serving a wide array of applications, the frontiers between competent statutory legislation and competent regulatory norms tend to overlap. The same occurs with the frontiers between the competence of different regulatory agencies, such as the Monetary Supervisory Authority and the Central Bank of Brazil, or between the Central Bank and the Telecommunications Authority.

In view of globalized electronic money transfers, payments, and financial services in general, the United Nations Convention on the Use of Electronic Communications in International Contracts (2005) becomes of even greater interest as guidance, and as a possible uniform legislative backbone, in connection with

operandi for agencies is playing catch-up at this point. Cyber crime laws and regulation, especially when it comes to the financial/banking sector, are not moving at the same pace as the technological advancement that has taken place within the past ten years. More and more banking services and transactions are moving away from the physical bricks-and-mortar space to embracing a new business model based on the philosophy of a customer gaining access to and utilizing his or her finances whenever and wherever he or she wants. Mobile banking and in general wireless data transmission appear like a target in the spotlight for cyber criminals.”


legal validity and enforcement of electronic communications associated to m-payments.

I. FINANCIAL INCLUSION\textsuperscript{21} IN BRAZIL

A. Concept and Outreach of Banking Correspondents

Banking correspondents were originally created with the primary purpose of working as payment vehicles that could be accessed by the poor and those in distant localities of a country with huge geographic size and diversity. Thus, from inception, banking correspondents were expected to meet goals of different natures: the public of financial inclusion, and the private goal of an increased “banked” population.

Several examples could be selected to illustrate this dual character. Perhaps the most important of these is given by a multi-purpose\textsuperscript{22} state-owned institution, Caixa Econômica Federal (Caixa), which increased its network of correspondents by 21 percent from mid-2010 to mid-2011 (then reaching 35,900 correspondents), three times its growth of branches in the same period.\textsuperscript{23} Caixa is one of the institutions accredited by the Brazilian Federal Government to channel financial support to social programs such as Bolsa Família,\textsuperscript{24} which helps 11 million families

\begin{footnotesize}
\begin{itemize}
\item\textsuperscript{21} For a discussion regarding the definition of financial inclusion, see FIN. ACTION TASK FORCE, FATF GUIDANCE ON ANTI-MONEY LAUNDERING AND TERRORIST FINANCING MEASURES AND FINANCIAL INCLUSION 12 (2011), available at http://www.fatf-gafi.org/media/fatf/content/images/AML%20CFT%20measures%20and%20financial%20inclusion.pdf.
\item\textsuperscript{22} For a discussion on Caixa’s dual purpose (social and economic), see GETULIO BORGES DA SILVA, CAIXAS ECONÔMICAS: A QUESTÃO DA FUNÇÃO SOCIAL 194 (2004).
\item\textsuperscript{24} Sixty-five percent of those who enjoy Bolsa Familia benefits possess a mobile phone, but only a minority of them have a bank account. Fernando Paiva, Inclusão Financeira, TELETIME, June 2010, http://www.teletime.com.br/6/2010/inclusao-financeira/tt/193052/revista.aspx.
\end{itemize}
\end{footnotesize}
(of monthly per capita income up to BRL70 (US$40), or up to BRL140 (US$80) where children through age 17 are members of the family) with financial aid for schooling, food, and gas. In December 2011, Caixa started testing the adoption of m-payments, and may extend their use to social programs such as Bolsa Família, to implement the Federal Government’s goal of using mobile technologies to improve the reach of social benefits.

This example shows that competition between private banks and public institutions in establishing their network of banking correspondents may be “asymmetrical,” and not free from questioning. Such problem has contaminated the structuring of a split of activities between banks and MNOs regarding the offering of m-payments as well.

Recently, the role of banking correspondents has been enlarged by the Central Bank, which has generated criticism, and shall be evaluated by the Committee on Finance and Taxation of the Chamber of Deputies. The criticism basically refers to the fact that the more banking correspondents are required to work similarly to banks, the less flexibility they have to operate without banking constraints such as shortened daily working hours, increased

---

26 MasterCard has developed application software to be downloaded into smartphones and features phones of subscribers to MNO Vivo, for use in SMS debit transactions for retail purchases. Mariana Mattiuzzo, Caixa Inicia Testes de Pagamentos Móveis, MOBILEPEDIA (Dec. 9, 2011), http://www.mobilepedia.com.br/noticias/caixa-inicia-testes-de-pagamentos-moveis.
30 In the form of Bill of Legislative Decree No. 214/2011.
31 “Although the framework for the use of agents by financial institutions is based on CBB’s regulations, CBB does not have a clear mandate under law to
reporting formalities, and others, which might put at risk the success reached in terms of the number of accredited banking correspondents.

Inclusion of banking correspondents in the chain of mobile payments brings certain issues: would provision of electronic money (for instance, by selling value-stored cards) qualify as a grant of credit, performance of which is allowed only to banks, or would that characterize “consigned stocking” of money? Should the role of banking correspondents be limited, otherwise, to local credit analysis on behalf of the accrediting bank? These questions illustrate the complexity and comprehensiveness of the agenda to be covered by referenced regulation.

B. Payment Systems in Brazil

Brazil is known for having a banking industry which accounts for an advanced technological platform, and has, for more than a decade, provided overnight clearing of checks, real-time electronic transfer of funds, and other state-of-the-art facilities.

This is due to the so-called Brazilian Payments System (SPB), 32 which established a specific network for the flow of electronic messages (National Financial System Network), used by banks, clearinghouses, the Central Bank, and by other supervisory authorities, for money transfers and for processing and clearing of payment orders.

Initially developed during times of high inflation, with particular focus on the fast processing of money transfers, the emphasis of the SPB has, since 2002, shifted towards risk-management 33 and fostering new methods of payment for retail.

regulate outsourcing. The Labor Law therefore has precedence over CBB’s regulations on agents. As a consequence, there are several actions against banks (brought by agents and by bank employee unions) demanding wage equality between bank employees and agents. 37 CONSULTATIVE GRP. TO ASSIST THE POOR [CGAP], UPDATE ON REGULATION OF BRANCHLESS BANKING IN BRAZIL 11 (2010), available at http://www.cgap.org/gm/document-1.9.42396/Updated_Notes_On_Regulating_Branchless_Banking_Brazil.pdf.


33 Louis de Koker points out the need for improvements to the risk-based
In 2008, the system comprised 131 banks, 19,100 bank branches, and 125.7 million bank accounts. The banking chain is complemented by an estimated 160,000 banking correspondents (institutions accredited primarily for performing bill payment services, and which have also been used for conveying loan requests, credit analysis, and other functions).

Also in 2008, efficient credit transfers (same day funds), made available via ATMs, Internet banking, and mobile banking, constituted 44 percent of the total transactions and 85 percent of the total amounts. Comparatively, payment cards (credit, debit, retailer, charge) reached respectively 37 percent and 2 percent, checks 13 percent and 12 percent, and direct debits (automatic, recurring debts) 6 percent and 1 percent.

On the telecommunications side, the number of active mobile accounts reached 245 million in January 2012. Out of the total number of accesses via mobile phones, 81.62 percent were prepaid.

---

approach, which certainly extends to Brazil’s implemented risk-management: “The FATF advises that its risk-based approach enables countries and institutions to further financial inclusion. It is, however, not clear what the FATF means when its [sic] uses the terms ‘risk’ and ‘low risk.’ It is also unclear whether current proposals for financial inclusion regulatory models will necessarily limit money laundering . . . as well as terror financing risks to levels that can be described as ‘low.’” Louis de Koker, Aligning Anti-Money Laundering, Combating of Financing of Terror and Financial Inclusion: Questions to Consider when FATF Standards are Clarified, 18 J. FIN. CRIME 361, 361 (2011), available at http://www.emeraldinsight.com/journals.htm?articleid=1954576&show=pdf.


35 In a comparative table with several countries (Germany, Belgium, Spain, United States, Finland, France, Holland, Italy, Japan, Portugal, Great Britain, Sweden, and Switzerland), credit transfers in Brazil (in 2009) show a high relative weight (49 percent), second only to Switzerland (54.7 percent). BANCO CENTRAL DO BRASIL, DIAGNÓSTICO DO SISTEMA DE PAGAMENTOS DE VAREJO DO BRASIL 10 (2010), available at http://www.bcb.gov.br/htms/spb/Diagnostico-Adendo-2010.pdf [hereinafter CENTRAL BANK DIAGNÓSTICO].


37 Brasil Fecha Outubro com Mais de 231,6 Milhões de Acessos Móveis, AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES (Nov. 18, 2011),
For purposes of reference vis-à-vis the above data, the current total number of inhabitants is about 190 million.\textsuperscript{38}

Change in the portfolio of payment methods used in the country may cause systemic impact, as more attractive payment methods may attract the unbanked population,\textsuperscript{39} increasing the flow of money in the formal economy.

Recent statistics point to substantial change in the popularity level of different payment methods. The period of 2004 to 2008 saw a growth of 129 percent in the number of transactions with debit cards, while the growth in the use of retailer cards was 108 percent, credit cards 101 percent, and direct debits 32 percent.

The impressive growth in the number of debit cards and retailer cards seems to indicate an increasing preference for handy tools that simply make payments and are not associated with credit. This phenomenon apparently favors the future growth of m-payments, as they are an even more convenient tool in this respect.

More recent data, from the period of 2005 to 2010, confirms such trends, as the number of debit card transactions increased 157 percent, while the use of credit transfers grew only 62 percent, and the use of checks decreased 34 percent.\textsuperscript{40}

The potential or actual systemic impact expected from such changes is dependent upon the Central Bank’s competence for providing framework regulation.\textsuperscript{41}

Statutory law\textsuperscript{42} gives the Central Bank exclusive powers to,

\begin{itemize}
\item \textsuperscript{38}In October 2011, the ratio was 118.62 accesses per 100 inhabitants. \textit{Id.}
\item \textsuperscript{39}Probir Roy, \textit{Mobile: Silver Bullet to Target the Non-Banked}, \textsc{The Fin. Express} (Jan. 21, 2010), http://www.financialexpress.com/news/Mobile--silver-bullet-to-target-the-non-banked/569707/.
\item \textsuperscript{40}\textit{Central Bank Diagnóstico}, supra note 36, at 8.
\item \textsuperscript{41}“Unlike legal tender, electronic cash may not be generated by central banks; rather, some of it may circulate outside the Federal Reserve-monitored banking system. Once it is outside that system, it may become ‘untraceable, unmeasurable and, as a result, a threat to economic stability.’” Ellen d’Alelio & John T. Collins, \textit{Electronic Cash Under Current Banking Law}, in \textsc{The Internet and Business: A Lawyer’s Guide to the Emerging Legal Issues} 91, 105 (Joseph F. Ruh Jr. ed., 1996).
\item \textsuperscript{42}Federal Law No. 4.596 (Dec. 31, 1964) (Braz.) (updated on several occasions).
\end{itemize}
among other things: (1) issue paper money and metallic money; (2) render services for providing the financial environment; (3) control every sort of credit; (4) control foreign capital; and (4) supervise financial institutions. Grounded on such attributions, the Central Bank’s by-laws established, in Article 15(VIII), that it shall evaluate risks and impacts of the monetary or exchange policies, as well as immediate or potential systemic impacts which may affect clearing chambers.

Among the aspects deemed systemically material by the Central Bank are fund transfer systems with average daily financial flow higher than 4 percent of the average daily flow of the Reserves Transfer System, or those transfers which may put at risk the fluidity of payments in the context of the SPB.

With regard to possible future popularity of m-payments, a recent survey detected that 71 percent of respondents would consider replacing credit or debit cards with mobile phones, and 66 percent would be willing to use mobile phones to manage bank accounts, while 59 percent were suspicious about the safety of the service, and 15 percent have mentioned fear of suffering mobile phone cloning.

44 Id. at 5 (Art. 11(VI)(q)), 25 (Art. 21(XIV)(f)), 96 (Art. 109-A).
47 This result seems consistent with other research carried out by KPMG, which has indicated that 83 percent of respondents believe m-payments will be the main method of payment within four years. Marcelo Brandão, Pagamentos Móveis Serão “A Bola da Vez”, CONSUMIDOR MODERNO (July 19, 2011), http://consumidormoderno.uol.com.br/parceiros/pagamentos-moveis-ser-o-a-bola-da-vez.
48 Turchi, supra note 46.
C. Mobile Money Policy

In a country where estimates point to 50 percent of salaries being paid in cash and 70 percent of transactions involving “physical” money, there seems to be general consensus on the need for public policies and programs that promote higher social inclusion in mobile banking.

A bill of law was submitted to the Brazilian Congress in 2011 addressing this objective, and the Central Bank has convened financial institutions and defined some basic operational standards (e.g., use mobile line number as standard pattern of identification, establish financial limit for individual transactions, and others), which must be agreed upon by the telecommunications sector and the retail sector in order to be ultimately implemented.

The Central Bank has developed a Financial Inclusion Project, the latest Report of which is dated 2011. The 2009 Report pointed out that, “Mobile banking in Brazil will only reach material role if those who are currently excluded are able to use it for transactions linked to electronic accounts, which, on their turn, shall be of simple access and management,” and that “mobile operators shall establish alliances with banks, or offer, on their own account, services which are not deemed exclusive of banks.”

The 2009 Report lists several actions planned by the Central Bank, which include: (1) clarifying and creating rules for the issuance of pre-paid instruments and electronic money by banks

---

49 Only 30 percent of the adult population possesses bank accounts. CGAP, supra note 31, at 4.


51 This Report is later than CGAP’s study UPDATE ON REGULATION OF BRANCHLESS BANKING IN BRAZIL (see CGAP, supra note 31), which mentioned the lack of an official document outlining the financial inclusion policy.

52 Free translation from Portuguese to English.

and by non-bank entities; (2) requiring interoperability and efficiency of the retail payment systems; (3) providing better regulation on money remittances services; and (4) ensuring greater flexibility for selection of the kinds of institutions allowed to capture deposits. 54

In April 2012 the Central Bank and the Ministry of Communications jointly created a working group aimed to propose guidelines for mobile payment regulation in the country. 55 According to the Central Bank’s officers, the group’s first report was expected to be released in 2012, and will provide general concepts for individual responsibility of companies and regulatory bodies involved in mobile payment processes. The report will leave details such as tariffs to be addressed by eventual regulation, along with rules on security of financial and of non-financial parties, money laundering prevention, and financial inclusion.

D. Integration of Banks, MNOs, Retail, and e-Government Interests

The Central Bank has stated that it considers the lack of interoperability and absence of sufficient cooperation to be the major obstacle preventing effective take-off of m-payments in Brazil. 56

Negotiation between banks, MNOs, and respective supervisory authorities is essential for overcoming this impediment. Today, major banks and major MNOs have their own systems, which are incompatible with one another.

54 “Although prepaid cards may not fall under the definition of deposit (because the prepaid funds may not be repayable), the Banking Law requirement that only CBB-licensed and supervised institutions are permitted to collect funds from third parties is generally viewed as prohibiting nonbanks from issuing e-money or other stored-value instruments, such as electronic accounts stored in mobile phones.” CGAP, supra note 31, at 13.


56 CENTRAL BANK DIAGNÓSTICO, supra note 36.
Therefore, a model where m-payment offerings of each bank work in conjunction with the systems of each individual MNO, and where a banking correspondent has no exclusivity ties with certain banks or MNOs, has been considered fundamental to proliferation of mobile banking in Brazil.57

The first joint ventures formed by banks and MNOs were not the product of mature discussions between interested parties. Such nascent ventures have not been maintained, arguably due to pressures by regulatory or supervisory authorities. These authorities may have considered the initiatives premature, for issues such as the sharing of banking and telecommunications data and eventual commingling of associated statutory seccreies had not yet been discussed or regulated.

More recent joint ventures have had varied scopes and have not yet been subject to scrutiny by supervisory authorities.

Given this context, a bill of law on m-payments may harmonize remaining divergences between banks, MNOs, retail, and government.

II. FINANCIAL INTEGRITY CONCERNS FOR FINANCIAL INCLUSION

A. Money Laundering Concerns

Together58 with terrorism59 and its financing,60 money

57 Lobo, supra note 50.
58 Combat terrorism and money laundering are intertwined, as exemplified by the USA Patriot Act, whose provisions against terrorism are inspired by FATF-GAFI’s Recommendations. AGUSTÍN ZBAR, TERRORISMO INTERNACIONAL Y DERECHOS HUMANOS: APUNTES PARA UNA LEGISLACIÓN ANTITERRORISTA 94 (Fundación Abravanel ed., 1st ed., 2008).
60 A report in March 2008 by the U.S. Bureau for International Narcotics and Law Enforcement Affairs has identified the risk of terrorism financing via m-payments, for instance, through “smurfing,” a technique of making numerous low-value deposits in order to evade detection by law enforcement and
laundering is one of the major m-payments issues affecting financial integrity.

Brazil’s Federal Law 9.613 of March 3, 1998, establishes the legal framework governing money laundering by defining relevant offenses, setting forth preventive measures, outlining a reporting system, and contemplating procedures for international cooperation. It also includes a non-exhaustive list of predicate offenses, such as terrorism and its financing. The contents of such legislation is consistent with a number of international initiatives, such as the Vienna Convention, Palermo Convention, U.N. Convention against the Financing of Terrorism, U.N. Convention Against Corruption, the FATF 40+9 Recommendations, and others.

In the Brazilian Public Administration, anti-money laundering relies on the Council for Control of Financial Activities (Conselho de Controle de Atividades Financeiras, “COAF”), which is a central authority in charge of providing financial intelligence for the system, and on sector-specific authorities (local SEC, Central Bank, etc.) and is responsible for supervising all entities in the banking and financial sectors.

Supplementary Law No. 105 of January 20, 2001, authorized COAF’s access to data protected by banking secrecy, and Federal Law 10.701 of 2003 has established a national registry of bank accounts. COAF belongs to the structure of the Ministry of Finance, and has both policy and operational missions. COAF is in charge of coordinating Brazil’s participation in forums such as FATF, GAFISUD, Egmont Group, and CICAD/OAS, all in accordance with a strategic plan referred to as “ENCLA.” ENCLA congregates all relevant ministries and agencies at Federal and State levels, as well as Congress, Attorneys General, and the Judiciary, as mentioned in COAF’s Management Report of 2011.\(^\text{61}\)

\[^{61}\text{Conselho de Controle de Atividades Financeiras [COAF], Prestação de Contas Ordinárias Anual Relatório de Gestão do Exercício de 2011 16-17 (2012), available at https://www.coaf.fazenda.gov.br/}^\]
Record-keeping, know-your-customer requirements, and suspicious transaction reporting (STR) provisions have been widespread throughout such formal and organizational structure. Newly established Federal Courts specialized in prosecuting relevant cases have enhanced anti-money laundering (AML) efforts.

The definition on AML controls applicable to m-payments requires: (1) new technology capable of tracking transactions and of processing massive extra amounts of data; and (2) sensitive criteria for establishing investigation parameters suitable for a variety of geographic regions, business sectors, and social classes.

The principle of know-your-customer must be complied with by the banking sector as determined by Federal Law No. 9.613, as well as by the telecommunications industry as similarly required by Federal Law No. 10.703 of 2003.

Central Bank’s 2009 Ruling (“Circular”) No. 3.461 consolidated applicable AML requirements, including those regarding banking correspondents.

An example of implemented AML controls in the financial industry has been given by Redecard, a local private company.

62 Today banks are required to keep records of electronic transfers of BRL1,000 (US$600) or higher.
63 Requiring complete data (inclusively, data of people authorized to manage accounts of legal entities): commercial or residential address, phone number, consulted sources of reference, data of account opening, and signature.
64 Name of subscriber, identity card, and serial number and code of the associated mobile phone.
65 Pursuant to the telecommunications regulatory and supervisory authority (Anatel), one year after the entering into force of Law 10.703—which imposed the duty of keeping updated enrollment data on subscribers of prepaid mobile accounts—92 percent of the latter were enrolled. Accuracy of the enrollment data, however, was not sufficiently verified by MNOs. PEDRO AUGUSTO ZANIOLO, CRIMES MODERNO: O IMPACTO DA TECNOLOGIA NO DIREITO 73 (2007).
66 Redecard is present throughout Brazil in every municipality with electricity and telecommunications. It is considered one of the ten largest electronic payments companies in the world and is worth BRL15 billion (almost US$10 billion) in market value. REDECARD, SUSTAINABILITY ANNUAL REPORT 2010 8 (2010), available at http://www.mzweb.com.br/redecard/web/arquivos/
that integrates the SPB and is the leader in credit, debit, and retailer cards services in the market, offering a great number (22) of different “flagships,” as a result of investment in commercial and technical interoperability.

Redecard has launched “Redecard Celular,” a system that enables the use of credit cards in mobile phones, and “Redecard Móvel,” which converts mobile phones into credit card reading machines that has rapidly become a market leader. Redecard has mapped risks all across its operations, and received a B+ rating in the GRI Checked rating system developed by the Global Reporting Initiative. Its Sustainability Yearly Report mentions implementation of compliance with AML laws and regulations and monitoring, analysis, and reporting to COAF regarding transactions entered into via its accredited correspondents.

In fact, current regulation (Central Bank’s Resolution 3954) on banking correspondents establishes accountability of financial institutions for performance by their correspondents: “Section 2. The correspondent operates on behalf and under guidance from the contracting institution, which undertakes full liability for the services rendered before customers and users through the contracted party, which shall ensure integrity, reliability, safety, and secrecy of the transactions ( . . ) as well as compliance with the legislation and regulation applicable to such transactions.”

On February 29, 2012, the local Securities Exchange Commission published a draft adaptation of its rules to the recommendations issued by the GAFI/FATF (CVM Instruction 301/99). Criticism and suggestions from the public were accepted until March 30, 2012, having been submitted by a number of entities. After analyzing these public comments, the local
Securities and Exchange Commission issued Instruction 523/12, amending Instruction 301/99 and incorporating several suggestions.\(^7\)

Furthermore, on March 12, 2012, the Central Bank significantly increased the list of suspicious operations that may constitute money laundering. The new list, contemplated in Normative Letter ("Carta-Circular") 3.542, jumped from 43 kinds of transactions to 106. All listed categories of transactions must be reported to the Central Bank. Such regulation has received criticism by specialists who claim that the list is too broad and its criteria too subjective, leading to comprehensive presumption of illegality.\(^7\)

On that same date, the Central Bank also approved Normative Letters 3.583 and 3.584. Among other provisions, Normative Letter 3.583 determined that financial institutions shall only enter into or maintain business relations with clients that are fully identifiable. Although the Central Bank is not able to regulate institutions abroad, the Normative Letter has also determined that financial institutions shall inform the Central Bank whenever they are unable to comply with the rules provided for in that Normative Letter in any other country.

The other Normative Letter (3.584) has regulated financial institutions that operate in the exchange market through financial institutions located abroad. It has established, among other provisions, that Brazilian banks shall certify that the financial institutions with which they operate abroad actually exist in the objective of identifying the origin of resources," among other suggestions. BSM (BM&F Bovespa - Supervisão de Mercados) suggested several modifications in order to enforce the continuous monitoring of the operations addressed in the regulation. Banco do Brasil suggested terminology changes, such as to replace "clients" with "situations," as well as change of the term for notification to local SEC.


countries where they are incorporated and licensed, and indeed have offices.

B. Tax Evasion Concerns

The ease of entering into “informal” transactions makes m-payment a threat from the tax evasion standpoint.

In Brazil, banking secrecy may be breached upon request by the Central Bank to financial institutions whenever there is suspicion of tax evasion. Suspicion may be indicated by a customer’s statements of transactions in an amount lower than their market value, loans obtained from sources external to the financial system, operations in “tax havens,” expenses or investments exceeding stated available income, remittances abroad through non-resident accounts in amounts which exceed stated available income, and cancellation of taxpayer’s number of legal entities. In addition, the federal Internal Revenue Service has issued Normative Ruling 811/2008, which requires financial institutions to communicate on certain domestic transactions informing deposits, payments, credit orders, and withdrawals.

Main States in Brazil have also developed electronic tax invoicing, which may be instrumental for purposes of tracking tax evasion in m-payments, provided new technologies are created to ensure appropriate monitoring.

C. Foreign Exchange Concerns

Foreign exchange operations conducted by banks, securities brokers, and other institutions in Brazil are subject to control by the Central Bank (after relevant closing by commercial banks is performed) and must report to the federal Internal Revenue Service (envisaging the monitoring on collection of associated taxes over remittances abroad, and over exports or imports).

The Central Bank makes available application software for the

---

closing of the exchange, which facilitates the monitoring activity, and private clearing of exchange is forbidden by applicable regulation.

The definition on financial parameter for tracking m-payments will be an important tool also for the monitoring of infringing foreign exchange operations.

**D. Mandatory Acceptance**

In Brazil, credit cards and checks do not enjoy mandatory acceptance\(^\text{73}\) that is afforded to paper money and coins. 

Although the ease for falsifying paper money and coins is well-known, and may be greater than the perils associated with other means of payment, they seem to enjoy traditional social acceptance at higher levels than credit cards and checks.

Therefore, compulsory acceptance of m-payments shall—at least, at the initial phases of their popularization—be restricted to the government, applying to e-government, social programs, and to other public initiatives.

**E. Consumer Protection Issues**

The Brazilian Supreme Court has decided that banking activities are within the reach of the local Consumer Protection Code, which is a very stringent statute combining strict product liability, contractual protection, and other items of consumer defense.

There has never been any doubt that MNO’s activities are also subject to the Consumer Protection Code.

Given the fact that mobile phones have been compromised by viruses and by other kinds of attacks from hackers or crackers, full disclosure on associated risks is fundamental for meeting the duty of information.\(^\text{74}\) For instance, there is already certain technology


\(^{74}\) Based on the precedent of the lack of adequate disclosure by banks on their web sites regarding security exposures of tokens offered in connection with internet banking, one may expect this to extend to the offering of m-payment
capable of preventing “electronic pickpocketing”\textsuperscript{75} (credit card data—and, possibly, stored electronic money—swiped with contactless scanners from RFID-enabled cards), of which consumers should be made aware.\textsuperscript{76} Unencrypted SMS messages used for m-payments may constitute another source of concern. On the other end, it is important to point out that encryption, authentication, data checking and disclosure, and other means of consumer protection may affect interfacing and user experience, making mobile payment applications less user-friendly.\textsuperscript{77} Therefore, the proper balance must be struck in order to reconcile security and performance goals.

Liability for m-payment services is another topic subject to controversies, as m-payments involve liabilities inherent both to banking and telecommunications, and such merger may produce confusion for those who will be subject to liability. The Local Consumer Protection Code attributes joint liability to all members of the supply chain. If a telecommunications-centered model of m-payments is adopted, should banks be considered liable for ultimately providing funds to a MNO that has commercialized electronic money? Conversely, should interruption of airtime availability by a MNO that has partnered with a bank in a joint venture for selling m-payment services be subject to the bank’s liability in the event airtime is deemed to integrate the financial package of m-payments service? It is important to consider that the systemic impact m-payments will have in the near future may extend liability of m-payment services suppliers across the chain.


\textsuperscript{76} In the event of theft of a mobile phone which had electronic money stored in it, should this be deemed as money theft? Irrespective of whether access to the electronic money is protected with password and other possible (biometric) precautions? This may also be a point of concern regarding the need of proper advice to consumers on how they should react.

Several other matters oppose consumer protection to m-payments, implying a great challenge for applying generic concepts to certain peculiarities of m-payments, which include inverted burden of proof (applicable where consumers are “less knowledgeable” than supplier according to “ordinary rules of experience”), contractual limitation of liability (allowed only where consumer is a legal entity and there is “justifiable situation”), statutory warranty (generically qualified as of “fitness”), duty of care (which may recommend use of advanced electronic signature and certified electronic time-stamping), and right of repent (recognized to sales at distance, and not originally aimed at addressing the offering of electronic money downloading).

III. PERSPECTIVES AND POSSIBLE FUTURE DIRECTIONS

A. Singular Local Environment

The long-standing advanced level of automation in the banking industry in Brazil has implied a two-fold effect: on one side, it has prompted banks and MNOs to cooperate effectively, in the context of implementation of the SPB, generating an interesting tracking record of mutual cooperation; on the other side, it has inspired banks’ and MNOs’ plans to compete for the offering of m-payments services with a greater deal of individual participation and profit. Consumers have already been served with local availability of convenient electronic payment services. This environment has delayed regulation of m-payments in the country, as well as acceptance of joint ventures between banks and MNOs to exploit such market.

Recent initiatives have touched m-payment issues, as in the case of securities home-brokering. Broker Ágora has announced

---

78 According to some authors, the more electronic money resembles paper money, the more consumers’ liability for cautious possession of currency shall apply. See Teresa Rodríguez de Las Heras Ballell, El Reparto de Riesgos y la Atribución de Responsabilidad en el Uso de Tarjetas en la Contratación Electrónica, in DERECHO DE LAS NUEVAS TECNOLOGÍAS 319, 364 (Mariliana Rico Carrillo ed., 2007); d’Alelio & Collins, supra note 41, at 103.
that consumers may make withdrawals and transfers via mobile phones and smartphones in its portal.\textsuperscript{79} This is in line with the local SEC’s Instruction 505/2011,\textsuperscript{80} which regulates electronic customers’ enrollment and payment methods, in connection with securities brokerage.

Despite delayed introduction of m-payments in the country, a number of business alliances between banks, MNOs, and high-technology companies have rapidly grown, bringing different options of products and services to the market.\textsuperscript{81} Such developments have coincided with submission to the Congress of the first bill of law on m-payments.

**B. The Bill of Law at the Congress**

The bill of law purports to create STDM, a system of payments and transfers via mobile devices, and to establish the role of a clearinghouse and of services suppliers, which is to be further regulated by the monetary authority. It clarifies the intended scope by excluding Internet banking accessed via mobile phones from its reach.

The legal entities authorized to offer mobile payment services will have such activity as their sole corporate purpose, and will depend upon license from competent authority to operate.

Such legal entities will maintain individual electronic accounts associated with a number of mobile phone accounts, to which the


\textsuperscript{80} In effect since April 2, 2012.

\textsuperscript{81} Oi Paggo has provided SMS m-payments and recharge, separate from Oi’s airtime invoices; Cielo has offered a “plug” (Square Card Reader) to be connected to an iPhone, iPad, or iPod, for any person to receive payments made via credit card, upon a fee of 2.75 percent per transaction, without monthly fees, and being the amounts deposited in the user’s account on the following day; MasterCard’s NFC-based PayPass has been used in trial tests in Rio de Janeiro; Visa’s PayWave was launched, associated with Bradesco bank and Nokia mobile phones for contactless payment at merchants such as Starbucks, as well as Visa’s Mobile Pay, in association with Banco do Brasil, for payment via mobile of credit card and debit card; Buscapé Company has introduced DinheiroMail, apportioning electronic clearing of credits and expenses; Wappa has presented WappaTaxi for m-payment of transportation services.
user shall make deposits in order to be able to: acquire credits for use of the mobile phone; make payments; make transfers to other electronic accounts; make transfers to bank accounts held by the user; and make withdrawals before accredited establishments. Grant and possession of the electronic accounts may not be remunerated.

The legal entities may intermediate the offering of financial services such as credit, financial investments, insurance, and others to clients, and will be liable to the customers for the services they provide.

The clearinghouse will settle transactions on a real-time basis, and will be in charge of accrediting the establishments where money withdrawal may be available. It will be set up as a nonprofit private entity, and integrate the SPB.

The monies deposited by users in the electronic accounts will be maintained in accounts and financial investments within the National Financial System (SFN), and will not be considered as assets belonging to the legal entities that provide mobile payment services. The latter will own the earnings derived from investing referenced monies. Such operations shall be regulated and monitored by the monetary authority.

The justification of the bill of law mentions the objective of financial inclusion, pointing out that the banking system has high costs, bureaucracy, and limited geographic distribution. It emphasizes that legal entities allowed to offer mobile payment services may be subsidiaries of banks or of MNOs, and will contribute to expansion of the financial system and of convenience to users, who will be able to use mobile phones to make and receive payments. It also highlights the goals of reducing overall costs of the financial system, diversifying payment methods, and increasing competition in the offering of financial services by providing a low-cost alternative to credit and debit cards and enhancing security and efficiency.

CONCLUSION

Most business initiatives launched in the Brazilian territory demonstrate certain alliances between banks and MNOs, indicating
market assumption that this hybrid model better fits the local environment.82

Consultancies hired by the National Association of Banks (Febraban) and the IFC’s Report have also suggested that this kind of alliance should be especially recommended.83

The precedent of standardized procedures in SPEC upon cooperation between banks and MNOs, and legal constraints which require segregated management of the duty of secrecy and of exclusive activities, tend to drive efforts towards the solution set forth in the bill of law, that is, of a highly efficient (real-time settlement) clearinghouse and legal entities responsible for providing mobile payment services, being backed by solid controls in effect within the SFN.

Taking into account the dimension of Brazil’s market and targeted population, as well as the complexity and potential outreach of its banking and telecommunications industries, local legislators may prefer to await the outcome of initial private business initiatives and of preliminary administrative regulations in order to determine the best course of action for the normative process.

The impressive network of banking correspondents may be used in conjunction with providers of mobile payment services, possibly as accredited establishments for money withdrawals.

A virtual clearing system of mobile payments, coupled with regular banking structures, may be the solution selected by Brazil to implement mobile payments.


83 For further discussion, see id. at 34.
SAFARICOM AND M-PESA IN KENYA: FINANCIAL INCLUSION AND FINANCIAL INTEGRITY

Mercy W. Buku and Michael W. Meredith *
© Mercy W. Buku and Michael W. Meredith

Cite as: 8 WASH. J.L. TECH. & ARTS 375 (2013)
http://digital.law.washington.edu/dspace-law/handle/1773.1/1204

ABSTRACT

The recent and widespread availability of affordable mobile phone technology in developing countries has paved the way for the development of a number of mobile money and electronic remittance services. One of the most successful of these services is Safaricom’s M-PESA program, launched in the East African nation of Kenya in March 2007. Since then, the program has successfully enrolled 15.2 million users, transferred more than US$1.4 trillion in electronic funds, and contributed significantly to poverty alleviation and financial inclusion efforts in rural

* Mercy W. Buku, LLB Hons (University of Nairobi 1988), Dip Law (Kenya School of Law 1989); Advocate of the High Court Kenya, Commissioner for Oaths and Notary Public, ACIB (U.K.), CPS(K), CAMS (U.S.A.); Senior Manager Money Laundering Reporting Office Safaricom Limited, Kenya. Many thanks to Michael Meredith, Research Assistant, University of Washington School of Law for his tremendous contribution in researching and co-authoring this paper, to Professor Jane K. Winn, University of Washington School of Law, Brian Muthiora, Principal In-House Counsel Safaricom Limited, Louis de Koker, Professor of Law, Deakin University School of Law, Melbourne, Australia, and Laura Powell, student editor, University of Washington School of Law, for their invaluable input in critiquing and editing the paper.

Michael W. Meredith, University of Washington School of Law, J.D., 2012. Thank you to Mercy Buku for the opportunity to work with her on this piece and to Professor Jane K. Winn for her extraordinary mentorship and support.

This Article was presented at the Mobile Money in Developing Countries: Financial Inclusion and Financial Integrity Conference held in April 2012 at the University of Washington School of Law with the support of the Linden Rhoads Dean’s Innovation Fund.
Kenya. This Article seeks to trace the development of M-PESA in Kenya, provide a snapshot of the Kenyan implementation of and experience with the program, and consider the role that services like M-PESA might play in national and international anti-money laundering and counter-terrorist financing efforts.

TABLE OF CONTENTS

Introduction .................................................................377
I. Know Your Customer, Know Your Country: Kenya’s Demographics and the State of Financial Inclusion Prior to the Development of M-PESA ...........................................380
   A. The Kenyan Demand for Remittance Services:
      Kenya’s Pattern of Urbanization and the “Dual System” .................................................................380
   B. Challenges Faced by Kenya’s Financial Service Providers in Meeting the Kenyan Consumer’s Demand for Remittance Services ...........................................382
   C. Confidence in Safaricom and the Ubiquity of Mobile Phones in Kenya ...........................................383
   D. Kenya’s Consumer Profile ......................................384
II. M-PESA’s Pilot Program ........................................384
   A. The Players: the Role of Vodafone, Safaricom, the United Kingdom, and the Kenyan Government in M-PESA’s Pilot Program ...........................................385
   B. Implementation of M-PESA’s Pilot Program ..........386
   C. Lessons from the Pilot ..........................................388
III. M-PESA Launch and Measuring the Program’s Success in Kenya .................................................389
   A. The Rate and Sustained Growth of Customer Registration .................................................................389
   B. The Growth of M-PESA Retail Agents in Kenya ......390
   C. Volume of e-Money Transactions .............................................390
   D. Expansion of Services ..........................................391
   E. Financial Independence for Rural Communities and Female Empowerment ...........................................392
IV. Future Challenges: Anti-Money Laundering and Counter-Terrorist Financing Regulations Implicating M-PESA ......394
A. The Application of Traditional Kenyan Banking Law to Mobile Money .......................................................... 394
B. The CBK’s Electronic Payment Guidelines and Sector-Specific Regulations ........................................................ 395
C. Compliance With and Voluntarily Imposed AML Programs in Mobile Money ............................................. 396
   1. Staff and Agent Training for M-PESA Providers ................................................................. 397
   2. Identity Verification and “Know Your Customer” Procedures in M-PESA ...................................... 397
   3. Transactional Controls ............................................................................................................. 398
Conclusion ............................................................................................................................................. 399

INTRODUCTION

“The adoption of mobile phones has occurred at perhaps the fastest rate and to the deepest level of any consumer-level technology in history.”¹ The fixed line telephone—the predecessor to mobile phones—took 100 years to reach only 80 percent of the population, even in developed countries.² Meanwhile, mobile phones have been adopted “more than five times as fast”³ worldwide, and have significantly decreased communication costs in many parts of the developing world.

Nowhere is the benefit and impact of widely available mobile phone technology more apparent than in Africa, “where [alternatives to mobile phones such as] networks of both fixed line communication and physical transportation infrastructure are often inadequate, unreliable, and dilapidated.”⁴ The adoption of mobile phone technology “in Africa has increased from 3 percent in 2002 to 51 percent today, and is expected to reach 72 percent by 2014.”⁵

² Id. at 3.
³ Id. at 2-3.
⁴ Id. at 2.
As a result, affordable access to mobile phone technology has allowed a number of African nations to “leapfrog the [line] en route to 21st century connectivity.”

However, the positive impact of the adoption of cellular technology has not been limited to the communications or information technology sectors of developing countries. In fact, the successful development of mobile money services in Kenya provides a unique and interesting case study of how access to mobile phones can revolutionize and democratize the financial and banking industries of developing nations.

Currently, there are more Kenyans who own a mobile phone than have access to a bank account. In this respect, Kenya is not an exceptional case. Worldwide, only “one billion of the world’s 6.5 billion people have bank accounts . . . yet about three billion have mobile phones.” This global lack of access to financial services, combined with the increasingly widespread use of mobile phones, has given rise to an informal practice of using mobile phones as an alternative to traditional banking systems. Mobile phone users can transfer funds to other users through pre-paid mobile phone credits sent via short message service (SMS) communication. Upon receipt, these credits are exchanged for cash or traded for goods and services in a type of informal, mobile phone based economy that provides basic financial services to otherwise unserved or unbanked populations.

Seeking to improve and formalize this funds-transfer system, Safaricom—Kenya’s leading mobile service provider and an affiliate of the Vodafone Group—launched its M-PESA service. M-PESA, short for mobile money, is an SMS-based money transfer system that allows individuals to deposit, send, and withdraw funds using only their mobile phones. In the M-PESA system, Safaricom accepts cash deposits from customers who are


6 Jack & Suri, supra note 1, at 2.


8 Pesa is Swahili for money.
registered M-PESA users. In exchange for their deposits, users are issued “e-float” or “e-money” that is held in the user’s electronic account. The e-money issued is a shilling-for-shilling representation of actual deposited cash, which is held in trust. E-money can then be transferred, used to pay for goods and services, or withdrawn.

After its launch in 2007, the M-PESA program grew rapidly and reached approximately 65 percent of Kenyan households by the end of 2009. The program provided desperately needed access to reliable financial services and markedly improved the economic productivity of many impoverished communities throughout Kenya. As a result, the program was widely viewed as a model of success to be emulated across the developing world. However, the unique and uncontested success of M-PESA as a financial inclusion and poverty alleviation program in Kenya has been difficult to replicate in other developing nations.

This Article seeks to: (I) analyze relevant demographic information concerning the population of Kenya that might shed light on the financial needs of Kenya’s consumers and provide explanations for the extraordinary success of Kenya’s M-PESA

---


10 Id. ("Registration and deposits are free and most other transactions are priced based on a tiered structure to allow even the poorest users to be able to use the system at a reasonable cost. Transaction values are typically small, ranging from USD 5 to USD 30."); Mas & Radcliffe, supra note 5, at 170 ("[Retail] stores are paid a fee by Safaricom each time they exchange [cash for M-PESA credit] on behalf of customers.").

11 Jack & Suri, supra note 1, at 5 ("The average number of new registrations per day exceeded 5,000 in August 2007, and reached nearly 10,000 in December that year . . . [b]y August 2009, a stock of about 7.7 million M-PESA accounts had been registered. There are now about 23,000 agents, and data from late 2009 indicated that even by then more than two-thirds of Kenyan households had at least one member who used the service.").

program; (II) trace the development of M-PESA in Kenya since its inception in 2003; (III) provide a snapshot of Kenya’s implementation of the M-PESA program to date; and (IV) discuss some of the future challenges facing M-PESA, including the role that M-PESA and Safaricom might play in international anti-money laundering and counter-terrorist financing efforts.

I. KNOW YOUR CUSTOMER, KNOW YOUR COUNTRY: KENYA’S DEMOGRAPHICS AND THE STATE OF FINANCIAL INCLUSION PRIOR TO THE DEVELOPMENT OF M-PESA

Although the success of M-PESA in Kenya is unprecedented and attributable largely to Safaricom’s innovative business model and marketing strategy, some have suggested that M-PESA’s effectiveness was enhanced due to the demographic characteristics of the Kenyan consumer and Kenyan society that existed prior to M-PESA’s launch.\(^\text{13}\) Therefore, the state of affairs that gave rise to M-PESA’s success and inspired its development is worthy of brief consideration here.

A. The Kenyan Demand for Remittance Services: Kenya’s Pattern of Urbanization and the “Dual System”

The term “dual system” is used to describe the continued connection that urban migrants maintain with their rural homes and villages, despite spending a significant amount of time living or working in urban centers.\(^\text{14}\) The reasons for these sustained connections are multifold and include their ability to “ease the transition to urban life.”\(^\text{15}\) However, the explanation for these strong urban-rural connections that most concerns this Article is a financial one. Due to the severe disparity between urban and rural

\(^\text{13}\) See, e.g., Mas & Radcliffe, supra note 5.


\(^\text{15}\) Id.
wages, many laborers and household breadwinners migrate from rural centers to urban areas without their families in search of more lucrative employment opportunities. As a result, many rural households rely on remittances from urban centers for survival; the two societies become interconnected as a matter of economic necessity.\footnote{Id.}

Kenya provides a particularly compelling example of this “dual system.” In Kenya, “30 percent of households . . . depend on remittances for their survival,”\footnote{Id.} and over 78 percent of Kenya’s population lives in rural households. As such, Kenya’s consumer market expressed a meaningful demand for urban-to-rural remittance services prior to the implementation of M-PESA. In fact, some have suggested the urban-to-rural population ratio in Kenya struck a serendipitous balance that generated the largest possible demand for the domestic remittance services offered by M-PESA.

A recent study of demand patterns for remittance services in developing nations suggests “the potential market size for domestic remittances is related to urbanization ratios. More propitious [domestic remittance] markets will be those where the process of rural-urban migration is sufficiently rooted to produce large migration flows, but not so advanced that rural communities are hollowed out.”\footnote{Amrik Heyer & Ignacio Mas, \textit{Seeking Fertile Grounds for Mobile Money} 5-6 (Bill & Melinda Gates Found., Working Paper, 2009), available at http://mmublog.org/wp-content/files_mf/fertile_grounds_mobile_money.pdf.} Kenya’s history, culture, and public policy have functioned together to establish and maintain this demand-producing urban-to-rural population ratio. During Kenya’s colonial period, policies were implemented in the hopes of preventing the establishment of permanent urban centers. For example, in urban areas, labor was only recruited for temporary periods, wages were kept low, and only small accommodations not suitable for family living were available. As a result, “migrant workers would oscillate between . . . urban and rural area[s] throughout their working life.”\footnote{Morawczynski, \textit{supra} note 14, at 4.}
Kenya’s post-colonial government reversed these policies and sought to jumpstart economic development through a nation-wide program of urbanization. Subsequently, urban wages and the number of permanent residents in urban areas significantly increased. The impact of these policies was, however, muted due to the significant and sustaining links maintained by urban workers to their rural homes and rural communities. As explained by a number of scholars in the area, “In Kenya, migrants’ ties with [their] rural homes [are especially strong due to] an ethnic . . . conception of citizenship . . . expressed through burial, inheritance, cross-generational dependencies, social insurance, and other ties, even in cases where migrants reside more or less permanently in cities.”

Despite government policies seeking to increase urbanization, there was not an unsustainable drain of workers from rural areas to urban centers in Kenya. Instead, migrating workers continued to send funds to their rural homes and support the rural communities that they left in search of employment. This cultural phenomenon is not unique to Kenya. In fact, a strong tie to rural homes is part of the community spirit embodied in many African cultures. Nevertheless, there exists an especially strong demand for domestic remittance services in Kenya, due to its history, culture, and pattern of population growth.

B. Challenges Faced by Kenya’s Financial Service Providers in Meeting the Kenyan Consumer’s Demand for Remittance Services

Prior to Safaricom’s M-PESA launch, Kenyans had a number of options for local remittance services. These services included “commercial banks, post offices, forex bureaus, bus companies, and friends and family.” Almost all of these options, however, were either unavailable to the majority of Kenya’s consumers or were extremely unreliable and insecure.

The most commonly used remittance services—informal friend

---

20 Mas & Radcliffe, supra note 5, at 173.
21 Morawczynski, supra note 14, at 2.
and family networks and courier services provided by Kenya’s bus companies—risked the potential of lost or stolen funds and, occasionally, required the payment of prohibitively high fees. 22 Similarly, the Kenyan postal service, although traditionally a popular method for transferring funds to rural communities, “is perceived by customers as costly, slow, and prone to liquidity shortages at rural outlets.” 23

Finally, the ability to transfer funds through a commercial bank is substantially impaired by the fact that only an extreme minority of rural Kenyans has access to a bank account with which to receive remitted funds. Therefore, even with a number of remittance services available to them, most Kenyans experienced “service gaps, inefficiencies, and unmet demand, particularly among the low-income population.” 24

C. *Confidence in Safaricom and the Ubiquity of Mobile Phones in Kenya*

The development and implementation of a new payment system, such as M-PESA, is generally faced with a number of financial, cultural, and logistical challenges, not least of which is attracting users to the service and ensuring that they will trust their money to a previously unknown and untested commercial entity. At least in this area, Safaricom had a head start prior to M-PESA’s commercial launch.

Established in 2000 with 17,000 customers and only 50 employees, Safaricom has grown into one of the most accessible and well-recognized brands in Kenya. Today, Safaricom employs over 3,000 individuals and offers services to more than 16 million customers. In Kenya, almost 83 percent of the population who are fifteen years or older have access to a mobile phone 25 and Safaricom is responsible for a significant portion of that

22 Id. at 10.
penetration. Safaricom controls nearly 80 percent of the mobile phone market, placing it significantly ahead of its nearest rivals: Airtel, Yu, and Orange.26 As a result, even before the launch of M-PESA, Safaricom had developed meaningful brand recognition and trust with Kenya’s consumers upon which to build its remittance service.

D. Kenya’s Consumer Profile

Of course, there are a number of other factors relevant to the viability of financial inclusion services, such as M-PESA, in Kenya. One important factor is the demographic character of Kenya’s consumer population. It is relevant to note that Kenya is home to approximately 39 million people, which is about average for an African nation. Therefore, Kenya can serve as a useful model for other countries in this regard. However, Kenya is a relatively young country; over 42 percent of its population is under the age of fourteen. It is also important to note that more than 85 percent of Kenya’s population is literate and has had experience with mobile phone technology. The majority of Kenyans would most likely be able to adjust to using M-PESA’s text message services without much difficulty. Finally, an important aspect of Kenya’s population is its level of employment. Although 17.94 million individuals are included in Kenya’s labor force, the nation still counts nearly 40 percent of its citizens as unemployed. As a result, Kenya maintains a relatively high poverty level. Thus, for any financial service to be successful in Kenya it must not exclude a significant portion of the country’s consumers by being prohibitively expensive.

II. M-PESA’s Pilot Program

Taking these factors into account, Safaricom first launched M-PESA in Kenya as part of a six-month pilot program conceived and developed cooperatively between a number of public and private entities. The following section seeks to: (A) identify the

26 Id. at 5.
important corporations and governmental agencies involved in M-PESA’s pilot program, (B) explain how the M-PESA pilot program was implemented in Kenya, and (C) mention a few of the lessons learned as the pilot progressed.

A. The Players: the Role of Vodafone, Safaricom, the United Kingdom, and the Kenyan Government in M-PESA’s Pilot Program

M-PESA was conceived of at the 2003 World Summit for Sustainable Development, when the United Kingdom’s Department for International Development (DFID) approached a representative of Vodafone.27 The U.K. DFID was convinced that private organizations did not invest more heavily in international poverty alleviation efforts because poverty alleviation programs generally require a significant initial investment, but often fail to generate financial returns commensurate with that investment. Thus, the DFID believed that if the amount of money necessary for a program’s initial investment could be sufficiently reduced, poverty alleviation might become a profitable endeavor that would unleash the creative energies and logistical resources of some of the U.K.’s largest companies, such as Vodafone. Following this line of reasoning, the U.K. DFID developed an innovative use for the U.K.’s “challenge funds” intended to achieve the United Nations’ Millennium Development goal of reducing poverty by 50 percent by 2015: subsidizing the investment of private companies in poverty alleviation efforts.

Putting its ideas into action, the U.K. DFID proposed a number of public-private partnerships to Vodafone in which private poverty alleviation efforts in African nations, such as Kenya, would become more financially attractive to investors by using the U.K.’s “challenge funds” as a subsidy.28 One of the DFID’s proposed partnerships eventually resulted in M-PESA. Vodafone

---

28 Id.
won the bid to head up the DFID’s program and soon after partnered with the Safaricom team in Kenya to implement the M-PESA service.

Safaricom is a publicly traded company registered on the Nairobi Stock Exchange, but was supported by the Kenyan government during its development of M-PESA. Following a financial access survey conducted in 2006, which indicated very low levels of access to financial services throughout the country, the Central Bank of Kenya (CBK) announced its commitment to exploring “all reasonable options for correcting the [financial] access imbalance” and began to work closely with Vodafone and Safaricom to ensure the success of M-PESA. Perhaps the CBK’s largest contribution to the pilot program was simply recognizing that pre-mature regulation of programs like M-PESA might stifle the industry’s growth. As a result, the CBK imposed almost no regulatory safeguards on the M-PESA pilot program.

B. Implementation of M-PESA’s Pilot Program

The M-PESA pilot program in Kenya, headed by Vodafone and Safaricom, officially began on October 11, 2005. The pilot consisted of eight agent stores in three geographically disperse locations: the Nairobi Central Business District (a well-developed urban center), Mathare (a slum about 8 kilometers out of the center of town), and Thika (a rural market town approximately 32 kilometers out of the city).

Initially, M-PESA was conceived of as a means for microfinance institutions to disburse loans to their customers and to enable those customers to make loan repayments using their mobile phones. As a result, Vodafone partnered with Faulu Kenya, a local micro-finance institution that provided microloans to individual consumers and small business owners who would repay their loans, generally, by a few dollars every week. Five hundred Faulu Kenya clients were enrolled in the pilot program, provided

29 Mas & Radcliffe, supra note 5, at 173.
30 Id.
31 Int’l Fin. Corp., supra note 9, at 10.
32 Hughes & Lonie, supra note 27, at 70.
with M-PESA-ready phones, and instructed on how to use them to repay their loans (their incentive for accepting the deal was a free phone and a few dollars placed in their M-PESA account).\textsuperscript{33} As the pilot progressed, the trial participants recognized and explored the potential of the M-PESA service. As one Safaricom representative noted:

Aside from the standard loan repayments for which we had designed the system, we observed several other applications: People repaying the loans of others in return for services; Payment for trading between businesses; Some of the larger businesses using M-PESA as an overnight safe because the banks closed before the agent shops; People journeying between the pilot areas, depositing cash at one end, and withdrawing it a few hours later at the other; People sending airtime purchased by M-PESA directly to their relations up country as a kind of informal remittance; People outside the pilot population being sent money for various ad hoc reasons[,] for example, one lady’s husband had been robbed, so she sent him M-PESA to pay for his bus fare home; People repaying loans in return for cash on behalf of a few colleagues who hadn’t mastered the use of the phone—or simply sold it.\textsuperscript{34}

Based on this expanded use of the service and the demand from those outside the program to be involved, Safaricom expanded the pilot services by allowing users to purchase prepaid airtime at a 5 percent discount if purchased with their deposited M-PESA e-money. Not only did trial participants take advantage of the service but “a number of customers [set] up as informal airtime resellers as a side business.”\textsuperscript{35}

Six months later, on May 1, 2006, the pilot ended. Its success can be measured, in part, by the fact that “many trial users

\textsuperscript{33} Id. at 74.
\textsuperscript{34} Id. at 76.
\textsuperscript{35} Id.
continued to transact on the system after [the pilot concluded]."\(^{36}\)
The pilot did present, however, a number of stumbling blocks and lessons for the full launch.

\[C. \text{ Lessons from the Pilot}\]

The first lesson that became clear from the M-PESA pilot was that it would not primarily be used as a means to repay microloans. In fact, Safaricom’s partnership with Faulu Kenya generated more unnecessary complications than benefits to the consumer. “Many of their reconciliation methods were manual and paper based and reconciling M-PESA transactions in parallel with their existing systems only seemed to add complexity and additional work for Faulu back-office staff. Furthermore, Faulu was not able to maintain a stable [I]nternet connection.”\(^{37}\) Therefore, “Safaricom decided to proceed with a full commercial launch of the service without [their] microfinance capabilities.”\(^{38}\)

Additionally, agents involved in the pilot program were initially hesitant to pay out physical cash based solely upon an M-PESA text message. In order to assuage these insecurities for the full launch, agents were given individual M-PESA cash float accounts and reassurances from Safaricom’s head offices.

Finally, “consumer training was quickly identified as being probably the biggest challenge” to a countrywide implementation of M-PESA.\(^{39}\) Individuals that were not familiar with mobile phones needed significant training in order to navigate a mobile phone’s menu system and the M-PESA application in particular. Additionally, although many Kenyans were English-speaking, some, especially those in the rural areas, spoke primarily Swahili and other tribal languages. Thus, for the full rollout, Safaricom had to condense these languages that are not as compact as English, to no more than 160 characters for an SMS message to achieve optimal levels of customer registration in rural areas.\(^{40}\) As a result

\(^{36}\) Int’l Fin. Corp., supra note 9, at 10.
\(^{37}\) Id. at 4.
\(^{38}\) Id.
\(^{39}\) Hughes & Lonie, supra note 27, at 74.
\(^{40}\) Id. at 72-73.
of these efforts, all customer communications are currently in both English and Swahili.

III. M-PESA LAUNCH AND MEASURING THE PROGRAM’S SUCCESS IN KENYA

In addition to addressing the problems presented during M-PESA’s pilot program, M-PESA’s full launch would also have to overcome the adverse network effects that plague the implementation of nearly every new payment system. In order to overcome these obstacles, prior to the 2007 launch, Safaricom made a number of “significant up front investment[s]” in the product, including opening 750 M-PESA providers nation-wide and ensuring at least one M-PESA agent was available in each of Kenya’s 69 districts.41 Further, in order to cement trust and familiarity with the brand, Safaricom began a nationwide advertising campaign that included television and radio spots as well as traveling roadshows that provided customer training in the use of mobile phone technology and the M-PESA service.

The launch was described as a “massive logistical challenge that led to a great deal of customer and store confusion and, in the first months . . . several days’ delays to reach customer service hotlines.”42 Yet the gamble paid off and within one month Safaricom had registered over 20,000 customers for the M-PESA service.43 Since the launch of the service, about 15 million new customers have signed up and used it to transfer over US$1.4 trillion. As a result, M-PESA’s launch in Kenya has been universally hailed as a success based upon almost any meaningful vector of comparison.

A. The Rate and Sustained Growth of Customer Registration

One indication of M-PESA’s success is the sheer number of Kenyans who have chosen to register for the service despite other

41 Mas & Radcliffe, supra note 5, at 178.
42 Id.
43 Hughes & Lonie, supra note 27, at 63.
remittance services available to them. Between March 2007 (the
date of the program’s full launch) and May 2008, over 2 million
customers registered; and the number of customers “reached the 10
million mark in just over three years [after the service was
launched].” As of December 31, 2011, the reported number of
active M-PESA customers has topped 15.2 million. Currently, out
of Safaricom’s 17 million subscribers, 15.2 million (90 percent)
are registered for M-PESA, which is 63 percent of the adult
population in Kenya. These numbers reflect M-PESA’s
outstanding success as a mechanism of financial inclusion.

B. The Growth of M-PESA Retail Agents in Kenya

The number of M-PESA retail agents in Kenya has grown
almost as quickly as the number of M-PESA clients. During the
first year of service, despite Safaricom’s significant initial
investment in new M-PESA locations, the growth of agents lagged
behind the demand created by an expanding customer base. This
result, however, was partially by design. Since “store revenues are
dependent on the number of transactions they facilitate, Safaricom
was careful not to flood the market with too many outlets, lest it
depress the number of customers per agent.” As of December 30,
2011, the number of M-PESA retail agents has expanded to meet
customer demand and there are now over 35,500 M-PESA agents
in such diverse sectors as supermarkets, fuel stations, and
Safaricom dealers. In fact, there are now “over five times the
number of M-PESA outlets [in Kenya] than the total number of . . .
post offices, bank branches, and automated teller machines
(ATMs).”

C. Volume of e-Money Transactions

Another important measure of M-PESA’s success is the
amount of money transferred through its e-money system. Over
two million transactions are conducted over M-PESA every day.

44 Mas & Radcliffe, supra note 5, at 170.
45 Id. at 179.
46 Id. at 170.
That number constitutes 90 percent of all mobile money transactions in Kenya and 70 percent of all non-cash financial transactions. Cumulatively, these transactions amount to more than US$4.98 billion transferred per year, which accounts for 17 percent of Kenya’s gross domestic product. Over its five-year history, Safaricom’s M-PESA has moved more than US$1.4 trillion in peer-to-peer (P2P) transactions. As a point of comparison, M-PESA “processes more transactions domestically than Western Union does globally.”

It is important to note, however, that M-PESA has not replaced banks in Kenya. In fact, although some traditional banks initially resisted Safaricom’s implementation of M-PESA, many have recently developed partnerships with Safaricom to offer the M-PESA payment solution to their customers via their own mobile banking platforms. Nevertheless, the volume of transactions effected between banks under the Real Time Gross Settlement (RTGS) method is nearly 700 times the daily value transacted through M-PESA. On the other hand, the average mobile transaction is about a hundred times smaller than the average check transaction (Automated Clearing House, or ACH), and just half the size of the average ATM transaction.

**D. Expansion of Services**

Since its launch, M-PESA has also expanded beyond its initially conceived role as a money transfer service that might facilitate microloan repayment. The first notable new service was announced when Safaricom partnered with Pesa Point, one of the largest ATM service providers in Kenya, and allowed its users to make a withdrawal from their M-PESA account at any ATM. This service provided more convenience to consumers who needed to

---

47 Id. at 169.
49 Id.
make a withdrawal after M-PESA’s agents have already closed or from an agent who did not have enough currency on hand to fulfill a withdrawal request.

In 2009, Safaricom expanded M-PESA’s services again when it launched its pay bill service. At least “75 companies [began to use] M-PESA to collect payments from their customers. The biggest user is the electric utility company, which now has roughly 20 percent of its one million customers paying through M-PESA.”\(^5^0\) Since then, Safaricom has partnered with 25 banks and over 700 businesses to facilitate fund deposits, bank transfers and the regular payment of utility bills, insurance premiums, and loan installments, and more recently, since November 2012, M-PESA subscribers are now able to open interest earning bank deposit accounts electronically through their phones. The accounts are funded by transfer from the subscribers’ M-PESA accounts and attract varying rates of interest. The subscribers will also be able to borrow against funds held in their bank accounts.

Other notable services now offered through M-PESA also include: the ability to purchase airtime for Safaricom’s cellular service, the ability to use e-money to purchase goods and services at M-PESA partner outlets, international money transfer services currently offered in partnership with Western Union, M-Ticketing, M-PESA prepaid Visa cards, promotional cash prize payments, dividend payments, the ability to make charitable contributions, the transfer of Loyalty Points, and the ability to use M-PESA as a fundraising tool. The final category, M-PESA as a fundraising tool, deserves special attention following the recent success of the Kenyans for Kenya Famine Relief Initiative spearheaded by Safaricom and other businesses. The fundraiser raised KES678 million (US$8.5 million), of which KES170 million (US$2.1 million), or about 25 percent, was contributed through M-PESA.

\( E. \) Financial Independence for Rural Communities and Female Empowerment

Of course, M-PESA was not developed solely as a

\(^5^0\) Mas & Radcliffe, supra note 5, at 171.
moneymaking enterprise. In fact, at inception, its explicit purpose was to help achieve the United Nation’s Millennium Development Goals. Thus, another measure of M-PESA’s success is the manner in which it has helped reduce the impact of poverty for women and children in rural Kenya.

Since M-PESA allows the safe transfer and storage of money, rural Kenyans no longer need to make lengthy trips to urban areas to make monthly payments for basic services, such as light or heat. This saves not only time that would otherwise be directed toward economically productive activity, but also money (on average US$3 per transaction) that can be more usefully spent on food and placed into long-term savings.

M-PESA also has the potential to increase net household savings by “facilitat[ing] inter-personal transactions [that] improve the allocation of savings across households and businesses by [improving] the person-to-person credit market [and] . . . increas[ing] the average return to capital [in that market] . . . producing a feed-back to the level of saving.” 51 Whether this has actually resulted is up for debate: “While some customers use M-PESA as a savings device, [the service] still falls short of being a useful [method of savings] for most [of Kenya’s] poor.”52 As of 2009, the average savings balance of an M-PESA account was around US$3.53

Nevertheless, because M-PESA also makes the transfer of funds across large distances comparatively inexpensive, rural households are more likely to make efficient investments in human capital by sending “members to high paying jobs in distant locations . . . and [allowing them] to invest in skills that are likely to earn a [greater economic] return” in places outside their village.54 Moreover, M-PESA allows rural households to effectively spread risk. If a “risk-related effect arises,” M-PESA allows a quick transfer of funds.55 “Instead of waiting for

51 Jack & Suri, supra note 1, at 11.
52 Mas & Radcliffe, supra note 5, at 180.
53 Id.
54 Jack & Suri, supra note 1, at 11.
55 Id.
conditions to worsen to levels that cause long-term damage, M-PESA might enable support networks to keep negative shocks [such as a medical emergency] manageable.”

Finally, M-PESA has increased the bargaining power of weaker family members, in many cases women. These family members can now expect “larger and more regular remittances from better-off city-dwelling relatives” and can also create a private place to store and manage their own funds, giving them a level of financial independence previously unavailable to them.

IV. FUTURE CHALLENGES: ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING REGULATIONS IMPLICATING M-PESA

Despite its successes, one of the challenges M-PESA faces is compliance with the ever-changing requirements of local and international anti-money laundering (AML) and counter-terrorist financing (CTF) programs. Although M-PESA is subject to the same AML controls required of banks operating in Kenya, the CBK and Kenya’s telecommunication regulator, the Communications Commission of Kenya (CCK)—cognizant of the risk posed by premature regulation of the mobile money industry—have historically taken a very open and supportive stance towards telecommunication operators seeking to provide financial services to unbanked populations in Kenya. The following sections seek to outline the manner in which AML controls in Kenya have evolved in their application to services like M-PESA.

A. The Application of Traditional Kenyan Banking Law to Mobile Money

At the time of M-PESA’s launch, Kenya attempted to regulate mobile money service providers only though an expansion of pre-existing regulations applicable to traditional banks. Prior to 1990,

\[56\] Id.
\[57\] Id.
the only measures taken to control mobile money laundering were contained in generally applicable criminal laws (such as the Anti-Corruption and Economic Crimes Act) and guidelines issued by the CBK, pursuant to the Kenyan Banking Act, seeking to implement recommendations of the Financial Action Task Force (FATF). These FATF Recommendations included: know your customer (KYC) regulations, customer due diligence (CDD) procedures, transaction monitoring requirements, watch list screening procedures, suspicious activity reporting (SAR), and mandatory record keeping. In December 2009, more stringent regulations were imposed with the passage of the Proceeds of Crime & Anti-Money Laundering Act (AML Act). Kenya’s AML Act explicitly criminalized money laundering, provided enforcement measures to the Kenya government (such as tracing and seizure rights), and imposed severe penalties on money launderers. Moreover, the FATF Recommendations previously implemented only through CBK prudential guidelines became mandatory for all financial service providers, including mobile money service providers like Safaricom.

B. The CBK’s Electronic Payment Guidelines and Sector-Specific Regulations

In 2011, the Kenyan government deviated from its regulatory strategy of merely applying traditional banking law to mobile money service providers by developing sector-specific guidelines concerning mobile money and electronic payments. In consultation with stakeholders including Safaricom, the CBK issued its Electronic Payment Guidelines of 2011 and Retail Electronic Transfer Guidelines of 2011. These regulations notably required authorized electronic money issuers, such as Safaricom’s M-PESA Holding Company (which holds funds on behalf of M-PESA customers), to maintain a core capital of the greater of KES10 million or 1 percent of one-twelfth of the previous year’s total turnover.

Following the release of the CBK’s e-money guidelines and a substantial lobbying effort by Kenya’s banking industry, the Kenyan Parliament began debating the potential for a new payments law that would more rigorously control electronic
payments and place mobile money on an equal regulatory footing with comparable funds-transfer services provided by traditional banking institutions. These debates culminated in the enactment of the National Payment Systems Act (NPSA) in December 2011. The NPSA brings all payment service providers, including mobile phone service providers, into one regulatory framework and provides the CBK with direct oversight of these providers to ensure their safety and efficiency. Discussions are also currently underway concerning the passage of a Kenyan Anti-Terrorism Bill that will impose even further AML and CTF regulations on mobile money service providers.

C. Compliance With and Voluntarily Imposed AML Programs in Mobile Money

By all accounts, Safaricom’s M-PESA service has maintained compliance with all applicable AML regulations and has remained largely immune from corruption or misuse. In fact, in 2008, when the traditional banking industry lobbied the Kenyan Finance Minister to order an audit of the service, it was “declared . . . safe and in line with the country’s objectives for financial inclusion” with minimal incidences of fraud perpetrated by the use of the M-PESA system were uncovered through the audit.58 Safaricom’s own internal and voluntary AML procedures are largely responsible for this result.

As with any major financial service, however, there have been reported cases of fraud and social engineering scams whereby unsuspecting subscribers have lost money to confidence tricksters. Thus, the financial innovations that have transformed M-PESA into a major payment service with millions of transactions worth billions of dollars annually should be developed hand in hand with appropriate controls to protect the M-PESA service from being used as an easy tool for money laundering and terrorism financing.

In this regard, Safaricom has proactively developed and implemented a comprehensive set of internal AML policies and

58 Mas & Radcliffe, supra note 5, at 174.
procedures including: (1) agent training, (2) internal KYC policies, and (3) strict transaction monitoring.

1. Staff and Agent Training for M-PESA Providers

For many aspects of the M-PESA service, Safaricom only works directly with “master agents” who in turn are entrusted with the control of retail sub-agents. However, there is one area over which Safaricom maintains tight and direct control: staff and agent training. Safaricom maintains this control, in part, to ensure that M-PESA’s users receive a consistent and positive experience regardless of which agent they choose to patronize, but also to comply with Safaricom’s AML and CTF policies. Before a new agent is authorized to provide the M-PESA service, Safaricom provides in-depth and comprehensive agent training that covers all aspects of the service, as well as Safaricom’s AML, CTF, and KYC procedures. Additionally, staff members at all levels are taken through formal and web-based AML awareness training. The program, adapted from the AML policy instituted by the Vodafone Group, encompasses all aspects of the M-PESA service and is annually audited by the Vodafone Group Money Laundering Reporting Office to ensure its effectiveness.

2. Identity Verification and “Know Your Customer” Procedures in M-PESA

M-PESA customers and agents are also subject to comprehensive KYC verification and CDD checks to protect M-PESA and related services from being used for money laundering. These procedures include an automated watch-list screening program (screening both for Politically Exposed Persons and persons on international sanctions lists) and a KYC regime requiring retail agents to “validate a customer’s identity during each transaction using [a] national ID card presented by the customer.”

59 Should a customer or agent present a money-laundering risk, appropriate deterrent action is taken resulting,

when applicable, in the investigation and prosecution of suspects by the relevant law enforcement agencies.

3. Transactional Controls

In addition to the KYC controls mentioned above, Safaricom has implemented a number of transactional controls, including transactional limits and ongoing transaction monitoring to detect suspicious activity and prevent money laundering.

M-PESA transactions are closely monitored through an automated Transaction Monitoring System with appropriate exception parameters, based on set transactional patterns. Any exception alerts generated by the system are investigated and appropriate action is taken to close the account and/or to escalate the matter to management or the relevant law enforcement agencies for resolution.

Transaction limits are set at KES70,000 (approximately US$900) per transaction with a maximum daily limit of KES140,000 (approximately US$1800) for cash deposits, transfers, and withdrawals, a maximum holding limit of KES100,000 (approximately US$800), and a KES10,000 (approximately US$130) limit for airtime purchases. System restrictions are in place to prevent any attempt to circumvent these limits. Further,

Retail agents are also required to record transactions in a paper log book. For each transaction, the agent enters: the M[-]PESA balance, the date, agent ID, transaction ID, transaction type (customer deposit or withdrawal, agent cash rebalancing), value, customer phone number, customer name, and the customer’s national ID number. Most of this information is copied from the confirmation SMS that the agent receives. Customers are then asked to sign the log for each transaction, which helps to discourage fraud. The log book is branded by
Safaricom and all retail agents use the same format.\textsuperscript{60}

All transactional information is stored electronically on the M-PESA platform, appropriate reports of those transactions are made available to customers and compliance officers, and suspicious transactions are automatically reported in compliance with Kenya’s AML and CTF programs.

CONCLUSION

What lessons can be drawn from the development of M-PESA in Kenya? First, there are a number of characteristics of Kenya’s population and culture that generated a unique demand for remittance services and made Kenya especially supportive of M-PESA’s development. However, Safaricom’s diverse agent network, robust money transfer platform, low price, and strong mobile infrastructure were able to generate the trust, convenience, and brand recognition necessary to ensure early and consistently high levels of M-PESA service adoption.

Finally, and perhaps most significantly, M-PESA’s success in Kenya is due, at least in part, to the enabling environment provided by regulators such as the CBK and the CCK. The passage of Kenya’s NPSA and related legislation, coupled with increasing international efforts seeking to tighten control over mobile payment service providers might significantly alter the regulatory landscape for services like M-PESA and guide their progress in the future.

The development of AML and CTF efforts, however, is not a one-way street. In fact, the most recent Mobile Financial Services Risk Matrix issued by the United States Agency for International Development (USAID) Booz Allen Hamilton group was developed largely by incorporating Safaricom’s own risk mitigation policies, procedures, and processes. Thus, it is evident that Safaricom and its successful implementation of the M-PESA service in Kenya will continue to have an important influence on the development of

\textsuperscript{60} Id.
mobile financial services and the future of international AML efforts.
REPORTING OF SUSPICIOUS ACTIVITY BY MOBILE MONEY SERVICE PROVIDERS IN ACCORDANCE WITH INTERNATIONAL STANDARDS: HOW DOES IT IMPACT ON FINANCIAL INCLUSION?

Miriam Goldby*
© Miriam Goldby

Cite as: 8 WASH. J.L. TECH. & ARTS 401 (2013)
http://digital.law.washington.edu/dspace-law/handle/1773.1/1205

ABSTRACT

Among the obligations which countries are required to impose upon their financial institutions under the Financial Action Task Force’s (FATF) 40 Recommendations is the obligation to report suspicions of money laundering. This Article discusses the impact that a reporting regime such as that set up in the United Kingdom in response to FATF requirements is likely to have should it be set up in developing countries seeking to regulate mobile money services. This Article argues that certain features of the U.K. suspicious activity reporting regime make it unsuitable for wholesale adoption into such a context. A one-size-fits-all approach by the FATF in establishing suspicious activity reporting obligations is likely to reduce the accessibility, affordability and attractiveness of mobile

* Lecturer in Insurance and Commercial Law, Centre for Commercial Law Studies (CCLS), Queen Mary, University of London. Thank you to Prof. Louis de Koker and Prof. Jane K. Winn for their input in the writing of this article and their comments on earlier versions of it. Thank you also to Laura Powell for her assistance in editing and proofreading. Any remaining errors or omissions are purely my own.

This Article was presented at the Mobile Money in Developing Countries: Financial Inclusion and Financial Integrity Conference held in April 2012 at the University of Washington School of Law with the support of the Linden Rhoads Dean’s Innovation Fund.
money services, thus impacting negatively upon the goal of financial inclusion.

TABLE OF CONTENTS

Introduction ..................................................................................402
I. Financial Integrity Requirements Applicable to Financial Institutions .................................................................404
II. Some Features of the AML Reporting Regime in the United Kingdom ...................................................................408
III. Problems with Implementing a U.K.-Style SAR Regime in a Developing Country .......................................................413
Conclusion ...................................................................................415

INTRODUCTION

This Article seeks to draw upon the author’s research on the United Kingdom’s Suspicious Activity Reporting (SAR) Regime in order to establish some preliminary points of discussion regarding the impact that a similar regime is likely to have in developing countries upon mobile money services which have to comply with similar reporting requirements under the international standards issued by the Financial Action Task Force (FATF). SAR regimes are set up in compliance with FATF Recommendation 20, which provides:

If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report

---

promptly its suspicions to the financial intelligence unit (FIU).²

Mobile money services have made financial services accessible to millions of people in the developing world who are not able to make use of banking services. Generally the service consists of value being loaded onto and stored in a mobile phone account, the owner of which can then use it to carry out everyday transactions, such as grocery shopping and paying utility bills.³ The service thus consists broadly of a financial service (the maintenance of an account) and a telecoms service (the transmission of transaction messages to move value to and from accounts).⁴ The provider of the financial service (whether or not it is the same person as is providing the telecoms service) will be liable to comply with certain AML requirements, including customer due diligence, suspicious activity reporting and record-keeping in accordance with the FATF Recommendations.⁵ In countries where large swathes of the population do not have access to a bank branch, these types of services have revolutionized the way that people manage their finances. Accessibility and affordability of the services are key to the success of the service and to financial

---
² Id. at 19. The text of Recommendation 20 was previously found in Recommendation 13 and Special Recommendation IV.
⁴ See CHATAIN ET AL., supra note 3, at 12-14, who divide up the mobile-money service into five elements or functions: (1) mobile communications service; (2) customer interface; (3) transaction processing; (4) account provision; and (5) settlement.
⁵ This is in line with the findings of CHATAIN ET AL., supra note 3, at 28, according to whom “the provider who manages the account records is in the best position to supervise the AML/CFT procedures of the providers at the other stages, and it may be advisable to place the legal burden for regulatory compliance on that provider. This is because the account records function is where the information about customers, retail outlets, and activity all comes together.”
inclusion, a major development goal for these countries.

I. FINANCIAL INTEGRITY REQUIREMENTS APPLICABLE TO FINANCIAL INSTITUTIONS

Under the FATF Recommendations financial institutions are required to comply with certain requirements as to customer due diligence (CDD, which includes identifying the customer and monitoring account activity), record-keeping, and reporting of suspicious activities in order to protect financial integrity when performing transactions for customers. The expression “financial institution” includes 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, by way of business, but does not include “any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds.” It therefore includes mobile money service providers who provide customers with both the financial and the telecommunications services, but not those that simply provide the

---

6 FATF RECOMMENDATIONS, supra note 1, at 115.
7 Id.
8 An example of this is O2’s Wallet service. O2, a telecoms company, allows its customers to deposit money into their electronic wallet up to a certain maximum per year. This maximum can vary among customers, some being allowed £800, some £5,000, others £10,000. The service will only be provided after CDD has been undertaken and the customer has been approved. See Finance and Insurance Terms and Conditions – O2 Wallet Agreement, O2, http://www.o2.co.uk/termsandconditions/finance-and-insurance/o2-money-wallet (last visited Aug. 16, 2012). A similar service, Beem, is provided by Mobile Sense, also a U.K. company. See Mobile Money, BEEM, http://www.beemm.co.uk/legal (last visited Aug. 16, 2012). The website indicates that “[y]ou can open a Beem account wherever you are, you don’t need to be online. To open on the go just text OPEN to Beem at 07624 81 66 66 and follow the simple text prompts.” Using Beem, BEEM, http://www.beemm.co.uk/using-beem/account-setup (last visited Aug. 1, 2012). In this case a user is prompted to register a debit card, which provides Beem with a method of verifying the user’s identity. The limit allowed on a Beem account is £300 within any thirty-day period. A Beem account does not require linking it to a bank account. In this case the procedure for opening the account seems to differ and may need to be completed online.
telecommunications service (the sending or receiving of messages for effecting money transfers over accounts held with others). This means that in countries where bank accounts are ubiquitous and the mobile service is simply used to send messages instructing the financial institution to effect transactions over these accounts, the mobile communications service provider can avoid being designated a financial institution by simply acting as a conduit for the bank to provide the service. On the other hand the mobile money service provider may itself want to provide the account over which the transactions take place, usually because it is profitable to provide the service in view of high demand. This is particularly true in countries where large swaths of the population do not have access to a bank account. In this case, the mobile money service provider will be subject to anti-money laundering (AML) and counter financing of terrorism (CFT) rules applicable to financial institutions. Because the financial service would be provided on a regular basis, the developing country in question would not be able to exempt these businesses from the FATF requirements applicable to financial institutions.

Ensuring accessibility and affordability of mobile money services while at the same time protecting financial integrity in line with international standards may involve far greater difficulties in developing countries than doing so in the world’s advanced economies. The table below gives a brief overview of factors that are taken for granted in advanced economies that may, depending

---

9 See for example the products and services provided by Monitise, a U.K. company, which appear to consist of messaging services allowing payments to and from bank accounts to be effected over a mobile phone. Monitise does not appear to itself provide financial (as distinct from telecommunication) services. It simply provides the platform over which such messages may be sent. See MONITISE AMERICAS, INC., http://www.monitise.com/ (last visited Aug. 16, 2012).

10 Indeed the exclusion may only apply when “a financial activity...is carried out by a natural or legal person on an occasional or very limited basis (having regard to quantitative and absolute criteria), such that there is low risk of money laundering and terrorist financing.” FATF RECOMMENDATIONS, supra note 1, at 32 (emphasis added). Subsequently, “a country may decide that the application of AML/CFT measures is not necessary, either fully or partially.” FATF 2011 GUIDANCE, supra note 3, at 20.
on the service in question, constitute obstacles in the developing world.

<table>
<thead>
<tr>
<th>Accessibility</th>
<th>AE 11</th>
<th>DC 12</th>
</tr>
</thead>
<tbody>
<tr>
<td>Register through existing bank account with local bank</td>
<td>✓</td>
<td>?</td>
</tr>
<tr>
<td>Proof of address</td>
<td>✓</td>
<td>?</td>
</tr>
<tr>
<td>Proof of identity</td>
<td>✓</td>
<td>?</td>
</tr>
<tr>
<td>Smartphone technology</td>
<td>✓</td>
<td>?</td>
</tr>
<tr>
<td>Stable internet connection</td>
<td>✓</td>
<td>?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Affordability</th>
<th>AE</th>
<th>DC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulation:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Does not preclude market-entry by new providers</td>
<td>✓</td>
<td>?</td>
</tr>
<tr>
<td>▪ Does not make service prohibitively expensive</td>
<td>✓</td>
<td>?</td>
</tr>
</tbody>
</table>

Aware of the obstacles that are likely to arise in the implementation of financial integrity measures, the FATF published a report on the issue in June 2011.13 This report discusses instances of simplified due diligence which may be applied where there is difficulty in obtaining regular proof of identity and address by establishing alternative methods of verification. It also discusses the potential to apply the general risk exemption,14 under which financial institutions may be exempted

---

11 Advanced Economies.
12 Developing Countries.
13 FATF 2011 GUIDANCE, supra note 3.
14 This exemption applies: (a) in strictly limited and justified circumstances; (b) based on a proven low risk of money laundering and terrorist financing, and (c) relating to particular a type of financial institution or activity. Thus the application of the exemption depends on proving low money laundering risk. This could be done using Groupe Spéciale Mobile Association’s (GSMA) Methodology for Assessing Money Laundering and Terrorist Financing Risk. See Marina Solin & Andrew Zerzan, Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks (GSMA, Discussion Paper, 2010), available at http://www.ifc.org/ifcext/gfm.nsf/AttachmentsByTitle/Tool10.11.GSMAMethodology-AssessingAMLRisk/$FILE/Tool+10.11.+GSMA+Methodology+-+Assessing+AML+Risk.pdf. In the Philippines this
from complying with full CDD requirements in respect of certain low-risk products. It gives illustrations of different ways in which proof of identity and address may be obtained in places where people may not be living at a formal registered address and may not be able to provide formal proof of identity. For instance in India for the opening of a certain maximum-balance and maximum annual credits accounts, introduction and certification by an existing account holder or any other evidence as to the identity and address that is to the satisfaction of the bank, can suffice for the purposes of customer identification.\textsuperscript{15} Special provision is also made for customers without any acceptable form of identity, such as migrant laborers, opening what are called “small accounts.”\textsuperscript{16} In the Philippines would-be users of financial services from certain rural areas can produce a Barangay Certificate (i.e., a certificate issued by the elected head of the village) for the purposes of customer identification and residence.\textsuperscript{17} An interesting example of the application of the general risk exemption may be found in South Africa where Exemption 17 releases financial institutions from address verification requirements in respect of certain low-risk maximum balance accounts permitting only domestic transactions below a certain value.\textsuperscript{18} This exemption has reportedly resulted in the more widespread use of financial services including a mobile money service called WIZZIT.\textsuperscript{19}

After the service has been set up and the customer accepted as such, the FATF Recommendations require financial institutions to monitor their customer accounts and report suspicious activity. This places certain burdens on financial institutions and affects their relationship with their customers. Some salient features of the system set up in the United Kingdom in response to FATF requirements and the implications for developing countries resulted in lower customer due diligence requirements for certain low-risk customers of SMART Communications. \textit{See} FATF 2011 GUIDANCE, \textit{supra} note 3, at 23.

\textsuperscript{15} FATF 2011 GUIDANCE, \textit{supra} note 3, at 29.
\textsuperscript{16} \textit{Id.} at 33.
\textsuperscript{17} \textit{Id.} at 29.
\textsuperscript{18} \textit{Id.} at 32.
\textsuperscript{19} \textit{Id.} at 33.
wishing to promote financial inclusion through mobile money are discussed below.

II. SOME FEATURES OF THE AML REPORTING REGIME IN THE UNITED KINGDOM

While much has been said regarding the difficulties of implementing CDD requirements in developing countries, less attention has been devoted to the problem of SAR. In response to the FATF Recommendations, complex SAR systems have been set up in developed countries whereby suspicious activity reports (SARs) may be prepared and submitted by reporters and accessed and actioned by the authorities. The successful establishment and operation of such a system require the investment of time and resources that may not be available in developing countries. Salient features of the U.K.’s SAR system, administered by the Serious Organised Crime Agency (SOCA) and the difficulties of implementing such a system in a developing country are highlighted below.

As FATF Recommendation 20 suggests, the foundation of any SAR system will usually be legal provisions laying down criminal or administrative sanctions for failure by financial institutions to file reports on suspicious activity (i.e., activity on their clients’ accounts which may constitute money laundering). In the United Kingdom the failure to report an offense is enshrined in Section 330 of the Proceeds of Crime Act 2002 (POCA). The provision applies to information obtained by financial institutions in the course of business. If on the basis of such information a person knows or suspects or has reasonable grounds for knowing or suspecting that another person is engaged in money laundering s/he should make a disclosure by filing a SAR, as soon as it is reasonably practicable to do so. Thus the offense includes negligence-based liability. In other words, liability for breach of

21 Id. at §§ 330(2), 330(4). This implements Article 22(1)(a) of the Third Money Laundering Directive, which contains the same wording.
Section 330 may arise not only where a person knows or suspects and does not file a SAR, but also where a person should have known or suspected, as there were reasonable grounds to do so.\textsuperscript{22} This introduces an objective test of liability. In order for the obligation to arise, the person must be able to identify the whereabouts of the person or laundered money or s/he must believe, or it is reasonable to expect him/her to believe, that the information may assist in identifying the person or the laundered property.\textsuperscript{23}

The failure to report an offense is known as a secondary money laundering offense. In certain circumstances, where it carries out a transaction for a customer in spite of the fact that it suspects money laundering, a financial institution may also be liable for the primary money laundering offenses laid down in POCA, Sections 327-329, in particular Section 328—entering into or becoming concerned in an arrangement which one knows or suspects facilitates (by whatever means) the acquisition, retention, use, or control of criminal property by or on behalf of another person. In order to avoid such liability, consent to the transaction must first be obtained under Section 335. In order to obtain such consent the bank must make a disclosure by filing a “consent SAR.”\textsuperscript{24} The penalties for acting without consent are potentially very serious, if it is proven that the act constitutes a primary money laundering offense.\textsuperscript{25}

So what are the implications of these reporting obligations? Starting first with the implications for the regulator, a stringent

\textsuperscript{22} Id. at § 330(2).
\textsuperscript{23} Id. at § 330(3)(a).
\textsuperscript{24} Having made such disclosure, in order to carry out the transaction for its customer the relevant person must either receive explicit consent, or wait for the expiration of the notice period, id. at § 335(3), or, where consent is refused during the notice period, the expiration of the moratorium. Id. at § 335(4). The notice period is 7 working days, id. at § 335(5), and the moratorium period is 31 days. Id. at § 335(6). If no consent is received and either the notice or the moratorium period (if applicable) has not passed, the relevant person can do nothing. If it acts, it may be liable for a primary money laundering offense, as provided by Section 334(1). See R. v. Serious Organised Crime Agency, [2007] EWCA (Civ) 406, [51]-[52], [2008] 1 All E.R. 465 (Eng.).
\textsuperscript{25} See POCA § 334.
requirement with draconian sanctions as provided by U.K. law typically results in large volumes of SARs, which can only be useful to law enforcement if they are organized in and accessed by end-users through a central database. In its early years the U.K. SARs system experienced substantial backlog problems because reports were submitted on paper and then manually inputted into a database by the staff of the then National Criminal Intelligence Service.26 Law Enforcement Agencies (LEAs)—the end-users of the reports—had no access to the database, so SARs had to be distributed to the end-users within whose jurisdiction they appeared to fall.27 In order to address these problems, the system was reformed, so that the vast majority of reports began to be submitted electronically,28 and end-users were given direct access to the ELMER database of reports in 2006. As a result SARs that do not produce “hits” when database searches are undertaken will not usually be followed up on or used in investigations. Because LEAs with scant resources have to prioritize their work, the filing of SARs relating to money-laundering transactions where the predicate offense is a petty crime can therefore be a waste of time and resources for the reporter, unless the SARs in question supplement already existing intelligence. Furthermore, the fact that so many end-users have access to the entire database, which is in effect a database of suspects, can have important implications for individual right to privacy and the confidentiality of personal information.29

28 SERIOUS ORGANISED CRIME AGENCY [SOCA], SUSPICIOUS ACTIVITY REPORTS REGIME ANNUAL REPORT 2011 10 (2011) [hereinafter SOCA ANNUAL REPORT].
29 See EUROPEAN UNION COMM., HOUSE OF LORDS, MONEY LAUNDERING AND THE FINANCING OF TERRORISM VOLUME I: REPORT (2009), available at http://www.coe.int/t/dghl/monitoring/moneyval/reporting/activities/UK_Parlrep.pdf, where the Committee observed that “ELMER is in effect a database of suspects.” id. at 49, containing a large and ever-increasing number of entries, id. at 48-49, which can be accessed directly by LEAs not only for purposes related
From the point of view of financial institutions that have the obligation to file reports, compliance with reporting requirements is resource-intensive, in some cases requiring the setting up of automated systems for the identification of unusual activity, and in all cases requiring staff training and man-hours. These costs may have to be passed on to consumers in the form of increased service fees and charges, which may reduce the service’s accessibility. Where the necessary resources are simply not available, much suspicious activity may remain unidentified and therefore unreported. It is also important to note that the objective test of mens rea coupled with criminal sanctions for breach of reporting requirements gives rise to a certain amount of defensive reporting, i.e., the filing of reports even if the reporter does not believe them to be of any use to law enforcement, which is in effect a waste of resources. At the same time the objective test will not necessarily deter service providers who are complicit with their clients in to serious organized crime but also for other purposes such as “ensuring compliance with tax obligations” and investigating “housing benefit fraud.” Id. at 49. It also found it noteworthy that “[o]n receipt of a SAR no steps are taken to confirm whether or not the suspicion on which it was based is well founded,” id., and that SARs are only automatically deleted ten years following receipt (except for SARs that have been amended or updated, in which case deletion is postponed for six years). Id. According to the 2011 SAR Annual Report there are currently 78 end users with direct access to ELMER. See SOCA ANNUAL REPORT, supra note 28, at 53. However the concerns of the House of Lords Committee have been taken on board and some changes have been implemented. All SARs older than six years will be deleted from ELMER, id. at 35, and access by non-police end-users will be subject to compliance with Criteria for Direct Access to Suspicious Activity Reports. Id. at 34.


hiding instances of money laundering. A good illustration may be found in the United Kingdom case of *R. v. Swan*\(^{32}\) where there was ample evidence that both defendants should have been aware that their facilities and services (safe deposit boxes and a bureau de change) were being used for purposes which were not above board. Swan was recorded on tape giving advice to undercover officers on how to launder money through the bureau de change without giving rise to the need for her to report\(^{33}\) and how to hire a safe deposit box anonymously.\(^{34}\) Woolf had on occasion found illegal items such as false passports and firearms in client safe deposit boxes.\(^{35}\) Thus the existence of the obligation in and of itself is no guarantee of the usefulness of the reports that find their way to the authorities.

A further problem is that if a consent system, such as the one in the United Kingdom is in place, filing a SAR can disrupt business and alienate clients. Two civil disputes which arose in the United Kingdom between customers and their banks, *Squirrel Ltd. v. National Westminster Bank*\(^{36}\) and *K. Ltd. v. National Westminster Bank*,\(^{37}\) provide interesting illustrations of the awkward situations that may arise as financial institutions seek to operate in the midst of impossible conflicts between their duty to act in accordance with the customer’s mandate and their duty to abstain from carrying out suspicious transactions for the customer until consent is obtained. Where a customer is attempting to effect a money transfer, and especially in cases such as these involving the transfer of substantial amounts of money between businesses in different jurisdictions, the delay in effecting the transfers while a financial institution awaits consent from the authorities will have an impact not merely on the relationship between the financial institution and its customer but also on that between the parties to the business transaction (failure to make payment would put a business in breach of its contract with its counterparty). While the financial

\(^{32}\) [2011] EWCA (Crim) 2275 (Eng.).

\(^{33}\) Id. at [3].

\(^{34}\) Id. at [4].

\(^{35}\) Id. at [7].

\(^{36}\) [2005] EWHC (Ch) 664, [2006] 1 W.L.R. 637 (Eng.).

\(^{37}\) [2006] EWCA (Civ) 1039, [2007] 1 W.L.R. 311 (Eng.).
institution may not carry out its customer’s mandate (and indeed the court held in the above cases that when a conflict arises between a financial institution’s duties to its customer and its duties under the criminal law, the latter should prevail), neither may it explain to its customer the reason why, as, if it does, it may find itself in breach of the tipping-off provisions in POCA\(^38\) which implement FATF Recommendation 21(b).\(^39\) While the reporting institution is protected, the customer is left, for all intents and purposes, without a remedy, though the courts have shown some willingness to hold SOCA accountable where it acts outside its powers in withholding consent.\(^40\) Any suspicion will suffice to trigger the financial institution’s obligation to report—the suspicion does not have to be reasonable.\(^41\)

III. PROBLEMS WITH IMPLEMENTING A U.K.-STYLE SAR REGIME IN A DEVELOPING COUNTRY

It is not hard to envisage the problems that are likely to arise in attempting to set up a U.K.-style SAR regime applicable to mobile money service providers in a developing country. First of all, in a developing country the application of simplified due diligence will be necessary in many cases in order to achieve financial inclusion, but where simplified due diligence is applied, it is not usually possible to obtain a full client profile. As a result, identification of

\(^{38}\) POCA § 333.

\(^{39}\) This provides: “Financial institutions, their directors, officers and employees should be . . . prohibited by law from disclosing (‘tipping-off’) the fact that a suspicious transaction report (STR) or related information is being filed with the FIU.” FATF RECOMMENDATIONS, supra note 1, at 19.


\(^{41}\) “Suspicion” is defined in K. Ltd. v. Nat’l Westminster Bank, [2006] EWCA (Civ) 1039, [16] as “a possibility, which is more than fanciful, that the relevant facts exist.” In the same case it was held that the existence of suspicion was a subjective fact and that there was no legal requirement that there should be reasonable grounds for the suspicion. Id. at [21]. In Ahmad v. HM Advocate, [2009] HCJAC 60 [30]; (2009) SCL 1093, 1108 (Scot.) it was held that “There is nothing in the language of s 330(2) which states or requires that money laundering is in fact taking place. It is plain that the obligation thereunder can arise if a person suspects or has reasonable cause for suspecting that it is.”
suspicious activity will be harder, because the service provider will not always be aware of the client’s background and what constitutes unusual activity for the client. In addition, the ability to file meaningful (and therefore useful) reports will be reduced, for example because the client used an alias or because the reason for suspicion is not included or is not sufficiently clear to assist in gathering intelligence for an investigation.\footnote{See Louis de Koker, \textit{Aligning Anti-Money Laundering, Combating of Financing Terror and Financial Inclusion: Questions to Consider When FATF Standards are Clarified}, 18 J. FIN. CRIME 361, 377 (2011).}

Another problem is that, as far as reporting obligations are concerned, under FATF standards no risk-based approach applies: all suspicions must be reported.\footnote{See FATF RECOMMENDATIONS, \textit{supra} note 1, at 79: “All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction.” See also FATF, \textit{GUIDANCE ON THE RISK-BASED APPROACH TO COMBATING MONEY LAUNDERING AND TERRORIST FINANCING: HIGH LEVEL PRINCIPLES AND PROCEDURES} 27 (2007), available at http://www.fatf-gafi.org/media/fatf/documents/reports/High%20Level%20Principles%20and%20Procedures.pdf [hereinafter FATF 2007 GUIDANCE]; FATF 2011 GUIDANCE, \textit{supra} note 3, at 40-41.} Thus reports must be made also with respect to suspicious transactions that are low-value and high volume, i.e., transactions of the type usually carried out using mobile money services. Service providers will need to train staff and devote resources to make these reports in spite of the fact that individual transactions do not present a significant profit margin. This may mean that, depending on the circumstances, certain types of customer may have to be excluded altogether. Furthermore, the authorities will rarely have the resources to justify the investigation of such alleged instances of money laundering,\footnote{See de Koker, \textit{supra} note 42, at 377.} at least not unless the number and pattern of linked transactions indicates a potentially serious problem. It is submitted that any attempt to apply a consent regime to this type of transaction would be ill-advised and likely to fail, both because the timely identification of suspicious and unusual activity is problematic for the abovementioned reasons, and because authorities are unlikely to be able to respond to requests for consent with a promptness that would allow the transaction to be carried out smoothly. Even if a
consent system is correctly implemented, it is likely that customers will abandon mobile money services in favor of more efficient informal payment methods.

A final potential issue involves evaluations of the system that may be carried out by other countries or external entities such as the FATF. In the past the FATF has criticized certain countries for the low volumes of SARs being filed, a prime example being Switzerland in 2005. If the same approach were applied in a developing country, SAR systems may be geared by the regulatory agencies responsible for them to generate defensive and over-reporting in order to improve the country’s statistics. An undesired effect could be the establishment of (informal) SARs targets and, potentially, artificial filings by reporters in order to reach an (informal) “quota.” This of course would lead to a further waste of authorities’ resources.

CONCLUSION

The above analysis leads to a few important conclusions. It is extremely difficult to construct an efficient and effective SAR system. Even in advanced economies like the United Kingdom, where a SAR system has been in operation for a considerable period of time, there are still open questions as to the system’s effectiveness. The inclusion of financial activity taking place by means of new payment methods such as mobile money within the ambit of a SAR system will require that system to be adapted, especially where a new type of provider, (i.e., a telecommunications company rather than a traditional financial

---

45 “The number of reports of suspicions filed with MROS seems low given the scale of the Swiss financial market and the activity that is carried out there.” FATF, THIRD MUTUAL EVALUATION REPORT ON ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM: SWITZERLAND 7 (2005), available at http://www.fatf-gafi.org/media/fatf/documents/reports/mer/switzerland%20resume%20english.pdf.

institution) with different types of internal monitoring and record-keeping processes, is providing the service. It is submitted that the FATF reporting requirements do not differentiate sufficiently among different circumstances and are not appropriately tested for unwanted “side-effects” such as wasteful defensive reporting or the shunning by consumers of regulated services in favor of informal ones, which may be cheaper and more efficient due to the absence of regulatory burdens.

In order to assist developing countries in designing a SAR system that will achieve some measure of financial integrity in this type of situation, FATF must do its utmost to move away from a one-size-fits-all approach and identify the most effective means to monitor mobile money transactions in developing countries. This entails the possibility of doing away with a traditional SAR system altogether and considering alternatives which allow countries to tailor their approach to financial integrity to their own environments. While the SAR system set up in the United Kingdom may be suitable for the jurisdiction in which it operates (and even this is as yet an open question), the application of suspicious activity reporting requirements in the same way in developing countries would be unsuitable. In particular, red tape in submitting reports should be kept to a minimum and, pending development of an appropriate and reliable infrastructure for web-based communications, reports in all forms should be acceptable. Depending on the circumstances, compliance with CDD and record-keeping requirements may preclude the need for SARs except for actual and strong suspicions. Instead a service provider’s records on a person officially under investigation could be made accessible to LEAs. As we have seen in the U.K. system SARs are put on a database which LEAs consult with search terms, usually for known nominals, and do not usually of themselves form the starting point of an investigation. This being the case, a similar effect could be achieved if LEAs were allowed, under certain conditions, to conduct searches of the records kept by service providers, which would preclude the need to file SARs.

47 See id.
48 For a discussion of record-keeping requirements applicable to mobile money service providers, see FATF 2011 GUIDANCE, supra note 3, at 40.
When drafting provisions granting these powers, however, it is important to build in safeguards against potential abuses by governmental agencies, which may have the effect of discouraging widespread use of mobile money services.\textsuperscript{49}

Finally, if a consent regime is put in place, it should only apply to high-risk transactions, for example transactions over a certain threshold value and/or transactions which the reporter knows or has reason to believe are linked to a serious predicate crime such as serious theft; fraud; corruption; the trafficking of weapons, drugs, or people; or terrorism offenses.

Much research remains to be done into the effectiveness of SAR regimes and this research should be undertaken before attempts are made to make these regimes applicable to mobile money service providers in developing countries. A one-size-fits-all approach is likely to result in many unintended effects which will at best slow down the dissemination of this type of financial service in the areas that need it most and at worst lead to its outright rejection by intended users.

ABSTRACT

Mobile banking and mobile payments in the United States have evolved differently than in other developed and developing countries. The current fervor for mobile payments in the United States is more about chasing affluence and advertising than creating access for the unbanked and underbanked. However, those individuals may eventually gain access to a broader range of financial services at lower costs depending on how the mobile payments ecosystem evolves in the United States. U.S. regulators have made it clear that existing financial services regulations apply to mobile banking and mobile payments, and the Consumer Financial Protection Bureau (CFPB) is poised to take a lead role in examining and regulating non-financial institutions in the mobile payments space. Finally, the U.S. Treasury Department and the Financial Crimes Enforcement Network (FinCEN) have stated that the United States will follow the revised

* Erin F. Fonté is a Shareholder, Payments Lawyer, and Certified Information Privacy Professional (CIPP) at Cox Smith Matthews (Austin, TX office). Her practice includes advising financial institutions, alternative payments providers, vendors and retailers regarding financial services, regulatory issues and payment systems laws, including mobile payments, stored value, and emerging payments. She is also head of her firm’s Privacy and Data Security practice. (Twitter: @PaymentsLawyer).
Financial Action Task Force (FATF) Recommendations. This could have an impact on who is eligible to participate in mobile payments, particularly the revised FATF Recommendations on transparency, customer due diligence and new technology.

Table of Contents

Introduction ..................................................................................421
I. Mobile Banking vs. Mobile Payments..................................422
   A. Mobile Banking ...............................................................423
      1. Common Mobile Banking Services .......................423
      2. Emerging Mobile Banking Services ......................424
      3. Mobile Banking and Financial Services Regulations ..................................................425
   B. Mobile Payments ..............................................................427
      1. Proximity Payments ...............................................428
      2. Remote Payments ...................................................428
      3. Disintermediation at Point of Sale (POS) ..............429
      4. Disintermediation at the Wallet.............................430
      5. Mobile Payments and Financial Services Regulations ..................................................431
         a. Federal Reserve Board ....................................431
         b. Financial Crimes Enforcement Network ..........432
         c. Consumer Financial Protection Bureau ..........434
         d. Conclusions on Regulatory Environment and Mobile Payments Industry Workgroup ....436
II. Mobile Banking/Mobile Payments and Anti-Money Laundering Issues .................................................................437
   A. Anti-Money Laundering/Bank Secrecy Act and Mobile Banking ..................................................437
   B. Anti-Money Laundering/ Bank Secrecy Act and Mobile Payments ..................................................439
   C. FATF and U.S. BSA/AML Regulations .........................440
      1. Summary of Updated FATF Recommendations ...440
      2. Transparency ..........................................................441
      3. Customer Due Diligence ........................................442
      4. New Technology ........................................................443
      5. Application of FATF Revised Recommendations
Mobile payments technology is poised to create a globally dramatic shift in how individuals pay for goods and services, track spending, and manage personal finances. Mobile payments are also becoming big business for non-financial institution alternative payments. Add the fact that many of these services are offered by non-financial institutions that are “disintermediating” the traditional banking relationship, and there is the potential for a fundamental shift in how individuals conduct day-to-day purchasing and interact with their finances.

In the United States, financial institutions have, over the past several years, rolled out mobile banking products via short message service (SMS) text messaging and smart phones. Many of these products are extensions of online banking offerings, and some are new and innovative, such as “deposit by phone” services where customers deposit checks by taking photos with their smart phones.

Outside the traditional financial institutions (FI) channels,
alternative payments providers, such as PayPal, are offering payments services and taking over the primary relationship with consumers. There has also been a lot of media and business press on which payments start-ups are getting funded and acquired, whether Square or PayPal are signing up the biggest and best merchants, and the lucrative potential upside for the company (like Google Wallet) or joint venture (like Isis or the newly formed Merchant Customer Exchange\(^2\)) that becomes the dominant standard for the mobile wallet.

However, despite a flurry of activity in the mobile payments space in the last few years, so far the proliferation of mobile services by FIs, and the ever-increasing list of new mobile payments providers, nothing has truly changed regarding the payments infrastructure and how unbanked and underbanked individuals gain access to the FI accounts, debit cards, credit cards, and other “minimum necessary access devices” to participate in mobile banking and mobile payments.

I. MOBILE BANKING VS. MOBILE PAYMENTS

To discuss where the United States is currently in terms of financial inclusion and financial integrity (i.e., effectively policing for fraud, money laundering and anti-terrorist financing issues), it is important to understand the types of entities and end-user customers currently involved in mobile payments in the United States. A “payment” at its most basic level is the transfer of money or wealth or value from one person or entity to another. As has been the case for about the past twenty years, and remains the case today, there are five and only five methods to process and settle payment transactions: cash, check (including substitute checks created pursuant to the federal Check21 Act), credit card and debit card rails (which include debit card, credit card, and stored value card transactions), automated clearing house (ACH) rails, and wire

transfers.

Even non-FI mobile payments providers must still use FIs in clearing and settling payments on the back end. In the United States, FIs accept, collect, and process payments, and participate in large-scale clearing and settlement systems such as debit card networks, credit card networks, the ACH network, and check image exchange networks like the Electronic Check Clearing House Organization (ECCHO) and The Clearing House. Mobile banking involves a FIs customer accessing and conducting transactions and performing other services directly to an account held at the FI through the customer’s mobile device.

A. Mobile Banking

The mobile phone and smart phone are transforming the banking industry. Over a decade ago, online banking “freed customers from brick-and-mortar branches, allowing them to execute transactions at any time.”\(^3\) Now consumers do not even want to be tethered to bulky desktop or laptop computers, and banking via mobile phone and tablet devices is the new evolution in “bricks-to-clicks.” It is projected that by 2013, an estimated 53 million consumers will bank by mobile phone (nearly 52 percent in annual compound growth from 2009).\(^4\)

1. Common Mobile Banking Services

Many FIs (both large and small) now offer some combination of the following banking services via mobile device, either by short messaging service (SMS) that older model “feature” phones use, or a truncated mobile website or mobile application (“mobile app”).\(^5\) Common mobile banking services now include:

- Account balance inquiries and statements;

\(^3\) Timothy R. McTaggart & David W. Freese, Mobile Banking: What Banks Need to Know When Outsourcing Their Platforms, 3 BLOOMBERG L. REP. – BANKING & FIN., no. 11, 2010 at 18.

\(^4\) Id.

\(^5\) Mobile apps are available for download through the Apple iPhone/iPad App Store, or through Google Play (formerly the Android Marketplace).
Bill payment services;
Funds transfers;
Branch and ATM location services; and
Transaction alerts based on dollar thresholds or other parameters.

2. Emerging Mobile Banking Services

FIs are also beginning to offer new and innovative services via mobile device. For example, USAA was the first FI to utilize the camera function on customer’s mobile devices to create its USAA Deposit@Mobile™ service where a customer can take a photo of the front and back of a check and deposit the check via the image captured to their bank account.6 Several FIs now offer a remote check deposit app for their customers.7

FIs are also rolling out new and innovative mobile features where the customer can exercise more control over their debit card or other aspects of their account, such as a debit card “on/off” switch via mobile banking. This service allows the customer to turn the debit card to “off” status when the card is lost or stolen, or the customer just wants to make sure the card is dormant. Other debit card controls include: (1) increasing daily withdrawal limits at ATMs, (2) increasing daily debit card purchasing limits (for big transactions like buying a sofa), and (3) allowing foreign transactions when the customer is traveling outside the United States.8

Several FIs are now building personal financial management

---

tools into their mobile banking services and offerings.\textsuperscript{9} FIs are even entering into the daily deal arena, with Bank of America offering coupons to holders of Bank of America debit and credit cards. The Bank of America coupons might also contain a geolocation or “contextual” component based on where the customer is or what their typical buying habits are.\textsuperscript{10}

3. Mobile Banking and Financial Services Regulations

Until very recently, there was some uncertainty as to whether certain federal and state banking and financial services laws, rules or regulations would apply to mobile banking services. In many respects, payments initiated via a mobile device are functionally the same as existing payments and funds transfers, and the mobile device is just another form factor.\textsuperscript{11} When in doubt, the safest course of action was to assume that if the underlying activity is governed by a particular law, rule, or regulation, then such law, rule, or regulation would also govern that same activity when conducted on a mobile device.

For example, if a mobile device is used to initiate an electronic funds transfer to or from a demand deposit account held at a FI, then the mobile device is most likely an “access device” under the federal Electronic Fund Transfer Act (EFTA),\textsuperscript{12} and Regulation E\textsuperscript{13} (issued by the Federal Reserve Board pursuant to the EFTA). EFTA and Regulation E govern electronic funds transfers (EFTs) to and from a customer’s account at a FI. EFTs are defined as

\begin{itemize}
  \item \textsuperscript{12} 15 U.S.C. §§ 1693-1693r (2012).
  \item \textsuperscript{13} 12 C.F.R. pt. 205 (2012).
\end{itemize}
transfers of funds initiated by electronic means, including, but not limited to, ATM transfers, debit card transactions, direct deposits and withdrawals, telephone initiated transfers and online bill payments.

Most importantly for both mobile banking and mobile payments is that the definition of an “access device” under Regulation E is actually much broader than many in the payments industry think. The definition of “access device” under Regulation E is “a card, code, or other means of access to a consumer’s account, or any combination thereof, that may be used by the consumer to initiate electronic fund transfers.”\textsuperscript{14} Some industry participants mistakenly think that Regulation E only applies to debit cards.

Similarly, if a mobile device accesses a line of credit for funding transactions, or is used to apply for a loan product, then the federal Truth In Lending Act (TILA),\textsuperscript{15} and corresponding Regulation Z (promulgated by the Federal Reserve Board),\textsuperscript{16} will apply, and the FI will need to meet the TILA disclosure and other requirements. The federal Gramm-Leach-Bliley Act (GLBA)\textsuperscript{17} and corresponding Regulation P\textsuperscript{18} (promulgated by the Federal Reserve Board) apply to any “financial institution” as defined under GLBA, and FIs offering mobile banking services are clearly covered by GLBA/Regulation P regarding customer privacy and data security issues. FIs are also expressly covered by Bank Secrecy Act and anti-money laundering requirements, as discussed further below.

Previous uncertainty as to whether current banking regulations apply to mobile banking services was laid to rest on June 29, 2012. In testimony and written statements provided to the U.S. House Financial Services Subcommittee on Financial Institutions and Consumer Credit, at a hearing entitled “The Future of Money: Where Do Mobile Payments Fit In the Current Regulatory Structure?”, representatives from the Federal Reserve Board (Federal Reserve), the U.S. Department of the Treasury’s Financial

\textsuperscript{14} 12 C.F.R. § 205.2(a)(1) (2012).
Crimes Enforcement Network (FinCEN), and the Consumer Financial Protection Bureau (CFPB) all made statements that current financial services regulations apply to mobile banking and mobile payments.\textsuperscript{19} And these regulators also stressed that application of such laws is not dependent upon the type of entity engaging in the services (i.e., FI or non-FI), but rather is dependent on the nature of the underlying activity itself. (The testimony and written statements are discussed in depth in Section I.B.5 below.)

B. Mobile Payments

The term “mobile payments” includes payments services and products offered not just by FIs, but by emerging and alternative payment providers as well, such as PayPal (non-FI account that processes and settles transactions between buyers and sellers), or BilltoMobile (allowing payment for goods and services by charging to mobile phone bill, and then customer chooses how to settle and pay phone bill), or Square (initially launched as alternative credit/debit card processing service for local and small merchants).

Current mobile payments operating models include:

- The FI model (discussed above);

- The mobile payments service provider model where the provider “offers mobile payment capabilities to its service users (which may include small merchants).” Transactions are processed over the provider’s systems, and may access an existing customer funding source held at or issued by a third-party, such as a demand deposit account or debit/credit/stored value card, or there may be a dedicated funding account at a provider; and

- The mobile network operator model where the “mobile network operator offers mobile payments capabilities for

purchases using mobile devices associated with its wireless network.” Transactions are generally processed over the operator’s wireless network and charges appear on the purchaser’s wireless bill or are funded on a prepaid basis.20

The three categories listed above describe the mobile payments model—who has the primary customer relationship, who is processing and settling the transactions, etc. There are also generally two different mobile transaction types (proximity payments and remote payments), and two points of “disintermediation” of traditional payments (disintermediation at point-of-sale (POS) and disintermediation at wallet).

1. Proximity Payments

Proximity payments occur where technology is embedded in, attached to, or displayed on the purchaser’s mobile device and interfaces with the merchant’s point of sale (POS) equipment to initiate payment. Proximity payments generally involve the purchase of goods and services from a merchant at a physical POS. For example, the Starbucks payment app is tied to a customer’s Starbucks gift card, and when launched for payment on the mobile device, creates a unique bar code displayed on the customer’s mobile phone and read by the Starbucks location’s POS terminal. Near Field Communication (NFC) will be used by mobile wallet providers such as Isis,21 and is designed to promote secure transactions via wireless communications between an NFC reader in a POS terminal and a secure NFC chip either embedded in or affixed to a mobile device. Proximity payments are also commonly referred to as “scan and go” or “tap and go” transactions.

2. Remote Payments

Remote payments occur when the purchaser uses their mobile device to initiate a payment to a merchant or other payee without

20 Douglass, supra note 11, at 7.
regard to proximity to the POS or payee themselves. There are two general types of remote mobile payments, mobile money transfer transactions and purchase payment transactions. An example of a mobile money transfer transaction is the person-to-person payments provided by a company called Popmoney. “Customers will send money directly from their bank accounts to another person using the other person’s bank-account number, e-mail address, or mobile-phone number.”22 An example of purchase payment transactions done remotely are the services provided by BilltoMobile where merchant charges are directly billed to a purchaser’s cell phone account.23

3. Disintermediation at Point of Sale (POS)

The most famous and successful company to achieve disintermediation from the established credit/debit card networks and processors is Square, a mobile POS startup co-founded by Twitter founder Jack Dorsey and launched in 2009.24 The initial goal of Square was to use a plug-in device for an iPhone or iPod (called a “dongle,” and, not surprisingly, square in shape) that turns the mobile device into a mobile POS terminal. Square has been one of the most successful non-FI entrants into the payments space since PayPal, and as of June 2012, was processing US$6 billion in payments annually.25

After seeing the success of Square, the companies that manufacture POS hardware and software created their own mobile POS devices. Verifone created its mobile POS device called Sail. Intuit, the company that created QuickBooks, launched GoPayment, a mobile POS device and virtual signature service that integrates with QuickBooks. PayPal launched PayPalHere.26

23 Id. at 36.
25 Id.
26 Id.
4. Disintermediation at the Wallet

Disintermediation at the wallet refers to the current race by several companies to create a virtual wallet where all of the payment cards in the average person’s wallet—debit cards, credit cards, store gift cards, stored value cards—are housed in a virtual wallet app on the purchaser’s smart phone. The smart phone is then used as the payment device that will interact with the POS for a proximity payment or to conduct a remote payment. There is currently a lot of time and money being invested by major credit card networks, mobile network operators (such as AT&T, Verizon, T-Mobile, and Sprint), major banks, major alternative payments providers (such as PayPal), and major technology companies (such as Google) to create and corner the market on the mobile wallet. While there are several other mobile wallet startups, the activities of mobile wallet providers Isis, Google Wallet, and PayPal are currently garnering a lot of attention.27

Isis is a joint venture between AT&T, T-Mobile, and Verizon, but is also partnered with Visa, MasterCard, and American Express; JPMorgan Chase, Capital One and Barclaycard also have agreed to issue cards for the wallet.28 Google Wallet involves MasterCard and payment processor First Data Corporation, and Sprint Nextel is the designated mobile network operator (but Google Wallet only works on Sprint mobile devices). Google Wallet is also going to include some form of coupon or offer redemption, and may be expanded to include loyalty and rewards components as well.29 The PayPal wallet just gained major publicity by announcing a partnership with Discover to bring PayPal’s digital wallet and payment services to millions of merchants in the Discover network, with services currently scheduled to roll out in 2013.30 Mobile payments industry pundits

27 See id; Annual Field Guide, supra note 22, at 34-47.
29 Annual Field Guide, supra note 22, at 40.
are waiting to see what Apple does on the mobile payments/mobile wallet front. Apple’s recent announcement of Passbook, along with confirmed rumors that the iPhone 5 includes NFC technology, have led industry observers to speculate as to whether Apple has its own mobile wallet offering in mind given that it manufactures the iPhone. And the recently announced Merchant Customer Exchange (discussed earlier in this article) is a merchant-created mobile wallet initiative.

5. Mobile Payments and Financial Services Regulations

As previously mentioned, there was until very recently some uncertainty as to whether certain federal and state banking and financial services laws, rules, or regulations would be applied to mobile payments services. The sections below summarize the positions taken by representatives from the Federal Reserve, FinCEN, and the CFPB that current financial services regulations apply to mobile banking and mobile payments activities.32

a. Federal Reserve Board

Stephanie Martin, Associate General Counsel at the Federal Reserve Board of Governors, commented that the Federal Reserve believes many current financial services regulations (GLBA/Regulation P, EFTA/Regulation E, TILA/Regulation Z, etc.) are written broadly enough to cover a lot of mobile banking and mobile payments activity.33 And with regard to non-FIs that provide mobile payments services, “[t]o the extent that nonbanks are involved, whether and the degree to which federal or state statutes and rules are applicable depends on the nonbank’s role in

---

32 See generally Future of Money Hearing, supra note 19.
the transaction and the specific provisions of the particular statute or rule.”

Martin stated that a mobile payment is just like any other type of payment in that it is ultimately moving money between bank accounts. This is true even if payment is initially charged to a consumer’s bill for services (such as a cell phone bill) or to a prepaid balance held by a nonbank. Settlement is still happening over the same existing rails. As Martin stated, “a new interface is not a new phenomenon.”

With regard to non-FIs, Martin stated that existing laws are in place to cover these services as well, such as EFTA/Regulation E and other federal consumer laws, and they apply to nonbank mobile payments (including stored value cards or funds associated with a stored value account), and that non-FIs are also subject to CFPB rulemaking and interpretive authority. Martin stressed that whether a particular law, rule or regulation applies often depends on a non-FI’s role. For example, a third party mobile app platform vendor just running “back office” services for the bank means the bank is still responsible. But for more independent non-FIs like managers of stored value card programs, money transmitters, and mobile network operators, financial services laws, rules, and regulations may be more likely to apply based on the specific activities carried out by the non-FI.

Martin concluded her testimony by explaining that regulators are still determining the extent that new and developing methods of mobile payments are subject to current laws. But when the mobile payments marketplace is more fleshed out, that will be the time to determine if additional legislative or regulatory proposals are needed.

b. Financial Crimes Enforcement Network

James Freis, Director of FinCEN, gave testimony regarding
FinCEN’s position about the applicability of BSA/AML provisions to mobile payments. He stated that “FinCEN’s rules for prepaid access, including mobile payments, are specifically designed to make [money laundering] more difficult to occur in significant amounts without leaving a trail and with obligations on the industry to alert FinCEN of [BSA/AML] red flags.”

Freis said that mobile banking involves communication and direction from an account holder about their account at a depository institution. If mobile banking facilitates communication between the FI and its customer, then the FI is already covered by BSA/AML requirements. Mobile payments, however, is the direction of funds outside of a bank account to effect payments or other transfers. Freis went on to state that:

FinCEN’s regulations also have made it clear that the acceptance and transmission of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another person or location, by any means, constitutes money transmission, and that any person wherever located doing business wholly or in substantial part within the United States engaging in money transmission, regardless of any other business lines the person is engaged in—such as the provision of telecommunications services—would likely be a money services business under FinCEN’s regulations, and as such must register and comply with all the reporting, recordkeeping, and monitoring requirements applicable to a money transmitter.

---


40 Id. at 2.

41 Id. at 5.
Freis also stated that “FinCEN’s regulations take a comprehensive approach in this area, focusing more on the activity at issue as opposed to the particular electronic communication vehicle.”\textsuperscript{42} With regard to mobile payments, Freis stated that “[f]or the sake of clarity, let me emphasize that a payment system allowing the transfer of funds from one mobile phone to another, such as by reference to a phone number, is subject to FinCEN’s regulations for prepaid access.”\textsuperscript{43}

Freis said that FinCEN has provided law enforcement with a “reference manual” regarding mobile payments. In preparing the manual, FinCEN has “seen an interesting trend in the mobile payments industry where different telecommunications systems and/or financial mechanisms may merge and become interwoven in the same overall mobile payments transactions.”\textsuperscript{44} Freis also said, toward the end of his testimony, that “[c]onsistent with past practice, FinCEN will interpret its regulations as they apply to various business models and provide guidance as necessary to industry with respect to the application of FinCEN’s requirements.”\textsuperscript{45}

c. Consumer Financial Protection Bureau

Although she did not provide written testimony at the hearing, Marla Blow, the Assistant Director for Card and Payments Markets at the CFPB, did provide a written Statement for the Record that was submitted to the subcommittee.\textsuperscript{46} In her statement, Blow echoed many of the same points and themes stated by Martin and Freis that existing financial and consumer protection regulations govern mobile payments. Blow wrote that “[o]ur mission is to

\textsuperscript{42} Id. at 4 (emphasis added).
\textsuperscript{43} Id. at 9.
\textsuperscript{44} Id. at 12.
\textsuperscript{45} Id. at 13.
make consumer financial markets work for consumers, honest businesses, and the economy as a whole. In carrying out this mission, the Bureau has a key role to play in the regulatory, supervisory, and oversight regimes governing mobile payments.\footnote{47}{Id. at 1.}

Blow stressed that under the Dodd Frank Act, the CFPB is required to regulate consumer financial products and services under federal consumer financial law. And she pointed out that with regard to mobile payments in particular:

The Bureau is engaged in ongoing coordination with the Federal Trade Commission, the Federal Communications Commission, the Federal Deposit Insurance Corporation, the Federal Reserve Board, the Office of the Comptroller of the Currency, the Treasury Department’s Financial Crimes Enforcement Network, and state banking regulators. We are committed to working closely with state and federal partners on this issue.\footnote{48}{Id.}

Blow stated that the CFPB is closely monitoring new developments and changes in the marketplace and in consumer use patterns regarding mobile payments. The primary responsibility for monitoring developments in mobile payments within the CFPB resides with the Card and Payment Markets team, part of the division of Research, Markets, and Regulations. Blow indicated that the Card and Payment Markets team has responsibility over credit, debit, prepaid, and mobile payments markets, and that this division of the CFPB is engaged in ongoing discussions with relevant parties, as well as other state and federal agencies.\footnote{49}{Id.}

Blow went beyond testimony and statements from other regulatory agencies by stating that while mobile payments can introduce innovation, it can also pose significant risks to consumers:

New technologies may be designed in ways that may not fall within existing regulatory frameworks.

\footnote{47}{Id. at 1.}
\footnote{48}{Id.}
\footnote{49}{Id.}
Existing rules may not have anticipated new developments enabled by modern technology and may prove inadequate for addressing emerging concerns. To the extent that technology companies begin to play roles traditionally performed by banking institutions, we may need to reconsider how well our existing regulations apply to a changed environment.50

d. Conclusions on Regulatory Environment and Mobile Payments Industry Workgroup

What is clear from the testimony and statements provided by representatives of the Federal Reserve, FinCEN and the CFPB is that: (1) regulatory agencies are monitoring the developing market and ecosystem for mobile payments; (2) the agencies and regulators take the position that many mobile payments services are already covered by existing laws, rules, and regulations that apply based on the type of activity being performed, not based on whether the provider is a bank or non-FI; and (3) as the mobile payments ecosystem becomes more mature, regulatory agencies will determine whether new legislation or regulations are needed to address any regulatory gaps governing mobile payments transactions.

Over the course of 2010 and 2011, the Mobile Payments Industry Workgroup (MPIW), which is being operated jointly by the Atlanta Federal Reserve and the Boston Federal Reserve, held a series of meetings with various industry players and regulators regarding the development of the mobile payments ecosystem and the regulatory landscape. On April 24, 2012, the Atlanta Federal Reserve and Boston Federal Reserve convened a meeting with representatives from federal and state banking agencies, the Federal Trade Commission (FTC), and the Federal Communications Commission (FCC) to discuss issues, concerns, and potential gaps in regulatory coverage.51

50 Id. at 2.
51 MARIANNE CROW ET AL., THE U.S. REGULATORY LANDSCAPE FOR
Several perspectives and overall themes emerged from the regulator meeting on mobile payments. First, the complexity of the regulatory framework for providers of mobile financial services in the United States prompts analysis of potential coverage gaps. Mobile payments essentially bring together two heavily regulated industries that are governed by separate sets of laws, rules and regulations—banking/financial services and telecommunications. There is a potential for regulatory gaps depending on the model and transaction flow of mobile payments.

Regulators also have an interest in ensuring safety and soundness of consumer protection in the emerging mobile payments environment. Existing regulatory guidance provides sufficient governance for existing mobile payments services. However, regulators will need to stay abreast of mobile industry trends and developments to effectively monitor the emerging risk environment. Third-party, non-FI vendor management in new mobile payments business models is critical to ensuring safety and soundness in mobile retail payments systems.

II. MOBILE BANKING/MOBILE PAYMENTS AND ANTI-MONEY LAUNDERING ISSUES

A. Anti-Money Laundering/Bank Secrecy Act and Mobile Banking

While mobile banking is providing greater freedom and ease to banking customers, it also presents new opportunities for criminals to launder money and finance terrorism. Money launderers and terrorist financiers can attempt to gain access to a mobile banking account by stealing a mobile phone with inadequate security features, or by attempting to hack transactions as they occur via a wireless network, or by tricking customers to disclose their financial account information via “mishing” attacks or fake bank


52 Id. at 3.
53 Id. at 4-5.
54 McTaggart & Freese, supra note 3, at 19.
apps. A “mishing” attack consists of a text message sent to a mobile phone stating something like “Notice: Issues Found On Your Shazam Mastercard. Please Call 13035780902!” 55 When the mishing victim calls the number, they reach an automated recording demanding the entry of the Personal Account Number (PAN) and additional confidential information. If the victim falls for the scam, then they voluntarily hand over their confidential financial account information to the fraudsters.

Some FIs have reported fake bank apps available on the Apple App Store and Android Marketplace (now Google Play). 56 The fake banking apps purport to be legitimate banking apps of actual FIs, but they are in reality “shell apps” that trick customers into entering user name, passwords, log in information and other mobile banking information.

The United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (the USA PATRIOT Act) 57 requires that FIs follow various requirements designed to prevent terrorists from accessing financing. FIs are required to develop policies and procedures to detect and prevent money laundering, and to submit suspicious activity reports (SAR) on suspected money laundering transactions. Given the increased risks that mobile banking poses, FIs must integrate their mobile banking operations into their overall Bank Secrecy Act 58 and anti-money laundering (BSA/AML) policies and procedures.

As made clear by the recent testimony of Martin, Freis, and Blow (all discussed in Section I.B.5 above), regulatory agencies have taken the position that current banking regulations, including BSA/AML regulations, apply to banks engaged in mobile payments.

B. Anti-Money Laundering/ Bank Secrecy Act and Mobile Payments

The recent testimony of regulators discussed in Section I.B.5 above indicates that regulatory agencies have taken the position that current banking regulations, including BSA/AML regulations, also apply to non-FIs engaged in mobile payments depending upon the type of activity in which the non-FI is engaged. For example, Martin stated “[t]he applicability of existing laws to [non-FIs] that are providing mobile payments services often depends on the [non-FI’s] role in the transaction.”\(^{59}\)

If a non-FI’s activities fall within FinCEN’s definitions of “money services business” (MSB), then those entities must register as a MSB with FinCEN. In addition, the non-FI’s activities could also trigger registration under individual state money transmission laws. In general, non-FIs that are money services businesses or money transmitters, are also subject to the USA PATRIOT Act BSA/AML requirements.

Some non-FI payments organizations in the mobile payments arena, such as PayPal, have registered under the laws of certain states as an MSB/money transmitter, and have also complied with the recently updated FinCEN MSB registration requirements. On July 18, 2011, FinCEN adopted a final rule enacting amendments to the Money Services Business Definitions Rule\(^{60}\) that, among other things:

- Revises MSB definitions to further clarify what activities subject a person to the BSA rules pertaining to MSBs;

---

\(^{59}\) Martin, \textit{supra} note 33, at 5.

• Updates the MSB definitions to reflect past guidance and rulings and current business operations and to accommodate evolving technologies and emerging lines of business;

• Separates the provisions dealing with stored value from those dealing with issuers, sellers, and redeemers of traveler’s checks and money orders to more readily accommodate changes to be implemented in FinCEN’s pending Prepaid Access Rulemaking; and

• Replaces the term “currency dealer or exchanger” with the new term “dealer in foreign exchange,” a term used to include the exchange of instruments other than currency as a category of MSB.61

To the extent that a non-FI mobile payments provider will have the primary customer relationship and will be enrolling the customer in its payment services and conducting “customer identification program” activities normally performed by FIs, the non-FI will have to comply with the “customer identification program” requirements under applicable BSA/AML laws, rules, and regulations.

C. FATF and U.S. BSA/AML Regulations

1. Summary of Updated FATF Recommendations

On February 16, 2012, the Financial Action Task Force (FATF), the global standard setter in the fight against money laundering and terrorist financing, revised the FATF “40 + 9” Recommendations through the publication of the “International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FATF Recommendations.”62 This

---

61 Id.

most recent update to the FATF standards follows an extensive review and consultation process with member countries that began in June 2009 and includes revisions made with input from governments, the private sector, and various other stakeholders. In response to key issues arising from these extensive public consultations, “the FATF made a number of significant changes to the FATF standards to reflect practices in the financial sector, to set out clearer requirements for regulated entities and to apply the experience gained from the implementation of the FATF Recommendations by member countries.”

Main changes to the FATF Recommendations affected areas of: the risk-based approach to regulation and compliance; transparency and beneficial ownership; customer due diligence (CDD); new technology; international cooperation; sanctions; corruption and politically-exposed persons (PEPs); financing of proliferation; and tax crimes. Of these various recommendations, the ones most affecting mobile banking and mobile payments in the United States relate to transparency, CDD, and new technologies.

2. Transparency

With regard to transparency, the FATF has strengthened its existing recommendations to require regulated entities to gather reliable information regarding the beneficial ownership and control of companies, trusts, and other legal persons or legal arrangements. The Interpretative Notes to the revised FATF Recommendations (which provide examples of the various identification documents that can be used to identify legal persons in connection with various arrangements) are intended to encourage regulated entities to implement mechanisms to require reliable, current, and accurate

---


64 See generally FATF RECOMMENDATIONS, supra note 62.
information regarding the beneficial ownership of legal persons and legal arrangements.  

FinCEN is currently conducting a rulemaking process pertaining to the development of a “CDD regulation that would clarify, consolidate, and strengthen existing CDD obligations for financial institutions and incorporate the collection of beneficial ownership information into the CDD framework.” The rulemaking is in furtherance of the broader U.S. Treasury Department plan to enhance the transparency of legal entities with respect to beneficial ownership consistent with international standards, which also involves working with the U.S. Congress to promote legislation that enhances transparency of legal entities in the company formation process.

3. Customer Due Diligence

The revised FATF Recommendations regarding CDD are more prescriptive as to the specific steps financial institutions and other regulated entities should take when conducting due diligence, particularly for higher risk dealings with particular customers and cross-border correspondent banking and other relationships. In appropriate circumstances, where the risks of money laundering or terrorist financing are assessed as low, the revised Recommendations suggest that regulated entities could be allowed to conduct simplified CDD measures, which take into account the nature of the lower risk.

---

65 FATF RECOMMENDATIONS, supra note 62, at 88-91.
4. New Technology

The revised FATF Recommendations set more rigorous standards for financial institutions with respect to the launch of new products, business practices or the use of new or developing technologies. The revised Recommendations require the FI to undertake a risk assessment prior to the launch of new products or business practices, or the use of new or developing technologies. Specifically, the revisions require the financial institution to “identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including the new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products.” Pursuant to the revisions, financial institutions are also required to take appropriate measures to manage and mitigate those risks. Mobile payments are an area of new technologies where financial institutions (and perhaps other entities developing such new mobile payments) must take appropriate measures to analyze, manage, and mitigate risks regarding money laundering and terrorist financing risks.

FinCEN has stated that the revised Recommendations on new technology clarify that FIs should conduct an anti-money laundering/counter terrorist financing risk assessment prior to the launch of new products, business practices, or the use of new or developing technologies.

---

68 FATF RECOMMENDATIONS, supra note 62, at 17.
69 FATF RECOMMENDATIONS, supra note 62, at 17.
developing technologies. 71 Freis commented that he “hope[s] that within the United States financial institutions have already understood this expectation.” 72 Freis went on to point out in comments addressing the revised FATF Recommendations and how they will apply to FIs in the United States, that several civil money penalty enforcement actions against banks “highlighted potential risks associated with the initial adoption of new technologies or use of those technologies to provide innovative products and services, and that among common elements identified was a ‘failure to identify and assess the compliance and operational risks associated with [remote deposit capture] prior to implementation.’” 73

It is not a surprise that fraud and anti-money laundering found their way into remote deposit capture transactions where paper checks are used to create “substitute checks.” Remote deposit capture is an example of how a new technology that is rapidly deployed can provide a new entry point for fraud and money laundering activities and, therefore, is a new risk vector that FIs must take into account in their BSA/AML programs.

In the consent order issued by the Office of the Comptroller of the Currency against Citibank on April 5, 2012, it required Citibank to review its BSA/AML plan on an enterprise-wide basis and conduct a comprehensive assessment of its BSA/AML program that includes “an assessment of risk associated with foreign correspondent banking, pre-paid cards and mobile banking, cash-intensive businesses, remote deposit capture, private banking, and other higher risk products, services, customers or geographies.” 74 It is clear that by including mobile banking in a list of “higher risk products,” that the regulator (here the Office of Comptroller of the Currency) believes that mobile banking is currently a higher risk category requiring comprehensive controls and monitoring under a FI’s BSA/AML program.

---

71 Freis Remarks, supra note 66.
72 Freis Remarks, supra note 66.
73 Freis Remarks, supra note 66.
5. Application of FATF Revised Recommendations to Mobile Payments

According to the FATF, “regulated entities” would include mobile payments entities that are non-FIs, but whose conduct and activities are such that they are subject to anti-money laundering and counter terrorist financing. So, to the extent that Congress makes legislative changes or FinCEN makes regulatory to BSA/AML requirements and those requirements apply to the activities carried out by non-FI mobile payments providers, such providers will have to comply with those changes.

III. MOBILE PAYMENTS IN THE UNITED STATES ARE CURRENTLY ABOUT AFFLUENCE AND ADVERTISING, NOT ACCESS

A. Mobile Payments in the United States Developing Differently than in Many Other Countries

Other countries, including developed and developing nations, have outpaced the United States in mobile payments adoption. The adoption rates of mobile payments in the United States have been hampered by well-performing electronic payments network tied to use of traditional plastic cards, and by lack of some of “the more favorable conditions that exist in other countries where mobile payments have been more widely implemented.”

In developing countries, for example, individuals are using mobile text messaging/SMS for remittances and person-to-person money transfers. Several countries have tremendous market potential for these types of services due to extensive unbanked populations and lack of comprehensive physical and/or card network banking infrastructure, in addition to widespread mobile phone use. In many of these countries, mobile payments can replace the riskier use of cash where not many payment alternatives exist (e.g., India, Kenya, Philippines). In Kenya, for

---

75 Douglass, supra note 11, at 9.
76 Douglass, supra note 11, at 10.
77 Douglass, supra note 11, at 10.
example, M-PESA was a solution to the problem of a large number of risky cash transactions and the need for families to move money from urban to rural areas. Kenya has a limited banking infrastructure, but more than 50 percent of the population has mobile phones.78 “M-PESA users can send money to other mobile phone users as well as pay for school fees, bus transfers, cab fare and other similar small purchases.”79

In some developed countries, particularly within Europe and Asia, individuals use mobile phones with NFC chips to pay for transit and/or retail purchases. Strong partnerships have developed between mobile network operators, banks, and governments in many of these countries. Many of these countries also have economies with greater reliance on cash transactions, which mobile payments can replace (i.e., credit/debit transactions not as prevalent as in the United States). Governments have also been engaged early on in the process, providing early regulatory clarity. “Asian countries lead (e.g., Japan, Korea, Singapore), but Europeans have experienced some success with mobile purchase payments and mass transit.”80 In Japan, NTT DoCoMo has the FeliCa e-wallet application that utilizes NFC. The mobile network operator provides payment services, and charges appear on the customer’s wireless bill.81

In contrast to many developed and developing countries, the United States has a very well-established electronic payments system with numerous existing options to meet consumer needs outside of mobile; and U.S. consumers have historically used cash less frequently, relying more on debit and credit card transactions. It is currently debatable whether mobile payments are meaningfully faster or easier than current payment methods widely used in the United States. The United States also relies less on mass transit, which is an industry area where mobile payments have enjoyed success in other developed countries.82

78 Douglass, supra note 11, at 12.
79 Douglass, supra note 11, at 12.
80 Douglass, supra note 11, at 11.
81 Douglass, supra note 11, at 12.
82 Douglass, supra note 11, at 12.
1. Mobile Payments Adoption by “Banked” Individuals in the United States

The Consumer Research Section of the Federal Reserve Board’s Division of Consumer and Community Affairs (DCCA) carried out an online survey in December 2011 and January 2012 regarding the use of mobile technology to access financial services and make financial decisions in the United States.83 A report regarding the survey findings was released in March 2012. Key findings of the survey with regard to the U.S. population considered “banked” were:

- Mobile phones and mobile Internet access are in widespread use (87 percent of the U.S. population has a mobile phone, and 44 percent of mobile phones are smart phones).

- The ubiquity of mobile phones is changing the way consumers access financial services (21 percent of mobile phone owners used mobile banking within last 12 months; most common uses were checking account balances or recent transactions and transferring money between accounts).

- Mobile phones are also changing the way consumers make payments (most common use was online bill payment, and 21 percent of mobile payments users transferred money directly to another person’s bank, credit card or PayPal account).

- Perceptions of limited usefulness and concerns about security are holding back the adoption of mobile financial services (58 percent of mobile phone users said their banking needs were being met without the use of mobile banking, and more than one-third of mobile phone users

---

find it easier to pay with another method or do not see any benefit from using mobile banking).  

With regard to the “banked” population in the United States, the Federal Reserve survey found that many individuals with smart phones are using mobile banking functions, and a growing number of these individuals are making mobile payments outside of the common mobile banking channel:

Consumers use a variety of methods to make mobile payments, but the most common method is to input a credit card, debit card, or prepaid card number into a mobile phone (66 percent). Other mobile payment techniques used by consumers include making payments directly from a bank account (45 percent); using Google Wallet, PayPal, or iTunes (22 percent); or adding a payment to a mobile phone bill (8 percent).

2. Mobile Payments Adoption by “Unbanked” and “Underbanked” Individuals in the United States

“A significant number of Americans do not have a bank account of any kind, and many make regular use of alternative financial services such as payday lenders, check cashers, rent-to-own services, money orders, or pawn shops.” A 2009 survey by the Federal Deposit Insurance Corporation (FDIC) found that 7.7 percent of U.S. households had no checking or savings account, and thus were defined as unbanked. An additional 17.9 percent of U.S. households had a bank account but still used an alternative financial service at least once per year, and so were classified as “underbanked.” Over the past several years, the rise in the use of

---

84 Id.
85 Id. at 12.
86 Id. at 4.
88 Id.
gift cards, stored value cards and prepaid cards has provided quasi-
bank account functionality to a large portion of the underbanked
and unbanked population.

While there may be a digital divide in the United States
regarding Internet and broadband access across the socio-economic
spectrum, the divide does not exist for mobile phone access. Ap-
proximately 75 percent of the U.S. adults in households earning
less than US$20,000 per year have a mobile phone of some type,
and 20 percent have a smart phone. The Federal Reserve’s
“Consumers and Mobile Financial Services Report” found that
mobile phone use is high among younger generations, minorities,
and those with low levels of income—“groups that are prone to be
unbanked or underbanked.” A recent survey by the Center for
Financial Services Innovation shows that individuals under the age
of twenty-five are increasingly underbanked—some as a matter of
choice—and appear comfortable with alternative financial
services.

Mobile phones have the potential to expand financial access to
the unbanked and underbanked by reducing transaction costs and
increasing the accessibility of financial products and services. In
the Federal Reserve’s report, survey results found that the
underbanked make comparatively heavy use of both mobile
banking and mobile payments, with 29 percent having used mobile
banking and 17 percent having used mobile payments within the
past twelve months. Additionally, 62 percent of the underbanked
who use mobile payments have used it to pay bills. And 10 percent
of the completely unbanked reported using mobile banking in the
past twelve months, with 12 percent of those users having made a
mobile payment.

The Mobile Payments Industry Workgroup (MPIW) summary

89 AARON SMITH, PEW RESEARCH CTR., 35% OF AMERICAN ADULTS OWN A
90 FED. RESERVE, supra note 81, at 3.
91 COREY STONE & JOSHUA SLEDGE, CTR. FOR FIN. SERV. INNOVATION,
FINANCIAL FIRST ENCOUNTERS: AN EXAMINATION OF THE FRACTURED
FINANCIAL LANDSCAPE FACING YOUTH TODAY 7 (2010), available at
of the April 24, 2012 meeting with regulators stated that:

The goal of financial inclusion is to help low and moderate income (LMI) and underserved consumers enter the financial mainstream. Emerging technologies such as mobile may decrease costs to the underserved, but ultimately it is important to move the underserved into the banking system for financial management, financial literacy and security of financial transactions. In other countries, governments are more involved in implementing mobile payments for the underserved. Is this a policy issue for the United States to consider?92

The MPIW regulator meeting summary also stated that prepaid access is expanding from card and Internet to the mobile device, and that many of the underserved are migrating directly from cash-based payments to mobile (prepaid) accounts. “This group is a growing portion of the U.S. population and represents our most vulnerable consumers who need to be educated and protected under Reg. E.”93 The MPIW summary also stated that consumer advocates are watching developments in prepaid card and mobile closely.

The FDIC and U.S. Department of Treasury are looking at mobile payments for the underserved, but they don’t have any specific current initiatives. “The MPIW does not have a targeted objective for mobile financial inclusion, but both the Federal Reserve and Treasury are interested in finding opportunities for mobile solutions to support the underserved.”94

3. Will BSA/AML Keep Unbanked Out of Mobile Payments?

With regard to the unbanked in the United States and whether the FATF Recommendations, as incorporated into BSA/AML policies, will result in exclusion of the unbanked from mobile payments.

---

92 CROW ET AL., supra note 51, at 8.
93 CROW ET AL., supra note 51, at 9.
94 CROW ET AL., supra note 51, at 9.
banking and mobile payments, the answer is probably “yes” for mobile banking, and “maybe” for mobile payments.

The reasons that individuals in the United States are unbanked are: (1) a general dislike of dealing with banks (24 percent); (2) not writing enough checks to justify having a bank account (23 percent); (3) an unwillingness to pay bank service fees and charges that are deemed too high (13 percent); (4) and banks would not allow them to open an account (10 percent). Reasons 1-3 are preference reasons, and reason 4 is a category of “unbankable” individuals.

Mobile banking customers must still have a bank account; and in order to have a bank account, individuals must have all of the elements required by the BSA/AML “customer identification program” minimum requirements—name, address, date of birth, and drivers license or ID number. A certain segment of the unbanked population in the United States that are undocumented immigrants may never be able to open a bank account, or obtain a debit card, credit card, or reloadable prepaid card without proper documentation.

However, with regard to mobile payments, that segment of the unbanked population that is truly “unbankable” due to its inability to meet minimum “customer identification program” requirements, there may be a way to turn cash into digital stored value without having to go through the “customer identification program” process. For example, if a mobile network operator allowed charges to an individual’s cell phone bill, and then the unbanked individual paid their monthly bill in cash via a walk-up bill pay option, then it would be possible for that unbanked individual to conduct certain mobile payments transactions. Similarly, if an unbanked individual paid cash for an anonymous store gift card, uploaded that card information into a mobile wallet, and then used the mobile wallet for transactions utilizing those gift card funds, there is the possibility that the unbanked individual would never be subjected to a “customer identification program” process.

In other words, those funding mechanisms for mobile payments that are issued by regulated entities subject to BSA/AML

95 FED. RESERVE, supra note 81, at 19.
requirements (debit cards, credit cards, general purpose reloadable prepaid cards, ACH) may not be accessible to an “unbankable” individual who lacks proper documentation to complete the minimum “customer identification program” (CIP) process. However, funding mechanisms that are issued or provided by unregulated entities that do not have to abide by CIP requirements may be accessible to “unbankable” individuals if the funding mechanism is ultimately cash that is turned into stored value or virtual currency by the service provider. But the ability to evade CIP requirements is ultimately tied to whether the service provider’s activities are deemed “regulated,” and how effective their CIP and BSA/AML policies and procedures are if the service provider is regulated.

B. Current Focus of Mobile Payments Initiatives

Many surveys, regulators, and consumer groups see the potential that mobile banking and mobile payments have for lowering transaction costs and fees, and ultimately moving the “bankable” population from the ranks of the unbanked and underbanked into the fully-banked. However, that is not the current focus of many mobile payments initiatives.

There have been several publications tracking the mobile payments startups that have been receiving backing and venture capital funding over the past few years. Overwhelmingly these are companies that are chasing affluent mobile payments customers, or are otherwise trying to tie mobile payments in with the larger business goals of loyalty/rewards programs, targeted advertising and couponing, predictive modeling, and using transaction data to fuel Big Data analytics on how consumers purchase and consume goods and services.96 As discussed earlier in this article, there are several start-ups that are successfully disintermediating traditional payments at the POS, such as Square, Intuit GoPay, and PayPal. But those services do not necessarily bring the unbanked or underbanked into a world of more financial services.

The race is currently on among these big three mobile wallet ventures to roll out pilot programs and sign up merchants in exclusive arrangements, and each represents four major traditional industry segments involved in mobile payments attempting to stake out their territory and make significant money in the mobile payments space: (1) existing card networks and issuing banks (Isis, Google Wallet); (2) major alternative payments providers (PayPal); (3) mobile network operators who own the “pipes,” the networks over which mobile payments and m-commerce flows (Isis, Google Wallet); and (4) technology companies who have recently discovered the payments space and want to be a player (Google, Apple?). If Apple decided to enter into the mobile wallet arena, that could be a game-changer for the race to find “one wallet to rule them all.”

The “holy grail” of the mobile wallet concept is a wallet that is: (1) universally accepted by all merchants; (2) contains multiple types of funding options (debit card, credit card, store gift card, general purpose reloadable card, ACH, provider-funded accounts, and delayed payment such as BillMeLater); (3) has a built-in and automatic merchant or bank loyalty/rewards function; (4) can be used for targeted coupons, daily deals, and geo-location and contextual advertising; (5) has the capability to interface with social media; and (6) provides incredibly rich data on consumer buying and behavior. The question is whether any one company or group of companies can pull this off.

There are, however, a few startups and established companies entering the mobile space that do present an opportunity for the unbanked and underbanked to gain more access to financial services and other perks like loyalty/rewards programs. For example, startup Lenndo combines microfinance with social media, hoping to help the world’s underbanked consumers improve their financial status by using social media to evaluate their creditworthiness.97

Loyalty program Punchcard is partnering with mobile payments service Wipit to offer business owners the ability to

create loyalty and rewards programs targeting America’s 60 million “cash-preferred” consumers. Punchcard rewards users for frequenting businesses. But instead of loyalty cards or key tags, Punchcard provides users a mobile app they can use to take photos of receipts from local merchants participating in the program. This allows users to earn “punches” on their virtual loyalty cards. It is a simple, relatively intuitive method for verifying purchases, and also serves as a way for consumers to track their loyalty points.

Wipit is a prepaid mobile account that consumers can fund using cash at any one of 10,000 retail partner locations. It is meant to be used for mobile and online purchases by consumers who lack access to a bank account. Together, Wipit and Punchcard seek to give the cash-preferred crowd their own easy-to-use digital loyalty program to replace cards and key tags. “Payments and loyalty go hand and hand,” said Andy Steuer, CEO of Punchcard.98 “Wipit’s cash-preferred consumers are value conscious and a great fit for a program like Punchcard that continues to reward them for their loyalty. We’re excited to help businesses cater to Wipit’s targeted consumer audience of more than 70 million prepaid wireless subscribers in the U.S. who are rapidly adopting smart phones.”99 And according to Wipit CEO Richard Kang, the growth of smart phones in the prepaid wireless segment has created a huge opportunity to engage cash-preferred consumers with loyalty programs and location-based promotions.100

One industry area that may greatly assist the unbanked and underbanked is the ability to use prepaid cards for mobile payments. While other developing countries moved directly from cash to mobile, the unbanked and underbanked population in the United States moved from cash, to prepaid, and then to mobile. To the extent that prepaid card issuers and distributors have mobile offerings, that could allow the segments of unbanked and


99 Id.

100 Id.
underbanked individuals currently using prepaid to use prepaid for mobile payments.

CONCLUSION

Mobile banking and mobile payment adoption in the United States is increasing and will continue to do so. FIs continue to roll out additional mobile banking services, and non-FI startups are rapidly changing the mobile payments ecosystem, and are also becoming big business. Many new mobile payments services are “disintermediating” the traditional banking relationship at both the POS and the wallet, and the United States is entering a period of a fundamental shift in how individuals conduct day-to-day purchasing and interact with their finances.

The changes being brought about, however, have not escaped the attention of various U.S. financial services regulators, and several federal and state regulators are watching the development of mobile banking and mobile payments. While current regulations are adequate to cover many existing and developing mobile banking and mobile payments offerings, regulators are aware that there may be a need for additional legislative and rulemaking measures to address any gaps in regulatory coverage. In addition, the CFPB, as directed by the Dodd-Frank Act, will take an active role in reviewing and potentially regulating non-FI mobile payments providers. The FTC and the FCC have distinct roles in mobile payments as well—the FTC for USAP, privacy, and geolocation issues for non-FIs, and the FCC for mobile network operators participating in mobile payments. The regulators are focused on an activity analysis, rather than an entity analysis, when evaluating how to apply existing regulations.

FinCEN has made it clear that it considers certain mobile payments activities to fall within its definition of money services businesses, and has made it clear that BSA/AML requirements apply to non-FI entities based on the type of activities in which they are engaged. FinCEN has also indicated that the United States will implement the revised FATF Recommendations. Revised recommendations regarding transparency of beneficial ownership, CDD, and new technologies are particularly applicable to the mobile payments arena.
With regard to the unbanked and underbanked, current activities in mobile payments have not really, truly changed the underlying payments infrastructure in the United States and how unbanked and underbanked individuals gain access to the FI accounts, debit cards, credit cards, and other “minimum necessary access devices” to participate in mobile banking and mobile payments. While there are certain service providers who can facilitate cash into a mobile payments environments, those services may find themselves more regulated in the future. Current mobile payments initiatives are more about affluence and advertising, and less about access. Perhaps as the mobile payments ecosystem evolves, there will be more offerings to aid the unbanked and underbanked in gaining access to more financial services.

**PRACTICE POINTERS**

- If you represent a technology company or startup that is going to have a payment functionality, pay close attention to regulatory issues related to money transmission, BSA/AML, and privacy/data security, and take care of any regulatory hurdles on the front end.

- In addition to financial regulators, state banking regulators, the Federal Trade Commission, and the Federal Communications Commission all have varying roles in regulating mobile payments as well.