WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 8, ISSUE 3 MOBILE MONEY SYMPOSIUM 2013

THE 2012 REVISED FATF RECOMMENDATIONS: ASSESSING AND MITIGATING MOBILE MONEY INTEGRITY RISKS WITHIN THE NEW STANDARDS FRAMEWORK

Louis de Koker[*]

Cite as: 8 WASH. J.L. TECH. & ARTS 165 (2013)
http://digital.law.washington.edu/dspace-law/handle/1773.1/1196

ABSTRACT

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

---

[*] Chair of Law, Deakin University, Australia; Visiting Professor, University of Johannesburg; Visiting Scholar, George Washington University School of Law. I gratefully acknowledge Professor Jane K. Winn, University of Washington School of Law, who provided the opportunity for this Article to be written, and Laura Powell, student editor, University of Washington School of Law, for editing the Article.

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.

implementation challenges remain. These include mobile money-related privacy and cyber-crime concerns.

TABLE OF CONTENTS

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

[1] FIN. ACTION TASK FORCE [FATF], INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION: THE FATF RECOMMENDATIONS (2012), *available at* http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%20(approved%20February%202012)%20reprint%20May%202012%20web%20version.pdf [hereinafter FATF RECOMMENDATIONS].

[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.[3] 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.

Countries and Financial Inclusion: Findings and Guidelines (World Bank First Initiative, Final Report, 2008), *available at* http://www.cenfri.org/documents/AML/AML_CFT%20and%20Financial%20Inclusion.pdf.

[3] FATF, FATF GUIDANCE ON ANTI-MONEY LAUNDERING AND TERRORIST FINANCING MEASURES AND FINANCIAL INCLUSION (2011) [hereinafter FATF 2011 GUIDANCE], *available at* http://www.fatf-gafi.org/media/fatf/content/images/AML%20CFT%20measures%20and%20financial%20inclusion.pdf.

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.

[7] INT'L MONETARY FUND [IMF], ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (AML/CFT): REPORT ON THE EFFECTIVENESS OF THE PROGRAM, 83-84 (2011), *available at* http://www.imf.org/external/np/pp/eng/2011/051111.pdf.

[8] Luis Urrutia Corral, FATF President at the XVII Caribbean Financial Action Task Force Council of Ministers Meeting (Nov. 5, 2010), *available at* http://www.fatf-gafi.org/fr/documents/repositoire/reinforcingtheglobalamlcftstructure.html.

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

---

[9] *See* Louis de Koker, *Money Laundering Control and Suppression of Financing of Terrorism: Some Thoughts on the Impact of Customer Due Diligence Measures on Financial Exclusion*, 13 J. OF FIN. CRIME 26 (2006); Jennifer Isern & Louis de Koker, *AML/CFT: Strengthening Financial Inclusion and Integrity* (Consultative Grp. to Assist the Poor, Focus Note No. 56, 2009), *available at* http://www.cgap.org/p/site/c/template.rc/1.9.37862/; World Savings Banks Inst., *Anti-Money Laundering and Combat Financing of Terrorism Rules and the Challenge of Financial Inclusion* (World Savings Banks Inst., Position Paper Doc. 0565/09, 2009), *available at* http://www.wsbi.org/uploadedFiles/Position_papers/0565%20updated.pdf; PIERRE-LAURENT CHATAIN ET AL., PROTECTING MOBILE MONEY AGAINST FINANCIAL CRIMES: GLOBAL POLICY CHALLENGES AND SOLUTIONS (2011) [hereinafter CHATAIN ET AL., PROTECTING MOBILE MONEY].

[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[11] 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.[12] 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.[13] 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.

[12] *See e.g.*, FATF, GUIDANCE ON THE RISK-BASED APPROACH TO COMBATING MONEY LAUNDERING AND TERRORIST FINANCING: HIGH LEVEL PRINCIPLES AND PROCEDURES (2007), *available at* http://www.fatf-gafi.org/media/fatf/documents/reports/High%20Level%20Principles%20and%20Procedures.pdf [hereinafter FATF 2007 GUIDANCE].

[13] Louis de Koker, *Identifying and Managing Low Money Laundering Risk: Perspectives on FATF's Risk-Based Guidance*, 16 J. OF FIN. CRIME 334 (2009) [hereinafter de Koker, *Identifying*]; 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. OF FIN. CRIME 361 (2011) [hereinafter de Koker, *Aligning Anti-Money Laundering*].

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.[14] 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.[15] These resolutions target proliferation activities of specific states, for example through targeted financial sanctions. The resolutions also aim to prevent

[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.[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.

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

[16] FATF RECOMMENDATIONS, *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 persons[17] 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.[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."[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,"[21] such simplified measures are not appropriate.

The meaning of "specific higher-risk scenarios,"[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

---

[19] *Id.* at 31.
[20] *Id.* at 64.
[21] *Id.* at 66.
[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

---

[23] *Global Standard-Setting Bodies and Financial Inclusion for the Poor: Toward Proportionate Standards and Guidance* (Global P'ship for Fin. Inclusion, White Paper, 2011), *available at* http://www.gpfi.org/knowledge-bank/publications/global-standard-setting-bodies-and-financial-inclusion-poor.

[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.[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.[26] Conservative institutions tend to overestimate risk and avoid it or adopt over-designed controls.[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.

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

---

[25] See Section III.B for questions regarding the value of these processes when CDD is simplified.

[26] Bester et al., *supra* note 2, at 158-62.

[27] Louis de Koker & John Symington, *Conservative Compliance Behaviour: Drivers of Conservative Compliance Responses in the South African Financial Services Industry* (FinMark Trust, 2011), *available at* http://www.mfw4a.org/documents-details/conservative-compliance-behavior-drivers-of-conservative-compliance-responses-in-the-south-african-financial-services-industry.html.

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.[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.[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.[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.[31] Mobile money account providers that are not licensed as such, for example

---

[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." *Id.* at 9 (Rec. 20). This has now fallen away.

[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.

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

[31] FATF RECOMMENDATIONS, *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.[32] Those agents should be included in the AML/CFT programs of providers and should also be monitored for compliance with those programs.[33]

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.[34] 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.[35]

While Recommendation 16 gives rise to extensive general compliance obligations,[36] 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.[37] 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.[38]

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." FATF RECOMMENDATIONS, *supra* note 1, at 71.

[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. *Id.*

[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.[43] 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."[44] 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.

---

[43] 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?* (FinMark Trust, Exploratory Note, 2010), *available at* http://www.cenfri.org/documents/Financial%20inclusion/2010/RICA%20impact%20on%20financial%20inclusion_final.pdf.

[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

---

[45] de Koker, *Aligning Anti-Money Laundering*, *supra* note 13, at 370.

[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

[48] de Koker, *Aligning Anti-Money Laundering*, *supra* note 13.

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

---

[50] Pierre-Laurent Chatain et al., *Integrity in Mobile Phone Financial Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing* 13 (World Bank, Working Paper No. 146, 2008), *available at* http://siteresources.worldbank.org/INTAML/Resources/WP146_Web.pdf; CHATAIN ET AL., PROTECTING MOBILE MONEY, *supra* note 9, at 37-38.

[51] Marina Solin & Andrew Zerzan, *Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks* (Groupe Speciale Mobile Ass'n, Discussion Paper, 2009), *available at* http://www.gsma.com/developmentfund/wp-content/uploads/2012/03/amlfinal35.pdf.

[52] FATF, REPORT ON NEW PAYMENT METHODS (2006), *available at* http://www.fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf.

[53] FATF, MONEY LAUNDERING USING NEW PAYMENT METHODS (2010), *available at* http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf.

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

[54] U.S. AGENCY FOR INT'L DEV., MOBILE FINANCIAL SERVICES RISK MATRIX (2010), *available at* http://bizclir.com/galleries/publications/Mobile%20Financial%20Services%20Risk%20Matrix%20July%202010.pdf.

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.

---

[57] *See* S. AFR. DEV. CMTY., PROTOCOL ON FINANCE AND DEVELOPMENT 19 (ch. 8) (2006), *available at* http://www.sadc.int/files/2913/2634/9829/PROTOCOL_ON_FINANCE_AND_INVESTMENT_-_18_AUGUST_2006-FINAL.pdf.

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

[58] *Hidden Price of a Banking Scam*, OMBUDSMAN FOR BANKING SERVICES NEWS & MEDIA RELEASES, July 20, 2009, *available at* http://www.obssa.co.za/news/2009_0720_banking_scam.htm.

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.

[60] *The Future of Money: How Mobile Payments Could Change Financial Services: Hearing Before the H. Subcomm. on Fin. Inst. and Consumer Credit*, 112th Cong. 2 (2012) (statement of Troy Leach, Chief Tech. Officer, Payment Card Indus. Sec. Standards Council LLC), *available at* http://financialservices.house.gov/UploadedFiles/HHRG-112-BA-WState-TLeach-20120322.pdf.

[61] *See, e.g.*, Princess Máxima, U.N. Secretary General's Special Advocate, Address to the FATF Plenary (June 23, 2010), *available at* https://www.fic.gov.za/DownloadContent/RESOURCES/GUIDELINES/keynote%20address%20by%20H%20R%20H%20Princess%20Máxima.pdf.

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/CTF laws against political opponents or to pursue other policy objectives.[62] 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.[63] 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).

"Moreover, since the enactment of Chinese AML Provisions (2003), the main victims were those destroyed underground banks in the coastal regions of the Southeast China. Chinese critics claimed that the People's Bank of China was using AML legislations to assist state-owned commercial banks keeping their monopolistic positions in the financial markets." Jun Tang & Lishan Ai, *Combating Money Laundering in Transition Countries: The Inherent Limitations and Practical Issues*, 13 J. OF MONEY LAUNDERING CONTROL 215, 219 (2010). *See also* David Chaikin & Jason Sharman, *APG/FATF Anti-Corruption/AML/CFT* 18-13, 69-72 (FATF/APG, Research Paper, 2007), *available at* http://www.apgml.org/issues/docs/17/APG-FATF_Report_on_Anti-Corruption_AML.pdf.

[63] Louis de Koker, *Applying Anti-Money Laundering Laws to Fight Corruption*, *in* HANDBOOK OF GLOBAL RESEARCH AND PRACTICE IN CORRUPTION 351-52 (Adam Graycar & Russell G. Smith eds., 2011).

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]

---

[64] WIKILEAKS – THE SPY FILES, http://wikileaks.org/the-spyfiles.html.

[65] "[T]he National Communications Centre (NCC) [is] 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 globalized nature 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.

[67] Louis de Koker & Nicola Jentzsch, Financial Inclusion and Financial Integrity: Aligned Incentives? 18 (July 2011) (unpublished conference paper, Univ. of Münster), *available at* http://dro.deakin.edu.au/view/DU:30041719.

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.