Balancing Financial Integrity with Financial Inclusion: The Risk-Based Approach to "Know Your Customer"

Alan Gelb

Abstract

Recognizing the importance of financial inclusion as a policy objective, regulators have endorsed the use of a risk-based approach (RBA) towards know-your-customer (KYC) requirements aimed at strengthening financial integrity. This paper considers applications of the RBA in domestic banking, mobile money and international financial transactions against the features of a rigorous RBA where both the rigor and level of due diligence and the structure and balance of incentives should be proportional to the balance of risks, including that of exclusion. The emphasis is on Customer Identification and Verification (CIV), the most practical element of KYC for small customers. RBA in the financial sector remains a work in progress. A number of countries require lower levels of due diligence for bank and mobile accounts that carry restrictions on balances and transactions and are especially suitable for poor customers, but more clarity is needed on incentives. The challenge is greater for international transactions than for most domestic financial markets because of the greater variety of risks and the need to deal with multiple regulators. The paper offers a number of recommendations, including greater attention to national identification systems as these provide the basis for CIV and to encourage the use of digital technology to shift from cash-cash wire transfers to more transparent account-account transactions between identified holders.

Center for Global Development
2055 L Street
Fifth Floor
Washington DC 20036
202-416-4000
www.cgdev.org

Ruo Shuang Lim and Julian Palma contributed much to the analysis in this paper. Thanks are due to Dilip Ratha and participants in the Working Group on the Unintended Consequences of Anti-Money-Laundering Policy for Poor Countries (Center for Global Development, 2015) for useful insights. Comments from Louis de Koker have been exceptionally valuable.

CGD is grateful for contributions from the Bill & Melinda Gates Foundation in support of this work.

Alan Gelb. 2016. "Balancing Financial Integrity with Financial Inclusion: The Risk-Based Approach to "Know Your Customer"." CGD Policy Paper 74. Washington DC: Center for Global Development.
http://www.cgdev.org/publication/balancing-financial-integrity-financial-inclusion-risk-based-approach

Center for Global Development
Independent research and practical ideas for global prosperity

CGD Policy Paper 074
February 2016

Contents

1 Introduction

Together with financial stability, financial integrity and consumer protection, financial inclusion is one of the key objectives of financial regulation. An international body, the FATF, has set a number of standards to promote the effective implementation of legal, regulatory, and operational measures to promote financial integrity and combat money laundering (ML) and the financing of terrorism (TF). Essential to operationalizing financial integrity is the need for financial institutions to know who their customers are. A financial system in which customers are anonymous is one that can easily be abused and corrupted. Such a system is also more subject to the risk of financial cronyism and related financial instability. In addition, financial institutions that are not able to establish clearly the identities of their clients will be less willing to lend to them, thus hindering financial inclusion. Appropriate know-your-customer (KYC) rules governing all financial institutions are indispensable to the efforts of the global community toward both financial integrity and financial inclusion.

The challenge in designing such rules, at both the national and the international levels, is to ensure that they are consistent with the objective of financial inclusion. A consensus on this goal is shared among policymakers worldwide who are working to develop sound KYC rules. It is reflected, in particular, in the 2012 recommendations of the FATF that explicitly mandate a risk-based approach (RBA) to be developed through the principle of proportionality. As expressed by the G20 Principles for Innovative Financial Inclusion (G20 2011): "To strike the right balance, existing regulations should be carefully analyzed to establish whether their demands on service-providers are proportionate to the risk". What is less clear is how, precisely, to implement the risk-based approach in the financial sector. What exactly are the magnitudes of the various risks and the probability that they materialize? The question is perhaps most stark for small customers. If KYC rules are not defined differently for small than for large customers, the objective of financial inclusion will be undermined. Financial services providers will find it uneconomic to apply exacting rules to the smallest accountholders and may therefore choose not to accept them as customers, or may charge them more in fees than most low-income customers can afford. More generally, KYC rules need to reflect the realities and the risks posed by those seeking access to financial services.

This paper considers the elements of a rigorous RBA and how the approach is being implemented in some of the different segments of financial systems, and offers suggestions for improvement. Section 2 summarizes the essentials of a rigorous risk-based approach, taking as an example biometric systems to identify and screen individuals. For such an approach, risks need to be quantified for any particular system to enable the tradeoff between them to be evaluated. It is necessary to understand how alternative systems affect the tradeoff frontier between risks of different types, their relative costs and their convenience for users. It is also necessary to calibrate penalties to failures that are more or less serious depending on the context. By these standards, the RBA approach taken in the financial sector has shortcomings. It does not factor in the risk of financial exclusion due to

the cost and inconvenience of responding to KYC requirements and the related likelihood that more restrictive KYC regulations will shift resource flows away from the formal financial system and towards less transparent channels that are more likely to pose ML and TF risks. There is little hard guidance on what constitutes more or less serious levels of risk and how to modulate penalties accordingly. There is also a surprising lack of attention to the basic question of how individuals are identified in the first place, and the importance of facilitating access by poor customers to strong and unique ID credentials so that financial institutions can easily and cheaply verify their identities.

Nevertheless, many countries have adopted a pragmatic risk-based approach to KYC by introducing tiered requirements for more and less restricted bank accounts.[1] Section 3 summarizes the situation in several countries. Similar principles apply in the case of mobile money, and here too there has been progress: this is covered in Section 4. By and large, the risk-based approaches discussed in these sections apply to domestic transactions.

Section 5 considers the more complex international dimension. The treatment is brief because of the comprehensive discussion in the recent Report of the Working Group on the Unintended Consequences of Anti-Money Laundering Policies for Poor Countries (Center for Global Development 2015) but a number of points are highlighted. These include the need to deal with multiple regulators, to factor in the different levels of risks presented by different financial channels, and the problem posed by the absence of any accepted global standard for identification credentials other than for machine-readable travel documents. We also stress the potential role of technology in facilitating direct account-account transfers between identified parties as opposed to less transparent cash-to-cash wire transfers. This area is in flux with the rapid growth of the "Fintech" industry which can build on the widening access to mobile money.

Section 6 concludes with recommendations, including the urgent need for more research on the tradeoffs between KYC requirements and financial inclusion to enable a stronger information base for policy.

2 The Risk-Based Approach and Its Tradeoffs

RBAs are used to set policy in many areas, ranging from infrastructure standards (the probability that spending more to straighten out a bend in a highway will prevent accidents and save lives[2]) to health treatments (the balance between the personal risks associated with immunization and the communal risks of epidemics) to biometric screening (the risk of unauthorized access to a facility or program versus the risk of wrongful denial of access). While the details differ, all such approaches embody some core elements. These include: (i)

[1] South Africa's tiered approach reaches back to the adoption of Exemption 17 in 2002. De Koker 2004 describes the challenges that it sought to address.

[2] In 2012 the US Department of transportation estimated the value of a statistical life at $9.1 million. https://www.transportation.gov/sites/dot.dev/files/docs/VSL%20Guidance_2013.pdf

for any given system it is necessary to understand the tradeoff frontier between the different risks so that the optimal balance can be chosen; (ii) recognize how different systems that could be more costly or less convenient for users will shift the frontier between the risks so that the optimal system can be chosen, (iii) how to calibrate incentives and penalties to encourage those responsible for implementing the system to achieve the optimal risk balance, and (iv) be clear on who is responsible in case risks materialize.

Biometric screening provides an illustrative example of an RBA. Any particular technology -- a fingerprint system consisting of a particular scanner and software -- will yield a particular tradeoff curve between two types of error: Type 1 -- false acceptance of an invalid identity claim (possibly fraud), and Type 2 -- false rejection of a valid identity claim (unwarranted denial of service).[3] There will also be some proportion of the population that is unable to provide fingerprints of adequate quality to use the system (failure to capture). Spending more on a higher-quality ID system, for example including iris-scans or finger-vein recognition or ten fingerprints rather than one – will increase the precision of the system, allowing both Type 1 and Type 2 errors to be reduced at the same time. This choice raises another set of tradeoffs, between system performance, cost, and user convenience – a more complex system may increase convenience by providing more options or reduce it.

The optimal choices will be very different depending on the seriousness of Type 1 errors relative to those of Type 2. For example, consider two systems, the first to control access to a nuclear facility and the second to manage access to a health insurance scheme for the poor. The first case will involve costly investments in technology, and setting the parameters of the system to minimize the possibility of unauthorized entry even if users are somewhat inconvenienced. In the second case, the aim is to deter unauthorized use but to do so at reasonable cost and without denying service to legitimate beneficiaries or discouraging them so much that they stop trying to access the program. If penalties are levied on the security provider, they would be expected to be far higher for a breach of nuclear security than for a case of unauthorized health access.

How does the RBA, as practiced in the financial sector, stack up against this model? Certainly, the principle of a RBA has been accepted. Following the adoption of the RBA as an as an optional approach in 2003 and the G20's endorsement of financial inclusion as an important additional objective, in February 2012 the FATF revised its International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation to recommend the adoption of a RBA (FATF 2015). The standards require that financial institutions and designated non-financial businesses and professions identify, assess, and understand the risk of ML and TF, and adopt a RBA. The objective is to enable

[3] The tradeoff frontier is referred to as the Detection Error Tradeoff (DET) curve between false positives and false negatives.

countries, as well as AML/CFT-regulated institutions, to apply their resources more efficiently by focusing on higher-risk areas.

Accepting financial inclusion as a regulatory objective does pose special challenges for KYC in poor countries. Inclusion introduces new costumers and may call for new providers, some with little or no previous track record in the financial sector or in the formal economy at all. Some customers may not be literate, or have the legal identification that is taken for granted by people in rich countries. With modest financial accounts and small transactions the risks are lower – especially of money-laundering.[4] At the same time the cost of KYC requirements can be high relative to the profits that can be made from small customers. Excessively stringent regulation will deter both providers and potential customers, and increase the risk that transactions shift towards cash or other, less transparent mechanisms. Table 1 shows policy interventions suggested by CGAP 2012, intended to balance financial inclusion with other objectives of financial regulation.

Table 1

Proportionality in Regulation to Balance Financial Inclusion and Risks

Financial Inclusion Policy	Possible Risk
1. Tiered product standards to allow new types of financial products	Tiered KYC requirements for low value accounts risks smurfing[5] and the use of these accounts for purposes which compromise financial integrity.
2. Tiered regulatory requirements to allow new categories of providers	Arbitrage between tiers may threaten stability. If the risks of the new class of entities may not be well understood by supervisors, they may be harder to oversee.
3. Social lending	Since this lending is typically required by mandate or moral suasion it may adversely affect solvency. Lower underwriting standards may lead to higher than expected losses. If systematic, this can compromise stability.
4. Enabling innovative approaches to payment systems.	Risks may not be well understood by users or supervisors. Operational risk could compromise integrity. Technology may also raise consumer protection challenges (compromised PINs). Challenges may be heightened for first-time users.

Source: CGAP 2012.

[4] De Koker 2011 notes that the FATF has avoided explicitly linking low value with low TF risk.

[5] Smurfing refers to the practice of breaking up a large transaction into smaller transactions that are below the reporting threshold.

With this in mind we can benchmark KYC regulations in the context of financial inclusion against the requirements for a risk-based approach. First, the practical meaning of KYC in the context of small clients should be clarified. In principle the objective of KYC concerns the sources and uses of funds -- having sufficient knowledge about the business and activities of the customer to ensure these are legitimate. This level of due diligence will not be economic for the many small accounts relevant for financial inclusion. All that can be expected is accurate knowledge of the customer's identity (Customer Identification and Verification or CIV) as well as the ability to record and analyze the sources and destination of transfers between identified accounts and to track them over time.

Federal Financial Institutions Examination Council 2014 identifies four main steps in customer identification: information collection (taking ID credentials), verification (verifying the customer against credentials and verifying the credentials themselves), checking customers against government lists, and recordkeeping. Thereafter transactions should be monitored to find suspicious patterns of activity. If needed, a Suspicious Activity Report should be filed. To be effective, the first three steps require a robust system of legal identification. Credentials should prevent an individual from holding multiple accounts under different identities. It should be possible to authenticate the credentials against a central register to ensure that they are genuine and also to authenticate the customer against the credential. Not all countries possess ID systems with these capabilities.

In addition to posing a challenge for KYC, inadequate legal identification may require financial institutions to introduce their own costly systems to combat fraud, further discouraging the extension of service to small customers. Examples include the Bank Verification Number in Nigeria and systems introduced by bank consortia in Latin America to uniquely identify clients who may hold multiple accounts. Strong ID systems benefit financial inclusion in other ways as well. The case of Kenya, which insists on consistent identification of all holders of financial accounts, illustrates the value of sharing both negative and positive credit information. This helps new customers to build up credit records.

One shortcoming is that the regulations focus on the financial sector rather than providing a balanced perspective that includes the alternatives. Certainly, no level of either ML or TF activity can be condoned in principle. In practice however, customers can resort to less transparent options outside the formal financial system. Nowhere in KYC guidance or regulations does there appear to be a clear articulation of the tradeoff between ML/TF risks for the financial sector and the risk of increasing flows through more opaque channels. Since customers can resort to less transparent options to transfer resources within countries as well as between them, it cannot be optimal to regulate to the point where ML/TF activities through the formal system are expected to be zero.

Another shortcoming is failure to provide clear guidance on the calibration of due diligence to the scale of social risks.[6] This is especially important for small customers because of the likelihood that undifferentiated requirements will exclude them from the financial sector, either because they are not able to satisfy information requirements or because the cost of due diligence will make it uneconomic for financial institutions to serve them. A number of studies indicate that KYC costs are substantial and increasing, although they do not provide a breakdown of how the costs per client relate specifically to CIV or to the size of account balances and transactions.[7]

A third shortcoming is that, while the largest fines for AML/CFT violations appear to have involved egregious cases of willful violations, financial regulations need to more clearly articulate a correspondence between penalties and the seriousness of failures to apply KYC policies. There is no clear guidance on the calibration of penalties to the scale of risks.

The RBA also requires a clear assignment of responsibility. Looking down the chain, FATF recommendations are advisory so that countries have a range of discretion in deciding how to implement them, while the framing of country-level regulations invariably leaves ultimate responsibility for KYC to the financial institutions themselves. This risk assignment conforms to the principle that risks should be assigned to those best placed to know their customers and the risks associated with them. However, when combined a lack of clarity and unpredictable penalties it can be expected to result in risk-averse behavior by both country-level regulators and financial institutions. This will further lessen the incentive to service smaller small low-profit clients if doing so could possibly expose the intermediaries to any level of regulatory risk.

In sum, the RBA applied to the financial sector remains a work in progress. While the importance of differentiating KYC according to the level of risk has been recognized and also the critical concept of proportionality, these steps may not always be translated into the specific policies and guidance needed to apply the approach in a calculated way that takes into account the incentives of financial intermediaries to service small clients and the convenience of potential customers of the formal financial system.

3 The RBA in Domestic Banking

Despite these limitations, some countries have implemented a RBA in a pragmatic way. Opening a normal bank account can require the presentation of personal ID as well as other

---

[6] While there is no standard method of measuring money laundering, the literature suggests three methods: gravity models (Walker and Unger 2009), pricing aberrations (Zdanowicz 2005) and modeling the activities of rational laundering actors (Argentiero et al. 2008). However, such estimates of the size of money laundering may not correspond to how financial institutions or regulators understand money laundering and assess related risks.

[7] See for example Elliehausen 1998, PWC 2003, Sathaye 2008, Veris Consulting 2013, Financial Times 2014, KPMG 2014. The largest costs are reported to be enhancing systems for monitoring transactions, reviewing, maintaining and updating KYC processes and records and the recruitment of qualified staff.

supplemental documentation (that can be termed "ID+") such as proof of address and a declared source of income.[8] Such documentation can be difficult to provide for certain groups, such as rural or migrant workers, other low-income informal workers or members of traditional communities. In Peru, for example, opening a standard account with a financial institution requires providing information on occupation, work experience, and the purpose of opening the account. Moreover, it is not unknown for banks to conduct third-party residential visits or interviews with the client's employer to verify their identification. Such costly due diligence will discourage financial institutions from servicing low-value customers. Some countries apply a RBA by simplifying KYC requirements for restricted accounts intended for low-income customers and subject to limits on balances and transactions. One simplification is to require only ID for these accounts and dispense with ID+. To be useful this concession requires individuals to have access to free or low-cost ID that is acceptable for KYC purposes.[9] Peru, India and South Africa offer examples of this approach; see Box 1.

In all three countries, the KYC requirements for opening a regular banking account are more stringent. In addition to proof of identity and residence (required in all three), India requires the accountholder's age, South Africa requires at least address while Peru requires additional information (above). In terms of restrictions on account balances relative to the minimum wage, Peru imposes the tightest constraint – its maximum restricted balance is equivalent to only 2 to 3 months of minimum wages. In contrast, it would take some 12-15 months of deposits equal to the minimum wage to reach the balance restrictions in India and South Africa.[10]

Offering restricted bank accounts can be a powerful force for financial inclusion. In India alone, the number of BSBD (Basic Savings Bank Deposit) accounts increased from 73.45 million in March 2010 to 243 million in March 2014. The fact that many accounts may not yet be in use is a matter of cost, services and convenience that goes beyond the issue of KYC. Use is expected to pick up as, in line with the Jhandaan-Aadhaar-Mobile (JAM)

---

[8]De Koker 2004 notes best-practice FATF KYC requirements as both obtaining and verifying: name; permanent address; date and place of birth; nationality; occupation, public position held and/or name of employer; identity number; type of account and nature of the banking relationship; and signature.

[9]Some parts of ID+ may be useful for the banking relationship. For example, a fixed address enables the bank to be in touch with the client if needed – say, if an account becomes dormant. An address will also be needed if the financial services extend to credit. For some purposes an electronic address can serve as an adequate contact mechanism. However, these considerations extend beyond the narrow focus of regulatory KYC.

[10] Minimum wage estimates: World Bank 2014 for Peru (Doing Business), Mail and Guardian 2014 for South Africa and Paycheck 2014 for India.

strategy, a wide range of subsidies and welfare payments come to be made through direct transfers into individual bank accounts. [11]

Box 1: Restricted Bank Accounts in Three Countries

India, Peru, and South Africa have implemented the risk-based approach for the formal banking sector in the form of reduced KYC requirements for certain defined bank accounts on which limits on balances and activity (both inflows and outflows) have been imposed. The accounts are restricted to domestic transactions in all three countries, with a minor exception for South Africa.

In India, opening a restricted bank account requires only a photograph and a fingerprint or signature in the presence of a bank officer. Within a year of opening the account, the holder must show proof of having applied for an Aadhaar, a unique ID number issued by the Unique Identification Authority of India (see Box 2). Proof of Aadhaar identification needs to be provided within 12 months of opening the account. The maximum balance in a restricted account may not exceed 50,000 Rupees (US$763 at the exchange rate of November 1, 2015), the aggregate of all credits in a financial year must not exceed 100,000 Rupees, and total withdrawals and transfers in one month may not exceed 10,000 Rupees.

In Peru restricted accounts require only a national ID and are limited to a balance of not more than 2,000 Soles (US$608) and daily transactions capped at 1,000 Soles.

In South Africa restricted accounts are limited to a maximum balance of R25,000 (US$1,815), a daily transactions limit of R5,000 and a monthly transactions limit of R25,000. Banks are required to take a copy of the client's identity document (Identity Book or more recently ID smartcard) but not other documentation such as proof of address or tax number. Restricted accounts may operate across the Common Monetary Area of Southern Africa (which includes Lesotho and Swaziland).

Sources: GPFI 2011. (South Africa Exemption 17, 2004), IFC 2011 (Peru: SBS Resolution 2108-2011, Article 7), Reserve Bank of India 2011 (RBI/2010-11/389).

A key question for applying an RBA is whether the government provides free legal identification that is both acceptable for KYC requirements and widely available to the poor. Table 2 summarizes the situation for the three countries. All have reasonably robust ID systems that include a high proportion of the population and mechanisms to authenticate that the customer is in fact the person shown on the ID (or, in the case of the India, the correct holder of the Aadhaar number). This capability is lacking in some other countries, where many lack official credentials (Tanzania) or it is less easy to validate holders against their credentials.

[11] Under the JAM strategy (JanDhan-Aadhaar-Mobile) the government intends to shift resources from various welfare and subsidy schemes towards direct transfers into the bank accounts of 300 million poor. See http://indiabudget.nic.in/es2014-15/echapvol1-03.pdf

Table 2

ID, Coverage and Cost

	Identification System	Requirements for ID	Coverage	Cost
INDIA	Aadhaar, a unique ID number issued by the UIDAI, serves as proof of identity and address. Biometrics are used to enroll, de-duplicate and authenticate.	Supporting documents can be presented at enrollment but a person with no documentation can enroll through an introducer who is already enrolled.	Approx. 930 million and increasing	Free
PERU	RENIEC is responsible for both the civil registry and national ID. Uniqueness is ensured using biometrics.	Certified copy of birth certificate. One color photo. Affidavit from parents or family member	Almost total coverage of birth registration and ID.	Free first-time if poor, disabled or senior citizen Replacement card costs US$6.
SOUTH AFRICA	Every citizen must apply for a national ID book at 16. This is being replaced by a smart card ID. Biometrics are taken to ensure uniqueness.	Form B1-9. A certified copy of birth certificate. Two identical, color photographs. Fingerprints are taken at the Department of Home Affairs	Almost complete coverage of birth registration and ID	Free for first time issue. US$ 13 for subsequent issue.

Peru and South Africa have somewhat similar identity systems, based on ID books and cards and relatively robust, with biographic data supplemented by biometric data.[12] With birth registration rates above 95% for both countries (UNICEF 2013) and low or even no fees, at least for the first ID. Coverage is almost complete. India offers a different ID model. Its birth registration rate is lower (though rising rapidly) and people have accumulated a

[12] However, the South African ID system suffered a severe blow to its credibility when the UK introduced visa requirements in 2009. Rampant corruption in the Department of Home Affairs had resulted in the issue of identity documents and passports to many unauthorized people http://www.digitaljournal.com/article/266934

The government is shifting over to smartcard IDs and undertaking a comprehensive re-registration. Estimates of the number of undocumented residents run as high as 4 to 5 million relative to a total population of 53 million.

plethora of identification cards for a variety of purposes. Many are low quality with few provisions against multiple registrations, forgery or fraud. The Aadhaar program seeks to remedy this, and uses multi-modal biometrics to identify and authenticate individuals.[13] It is free and legally voluntary and can be based on referrals -- anyone already enrolled in the program – an "introducer" – can vouch for those seeking to apply with no additional requirements. This makes it widely accessible and a strong foundation for basic KYC requirements. In addition, India has adopted a distinctive approach to KYC, using financial access as a carrot for ID rather than ID requirements as a stick to limit financial access (Box 2). However, until the Aadhaar number is seeded into criminal and security-related databases it will not be possible to use it to check individuals against government lists in these areas.

Box 2: Carrots vs. Sticks: Technology-driven Identification in India:

Biometric technology is rapidly helping developing countries close the "identification gap" that separates the poor from the rich countries. India's ambitious Unique Identification (UID) program has established a low-cost, ubiquitous authentication infrastructure to easily verify identities online and in real-time. Aadhaar consists of a 12-digit unique identification number stored in a centralized database and linked to biographic and biometric information—a photograph, ten fingerprints, iris scans and more recently also digital face-print —of each individual who enrolls. Although the Aadhaar scheme is voluntary, the massive effort has enrolled some 930 million people. While there has been some institutional pressure to enroll, Aadhaar appears to have been welcomed by many who have felt "unrecognized".

Identification is sometimes encouraged by making it a prerequisite for access to social programs. In South Africa for example, birth registration was spurred by making it a requirement to receive generous child allowances. However this approach can also backfire, by causing people to shy away from useful programs, such as vaccinations for children, because of a reluctance to register. India's approach, of enabling people to open restricted accounts subject to later showing proof of identity, uses financial access as a carrot for registration rather than requiring registration as barrier to financial access.

These ID systems are robust compared with many others. All use biometric technology to ensure unique identity as well as to authenticate individuals.[14] Only India has released public data on the precision of its system (false, accepts, false rejects and failure to capture) which is very high. Precision is possibly a little higher than for the other two countries because of the more extensive biometric data taken for Aadhaar registration; on the other hand, the weaker birth registration foundation in India could mean that there are fewer biographic data checks

[13] Aadhaar is not a card. Authentication is carried out remotely against the number and locally-taken biometrics against the biometrics held in the central database. For more details see Zelazny 2012. The systems in Peru and South Africa enable offline authentication against a card.

[14] Unique identity and authentication are to be understood in a statistical sense, as meaning that there will be very few cases of multiple identities and a very high degree of accuracy in authentication.

on the original identity as registered in the Aadhaar database.[15] Yet again, and somewhat offsetting this argument, birth registration as currently practiced provides a far from flawless base for an identification system. Birth certificates come in thousands of versions; they are generally paper documents with no security features or mechanisms to authenticate a holder against a certificate (DHSS 2000). Customer Identification and Verification is only as robust as the identity that an individual is able to claim and to be verified against. [16]

4 Applying the RBA to Mobile Money

As of July 2013, at least 80 countries (including 37 in Africa) had mandated or were actively considering mandating the registration of prepaid SIM cards. With the SIM as the entry point for mobile money, how this is done will have implications for financial inclusion. One question is how an estimated 2 billion current and potential mobile clients, many without robust ID credentials, are to be identified. Mandatory SIM registration poses a challenge if there is no robust, widely-held ID. The East African Community practices flexibility in allowing a range of IDs, including driver's license, employer-issued ID, voter cards and affidavits from referees, thus accommodating all the countries in a regional group where only Kenya has a fully developed national ID system. The 2015 rollout of 23 million voter cards in Tanzania that lacks a widely-held national identity document will ease the situation assuming that these cards are accepted for KYC purposes.

Another possible concern is whether the cost to the industry of managing SIM registration will have an impact on inclusion, including in access to mobile money. In one study, the annual cost of mandatory prepaid SIM card registration to the Australian mobile communications industry was estimated at $10 million (GSMA, 2013a). Prepaid users account for only 33% of all users in Australia while the figure is generally above 90% for developing countries (Ericsson, 2013). This suggests that there could be a significant burden on mobile network operators although we have no definitive data. The rapid expansion in mobile coverage in countries that do require SIM registration suggests that the cost might not be a serious barrier.

Quite a number of countries have introduced graduated KYC requirements for restricted mobile money accounts. A GSMA survey of 37 mobile money providers conducted between March and May 2015 showed that 21 of them offered accounts with simplified KYC

---

[15] For estimate of the accuracy of India's Aadhaar program see Gelb and Clark 2013. The inclusion of iris, as well as fingerprints, helps to reduce errors, including those due to exclusion because very few people have both unusable fingerprints and iris. The results also show a considerable rate of false exclusion using just one or two fingerprints to authenticate individuals.

[16] Although technology is advancing, it is not yet practical to biometrically link an infant to a credential. DNA-linked birth certificates are technically possible. An investigation into the issuing of new biometric French passports suggested that as many as 10-15% could have been issued to the wrong people because of weakness in birth registration credentials (Le Parisien 2011) (European Parliament 2012). India has begun to record the biometrics of children as young as 5. This can create a very strong lifecycle identity chain for the future.

requirements and lower limits on transactions or balances (GSMA 2015). SIM card registration can reasonably constitute the minimal KYC requirement for opening a mobile account. One example is Sri Lanka, where customers may sign up for a Basic Account which allows for balances up to 10,000 rupees (US$ 877 at November 2015 exchange rates) and transfers of up to 5,000 rupees on the basis of the identification registered when obtaining the SIM card. In exchange for undergoing verification through in-person identity reconfirmation at a mobile money agent, they may upgrade to a "Power Account" with balance limits of up to 25,000 rupees and higher valued transactions (GSMA, 2013a) (MMAI and GSMA, 2013). Haiti has practiced a similarly graduated approach where holders of mobile T-cash accounts able to transact up to 2,500 Gourdes ($44) did not need to provide additional documentation to satisfy KYC whereas those requiring larger limits needed to do so. [17] Kenya's M-PESA system is arguably the most developed mobile money transfer system in the world. By the end of 2013 the number of accounts had reached over 18 million, a very high number for a country with around 24 million adult inhabitants. M-Pesa and its associated M-Shwari service (mobile saving) offer other examples of the tiered approach to KYC (Box 3).

Box 3: The Tiered Approach to KYC for M-Pesa and M-Shwari[18]

Each individual opening an M-Pesa account must show a government-issued identity document and complete an application form that requires name, ID number, and address. Should they want to receive more than KSH 100,000 (about US$980 at the exchange rate of November 1, 2015) per year, they are required to provide a copy of the identity document in addition to the application form.

M-Pesa users are allowed to open M-Shwari (savings) accounts without any additional documentation or verification. However*, using* M-Shwari requires verification of identity. For deposits up to KSH 250,000 identity is verified against the official government (IPRS) registry. For deposits up to KSH 500,000 individuals have to present the original of the identification document used at a Safaricom shop as well as a copy. For amounts exceeding KSH 500,000, individuals have to also present the original and a copy of their PIN (Personal Identification Number) Tax Certificate. The PIN identifies a person for purposes of transacting business with Kenya Revenue Authority, other Government agencies and service providers and is processed by Kenya's Tax Department.

Any movement of funds into and out of M-Shwari has to pass through M-Pesa, where individuals would have undergone basic customer due-diligence as described above. In addition, M-Shwari transactions are subject to the M-Pesa daily transaction limit of KES 150,000.

[17] Catholic Relief Services. 2012. See also Microcapital 2012.

[18] See http://www.safaricom.co.ke/personal/m-pesa/my-m-pesa-account/how-to-register-for-m-pesa and See http://www.gsma.com/mobilefordevelopment/tiered-risk-based-kyc-m-shwari-successful-customer-due-diligence

5 The RBA in the International Context

Applying the RBA to international financial transactions is more complex than for most domestic markets because of multiple regulators and multiple channels. As noted in The Unintended Consequences of Anti-Money Laundering Policies for Poor Countries (Center for Global Development 2015) money-laundering and terrorist financing involve different risks. In particular, it is easier to identify high-risk money-laundering transactions on the basis of the amounts concerned. Terrorist financing can involve unknown counterparties and even relatively modest transactions can be considered to be risky. Where terrorist financing involves known counterparties using their listed names, CFT objectives are pursued through the international sanctions framework, comparing financial sector clients against lists such as that produced by the Office of Foreign Assets Control (OFAC).

While there has been progress in working towards a coordinated global framework, financial institutions face multiple regulators at the international level and also fragmented regulation within some countries. In the US for example, state-level bank regulators play a significant role in addition to several national regulators. This can amplify the uncertainty facing financial institutions over the level of penalties for violating AML/CTF provisions, even if penalties for small slippages in the application of KYC measures can reasonably be expected to be less than those levied for egregious cases of tax fraud and sanctions violation. The range of possible penalties is wide. US penalties levied on banks for AML program violations are up to $25,000 a day, with a separate violation registered for each day the violation continues and at each office, branch, or place of business at which a violation occurs or continues.[19] A bank that violates certain Bank Secrecy Act (BSA) provisions faces criminal penalties up to the greater of $1 million or twice the value of the transaction.[20] From January 2010 to March 2015 the average penalty levied against depository institutions in the US was $80.6 million, with the smallest being a $25,000 fine levied on Eurobank and the largest being a fine of $500 million levied on HSBC.[21] Lack of clearer guidelines on the level of penalties within so large a range will deter a risk-based approach that encourages smaller flows if these have any potential risk exposure at all.

Money Transfer Organizations (MTOs) that facilitate cash-cash wire transfers between individuals who may not have bank or mobile accounts also face a fragmented regulatory system. In the US alone, 47 states apply independent regulatory systems to such firms, creating a quagmire of costly regulation and raising uncertainty. The penalties for violations of AML laws and regulations are lower than for banks in absolute value but have a similarly wide range of uncertainty. Penalties can include fines and prison terms. The maximum

---

[19] For more details on offences and penalties, see http://www.irs.gov/irm/part4/irm_04-026-007.html

[20] See FFIEC 2014.

[21] Based on calculations using data from FinCEN. For a more complete record of enforced actions against banks, see http://www.fincen.gov/news_room/ea/

criminal penalty for violating a BSA requirement is a fine of up to $500,000 or a term of imprisonment of up to 10 years, or both. From January 2010 to March 2015 the average penalty levied against such an organization was $106,653, with the smallest being a fine of $5,000 on Altima Inc. and the largest being a fine of $1 million on a former MoneyGram Chief Compliance Officer.[22,23]

MTOs are vulnerable to "de-risking" – the decision by correspondent banks to close their accounts due to their high level of perceived risk. Barclays, the last major bank providing services to MTOs sending money to Somalia, caused concern when it announced its intention to close their accounts in 2013; the bank later agreed to maintain its relationship with the last Somali remittance company, Dahabshiil, until the latter found a replacement bank. More recently in January 2015, Merchants Bank of California, which accounted for 60-80% of American remittances to Somalia, exited relationships with Somali remittance companies, causing an estimated annual decrease of $200 million in flows (Foreign Policy, 2015, BBC, 2015), Africa Research Institute 2014). In line with an RBA such difficult cases may require special treatment but one that factors in the risks and costs of financial exclusion as well as those of ML/TF.

At the same time, technology is disrupting this business model in the area of cross-country remittances. New entrants, including the rise of the so-called "Fintech" industry, are helping the industry move towards the use of direct account-to-account cross-border transfers between identified account holders. This method of transferring funds has already become the dominant form for Kenya, because of the widespread access to M-Pesa accounts.[24] The increased financial access enabled through mobile money opens the way towards an international analogue of the graduated KYC approach now used by some countries for domestic banking and mobile finance. Cross-border transfers would then be between identified holders of financial accounts and subject to transactions restrictions along the lines of those for domestic accounts. The limits need not be uniform across all remittance

---

[22] Based on calculations using data from FinCEN. For a more complete record of enforcement actions against MSBs, see http://www.fincen.gov/news_room/ea/

[23] Based on FinCEN reports, most penalties against MTOs are for instances of AML/CTF non-compliance (such as failure to register or renew registration, and failure to adhere to reporting and recordkeeping requirements), rather than instances of actual ML and TF having taken place. This is in contrast with enforcement actions against depository institutions, which are usually for both non-compliance and actual occurrences.

[24] Strong customer identification, including the ability to look across accounts owned by a single individual, is seen as critical for effective Know Your Customer (KYC) enforcement and to ensure that Kenyan institutions are able to maintain and build correspondent relations with institutions abroad. Individuals with M-Pesa accounts can receive and send transfers to the UK subject to daily limits on each individual account holder. Direct account-account transactions within established daily limits are facilitated by Western Union for 60 countries, with MTN for 10 African countries and with Vodaphone for Tanzania and South Africa. Nineteen hawala providers were recently integrated into the system.

channels – they could be lower or higher depending on the perceived riskiness of the countries as classified by the FATF.

A final complication for global application of the RBA is the lack of quality standards for identity systems and documentation other than the ICAO's standards for machine-readable travel documents.[25] The weak foundations of many identity systems mean that even national passports, which generally enjoy international recognition, confront perceived differences in the credibility with which they identify their holders depending on the issuing government.[26] It is natural for regulators in one country to question the credibility of identity documents issued by another country. The example of international travel suggests that stronger national identity documentation may be needed in some cases to enable full cross-border application of the risk-based approach.

6 Recommendations

Financial integrity and financial inclusion are both desirable objectives. The aim is less to argue for one at the expense of the other than to strengthen the quality and coherence of regulation so as to improve the tradeoff between them. Policies to combat the use of the financial system for money laundering and the financing of terrorism should not prevent access to financial services for legitimate purposes, especially by the poor. This has been recognized as has the importance of applying a RBA but more is needed to implement such an approach on a consistent basis.

Some countries have made a good start in applying a pragmatic graduated RBA to domestic banking and mobile money with the objective of reducing barriers to financial inclusion. In addition to the direct effect of reducing a critical barrier, this approach sends a clear signal to financial institutions that the regulators recognize the importance of financial inclusion and of efforts to extend access to poor customers.

On the international side the situation is more complex. Improvements can draw on the approaches taken for domestic financial markets as well as the use of new technology to increase transparency. A consistent approach towards an RBA requires enhanced coordination of efforts toward a strong yet balanced global KYC regime, both among the

---

[25] http://www.icao.int/security/mrtd/Pages/default.aspx

[26] Border officials implement a risk-based approach through primary and secondary examinations. The primary determines if a visitor is low or high risk. It comprises a physical examination of the passport, scanning a machine readable passport, checking the resulting identity against a list of "dangerous" individuals and lost or stolen passports, and a simple oral questioning on the purpose of visit. Additionally, the officer may use interpretative heuristics to assess the risk presented by the individual. This entails looking out for individuals fitting a particular profile, for example a travel history to known terrorist training grounds, or with specific characteristics, for example a particular ethnic group. Within a minute or two, the official decides if the traveler represents sufficient risk to be subjected to a secondary examination and more intensive questioning. If deemed low risk, the traveler is allowed to enter the country (Salter, 2004). The downgrading of the South African passport by the UK was noted previously.

national authorities of different countries and, within some countries, across individual agencies. Clearer guidance from the FATF could be useful for both.

Consider the overall picture including the implications of exclusion. Excessively onerous and costly regulations on financial flows and *ex post* sanctions on violations will tend to divert financial flows into less transparent channels, including cash – even though this increases costs and reduces convenience for legitimate users. The objective of overall financial integrity cannot be achieved if financial institutions are required to pursue KYC diligence up to the point where the expected risk is zero. The permanent record of direct account-account transactions between well-identified clients should be recognized as a public good over and above the public (and private) good created by financial inclusion. Banks do not generally receive subsidies or other incentives to encourage them to service small accounts, so that the (dis) incentive regime is one-sided.

Improve knowledge of the trade-offs involved. More quantitative research is needed on the nature and extent of illicit transactions, both domestic and international, and whether conducted through the financial system or through other channels. Investigation is also needed into the trade-offs between different types and levels of regulations and penalties and how these shift transactions between financial institutions and other channels.

Scale KYC requirements to client size. In line with the risk-based approach, KYC rules should recognize the minimal risks posed by smaller customers by allowing for graduated due diligence. For both banks and providers of mobile money, less onerous KYC measures should be required for restricted accounts especially useful for low-income customers with limits on their balances and on the size of transactions. KYC rules should also support leveling the playing field between banks and mobile money providers where smaller clients are concerned: the rules need to be similar across mobile and bank providers of the same service. In the mobile money domain, SIM card registration can constitute a minimal KYC requirement for opening a restricted account.

Clarify penalties and graduate them. In keeping with the principle of proportionality, regulators need to articulate what they regard as more serious and less serious failures of KYC processes, and set rules and penalties accordingly. In an undertaking as complex as regulation of financial services, it is impossible to fully and explicitly set out all the penalties for every imaginable violation of the rules. But the need for regulatory predictability demands that the basis for assessing penalties be as clearly defined as is feasible.

For smaller accounts and limited transactions, this involves meeting two criteria. First, penalties should be set according to whether the financial institution responsible for complying with the KYC requirements has failed to do so, and *not* on the basis of whether or how many violations have actually occurred. Second, penalties should be set on a graduated basis, with reasonable upper limits. For small accounts, penalties should increase as the failure to comply becomes more serious and more persistent. For accounts that handle high-value transactions, a sliding scale of penalties for ML/TF violations should also apply.

Similarly clear indicative guidance is needed for international transactions with respect to both the basis for penalties and the severity of the infraction. Along the lines just outlined for domestic transactions, penalties relating to small transactions need to be graduated in keeping with the seriousness of the failure to comply with mandated due diligence processes. Guidance from the FATF would be useful on the size of transactions considered small enough to pose minimal risk, possibly with differentiated limits depending on the countries involved.

Strengthen national identification systems National identification systems need to be strengthened, both to facilitate compliance with KYC rules for banks and mobile providers and to support the effectiveness of the above recommendations as they apply to cross-border transactions. To meet the standards needed for adequate KYC enforcement, government-issued ID systems need to be robust enough to prevent individuals from setting up multiple accounts under different identities. In principle, they can prevent multiple restricted accounts under the same identity if financial institutions can be required to share the ID numbers of the holders. Moreover, in principle and for countries judged to have the capacity to properly identify criminals and terrorists, including those identified globally, ID systems should allow for easy verification of credentials for individuals and companies and comparison against criminal and terrorist lists.

Multilateral organizations can play two important roles in the effort toward strengthening systems of identification worldwide: first, by supporting national governments in developing countries in their efforts to improve their ID systems, and second, by working toward establishing global quality standards for identity systems and documentation. Such an effort would also support the application of a risk-based approach to international financial transactions. At present the only global ID standard is the International Civil Aviation Organization's standard for machine-readable passports. Institutions like the World Bank and other multilateral development banks have begun to take a more systematic approach toward ID systems. Financial regulators should engage with this process, for example, by encouraging financial institutions to accelerate registration by acting as enrollment agents.[27]

Encourage international account-to-account transactions for greater transparency. Looking to the future, regulation should encourage a shift away from cash-based transfers toward direct international transactions between identified holders of financial accounts. . Technology is already facilitating this shift, with the rapid spread of mobile money and digital money transmission, including through the "Fintech" sector. Advances in this direction could both reduce the cost of remittances and increase their transparency, and thereby reduce KYC concerns while fostering financial inclusion.

Especially as international remittances are often in the nature of repeat transactions, this approach could extend to establishing notional "transmission accounts" with money transfer

[27] See also De Koker and Isern 2009.

operators for otherwise unbanked customers. These would be subject to the same minimal KYC requirements as for restricted bank or mobile accounts but would serve solely as vehicles for money transmission.

To avoid disruption to cross-border remittances this recommendation would need to be implemented in parallel with initiatives to promote domestic financial inclusion. In the interim, the suggested approach is to open up restricted accounts such as those portrayed in Box 1 to similarly restricted international transactions.

Recognize the need for different approaches for especially difficult cases. In cases where a country is deemed to pose particularly severe risks to global financial integrity, a special transfer system for transactions to and from that country might be set up as a "safer corridor," available only to those local financial intermediaries and transfer recipients included on a preapproved positive list. A positive list (in the present context, one that lists only those individuals and entities permitted to conduct transactions and excludes all others) is by its nature far more restrictive than a negative list (one that lists only those who may not conduct transactions and allows all others). Hence a "safer corridor" system available only to those appearing on a positive list should be adopted only for very extreme cases, namely, those countries that have been flagged as representing a particularly serious risk for ML/TF *and* that lack the most basic capacity to apply even minimal KYC processes. Even under these conditions, a balanced assessment of the risks of shifting financial flows toward less transparent channels might reasonably support some minimum permitted level of transfers. FATF guidance on the process for establishing and operating such safer corridors would be desirable. One approach toward such a "safer corridor" has been under exploration for Somalia (Box 4, next page).

Box 4: A "safer corridor" for Somalia

The "safer corridor" concept is still under exploration, and the details have not yet been fully worked out. It would entail a third-party entity (the "safer corridor portal") taking responsibility for auditing procedures at money transfer operators to ensure appropriate compliance, audit sender and receiver identities, monitor remittance amounts for abnormal activity, and scrutinize any key intermediate correspondent channels such as clearinghouses in third-party countries. Critically, the safer corridor portal's reviews would take place on an ongoing and real-time basis to ensure that the standards required for an operator to register with the authorities are maintained. The safer corridor portal itself would also undergo rigorous external compliance checks to minimize reputational risks to those involved.[28]

In recent years a crisis emerged in remittances from the United Kingdom to Somalia, as high perceived risks prompted an increasing number of U.K. banks to end their relationships with money transfer operators sending money to Somalia. In response, in 2014 the U.K. government began the development of a U.K.-Somalia "Safer Corridor" Pilot.[29]

[28] Beechwood International. 2013.

[29] See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/471064/UK-Somalia_Safer_Corridor_Initiative.pdf

References

Africa Research Institute. 2014 Somali money matters – an update on the remittances saga. January. Retrieved April 17 2015. http://www.africaresearchinstitute.org/blog/somali-money-matters-an-update-on-the-remittances-saga-by-edward-paice/

Argentiero, Amedeo, Michele Bagella, and Francesco Busato . 2008. "Money Laundering in a Two-Sector Model: Using Theory for Measurement". European Journal of Law and Economics, 26(3): 341-359.

BBC. 2015. "US Bank to axe Somalia transfers over al-Shabab fears." Retrieved April 17 2015. http://www.bbc.com/news/world-us-canada-31159900

Catholic Relief Services. 2012. "Banking with Mobile Phones in Haiti: A Report on a T-cash Pilot Project".

Center for Global Development. 2015. Unintended Consequences of Anti-Money Laundering Policies for Poor Countries. A GCD Working Group Report. November.

CGAP 2012. Financial Inclusion and the Linkages to Stability, Integrity and Protection: Insights from the South African Experience. November. Retrieved April 17 2015. http://www.cgap.org/sites/default/files/I-SIP%20Report_1.pdf

De Koker, Louis. 2004. "Client Identification and Money Laundering Control: Perspectives on the Financial Intelligence Center Act 38 of 2001. Journal of South African Law, Volume 4: 715-46.

De Koker, Louis. 2011. "Aligning Anti-Money Laundering, Combating of Financing of Terror

and Financial Inclusion: Questions to Consider when FATF Standards are Clarified". Journal of Financial Crime, Vol. 18 No. 4: 361-386

De Koker, Louis and Jennifer Isern. 2009. "AML/CFT: Strengthening Financial Inclusion and Integrity". CGAP, August.

DHSS (Department of Health and Human Services). 2000 Birth Certificate Fraud. September.

Retrieved April 17 2015. https://oig.hhs.gov/oei/reports/oei-07-99-00570.pdf

Elliehausen, Gregory. 1998. "The cost of banking regulation: A review of the evidence." Federal Reserve Bulletin, 84(4): 252-253.

Ericsson. 2013. The End of Prepaid and Postpaid. September. Ericsson: Australia.

European Parliament.2012. Proceedings. Retrieved May 7 2015. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20120419+ITEM-011+DOC+XML+V0//EN

FATF 2015. The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. October.

Retrieved April 17 2015. http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

*FATF. *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion*. Retrieved April 17 2015. http://www.fatf-gafi.org/media/fatf/documents/reports/aml_cft_measures_and_financial_inclusion_2013.pdf

Federal Financial Institutions Examination Council. 2014. Bank Secrecy Act Anti-Money Laundering Examination Manual.
Retrieved April 17 2015.
http://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_011.htm
https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_002.htm
Financial Intelligence Center, South Africa 2004. Public Compliance Communication No. 21 (PCC21) On the Scope and Application of Exemption 17 in Terms of the Financial Intelligence Center Act No. 38 of 2001, As Amended.
Retrieved April 17 2015.
https://www.fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/PCC%2021%20Exemption%2017%20final.pdf
Financial Times. 2014. "HSBC Wrestles with Soaring Costs of Compliance." August 4. Retrieved April 17 2015. www.ft.com/cms/s/0/0e3f0760-1bef-11e4-9666-00144feabdc0.html
Foreign Policy 2015. "Bank Crackdown Threatens Remittances to Somalia". Retrieved April 17 2015. http://foreignpolicy.com/2015/01/30/bank-crackdown-threatens-remittances-to-somalia/
Gelb, Alan and Julia Clark. 2013. "Performance Lessons from India's Universal Identification Program" CGD Policy Paper, No. 20.
http://www.cgdev.org/publication/performance-lessons-india%E2%80%99s-universal-identification-program
GSMA. 2013. Tiered risk-based KYC: M-Shwari successful customer due diligence. July 8. Retrieved April 17 2015. http://www.gsma.com/mobilefordevelopment/tiered-risk-based-kyc-m-shwari-successful-customer-due-diligence
GSMA 2013a. The Mandatory Registration of Prepaid SIM Card Users" White Paper. GSMA: United Kingdom.
GSMA. 2015. Proportional Risk-Based AML/CFT Regimes for Mobile Money: a Framework for Assessing Risk Factors and Mitigation Measures. August.
GPFI. 2011. South Africa's engagement with the standard setting bodies and the implications for financial inclusion. Retrieved October 2015
http://www.gpfi.org/sites/default/files/documents/South%20Africa%E2%80%99s%20Engagement%20with%20Standard%20Setting%20Bodies%20and%20Implications%20for%20Financial%20Inclusion.pdf
G20. 2011. G20 Principles for Innovative Financial Inclusion. Retrieved April 17 2015.
http://www.gpfi.org/sites/default/files/documents/G20%20Principles%20for%20Innovative%20Financial%20Inclusion%20-%20AFI%20brochure.pdf
International Finance Corporation.2011. IFC Mobile Money Scoping Report: Peru. Retrieved April 17 2015.
http://www.ifc.org/wps/wcm/connect/ff940d804a02ec039d90fdd1a5d13d27/Peru+Public.pdf?MOD=AJPERES
KPMG. 2014. Global Anti-Money Laundering Survey. Retrieved April 17 2015.
http://www.kpmg.com/KY/en/IssuesAndInsights/ArticlesPublications/PublishingImages/global-anti-money-laundering-survey-v3.pdf

Le Parisien. 2011. "*Plus de 10 % des passeports biométriques seraient des faux"*. Retrieved May 7 2015. http://www.leparisien.fr/faits-divers/plus-de-10-des-passeports-biometriques-seraient-des-faux-19-12-2011-1775325.php

Mail & Guardian. *2014*. "Minimum Wage is No Magical Fix". June 19. Retrieved April 17 2015. http://mg.co.za/article/2014-06-19-minimum-wage-is-no-magical-fix,

Microcapital. 2012. Microcapital Brief: Mexico, Indonesia, Haiti Use Tiered Savings Account Requirements to Promote Financial Inclusion. February 10. Retrieved April 17 2015. http://www.microcapital.org/microcapital-brief-mexico-indonesia-haiti-use-tiered-savings-account-requirements-to-promote-financial-inclusion/

MMAI and GSMA 2013. "Mobile Money: The Opportunity for India". Position Paper. http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/12/MMAI-GSMA-on-Mobile-Money-in-India-for-RBI-Financial-Inclusion-Committee_Dec13.pdf

Paycheck. 2014. Minimum Wages in Central Sphere. Retrieved April 17 2015. http://www.paycheck.in/main/salary/minimumwages/central-sphere/minimum-wages-in-central-sphere-w-e-f-april-1-2014-to-september-30-2014

PWC. 2003. Anti-money Laundering Current Customer Review Cost Benefit Analysis. The Financial Services Authority: United Kingdom.

Reserve Bank of India. 2010. Opening of "Small Account. DBOD.AML.No. 77/14.01.001/2010-11. Retrieved April 17 2015. https://rbi.org.in/scripts/NotificationUser.aspx?Id=6240&Mode=0

Safaricom 2015. *How to Register for M-Pesa*. Retrieved April 17 2015. http://www.safaricom.co.ke/personal/m-pesa/my-m-pesa-account/how-to-register-for-m-pesa

Salter, Mark B. (2004). "Passports, Mobility, and Security: How Smart Can the Border Be?" International Studies Perspectives, 5(1): 71-91.

Sathye, Milind. 2008. "Estimating the cost of compliance of AMLCTF for financial institutions in Australia". Journal of Financial Crime, 15 (4): 347-363.

UNICEF. 2013. Birth Registration Data. Retrieved April 17 2015. http://data.unicef.org/child-protection/birth-registration

Veris Consulting. 2013. The Global Cost of Anti-Money-Laundering Compliance. Washington DC.

Walker, John and Bridgette Unger. 2009. "Measuring Global Money Laundering: "The Walker Gravity Model". Review of Law and Economics, 5(2): 821-853.

World Bank. 2014. Doing Business. Retrieved April 17 2015. http://www.doingbusiness.org/data/exploretopics/employing-workers

Zelazny Frances, 2012. "The Evolution of India's UID Program: Lessons Learned and Implications for Other Developing Countries" Policy Paper 008, Center for Global Development, August.

Zdanowicz, John. 2005. "Trade-based Terrorist Financing Analysis: Suspicious Trade with Al Qaeda Countries" Review of Law and Economics, 5(2): 855-878.