Overcoming the Know Your Customer hurdle: Innovative solutions for the mobile money sector

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

For more information, please visit the GSMA corporate website at www.gsma.com

Follow the GSMA on Twitter: @GSMA

Author: Kennedy Kipkemboi

Co-authors: Jim Woodsome and Michael Pisa

GSMA Mobile Money

The GSMA's Mobile Money programme works to accelerate the development of the mobile money ecosystem for the underserved.

For more information, please contact us:

Web: www.gsma.com/mobilemoney

Twitter: @gsmamobilemoney

Email: mobilemoney@gsma.com

Acknowledgements

The authors would like to thank the experts and practitioners who shared their knowledge. In particular, we would like to thank Chidozie Arinze, Oluwaseun Omotosho, and Oluseyi Osunsedo (9 Mobile); Alan Gelb and Anit Mukherjee (Center for Global Development); Thierry Artaud (MOSS ICT Consultancy); Thomas Louis Abira, Caroline Mbugua, Alfred Mugambi, and Mercy Ndegwa (Safaricom); Daniel Barrientos and Jose Manuel Ayala Marti (Tigo El Salvador); and Yiannis Theodorou, GSMA Digital Identity, and the GSMA Mobile Money team. Any errors or omissions remain the responsibility of the authors.

Contents

Introduction

Like all financial institutions, mobile money providers have a responsibility to identify their customers and understand the risks these customers may pose before providing services. When prospective customers lack formal identification, or when their identification is difficult to authenticate, providers cannot easily verify their identities or perform customer due diligence (CDD). This imposes two main constraints on digital financial inclusion: on the supply side, expensive customer identification and due diligence procedures can render low-income customers unprofitable, thereby constraining the size of the viable market; on the demand side, lengthy or inconvenient onboarding procedures can deter potential customers from signing up for mobile money services.

Efficient and effective CDD procedures can help address both constraints. On the supply side, they can reduce compliance costs for providers, making it more profitable to provide services to low-income customers. On the demand side, they can accelerate account opening, facilitate mobile access, and make it easier to conduct transactions—all of which make mobile money a more attractive service to prospective customers. These two effects combined can increase the uptake of mobile money services, boosting financial inclusion.

In this paper, we examine innovative approaches to conducting customer identification, verification, and due diligence (collectively referred to as "Know Your Customer" or KYC). These innovations can make it easier and more affordable for mobile money providers to attain new customers, especially those who are low-income or rural dwelling, while ensuring compliance with regulatory requirements. We focus on two recent trends: (1) simplifying onboarding for restricted accounts; and (2) using digital IDs to enable electronic KYC (e-KYC). While both practices are still relatively new, they have already proven to be beneficial.

After examining how different countries have implemented these practices, we draw lessons for governments and industry actors that wish to take a similar path and identify the prerequisites that must be in place for them to do so. We close by considering the steps that low- and middle-income countries can take to lay the groundwork for these policies, accounting for those with and without a strong national ID system.

1. World Bank Group (2014) Global Financial Development Report 2014: Financial Inclusion
2. World Bank Group (2018) The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution
3. World Bank Group (2018) Global Findex Database
4. Ibid

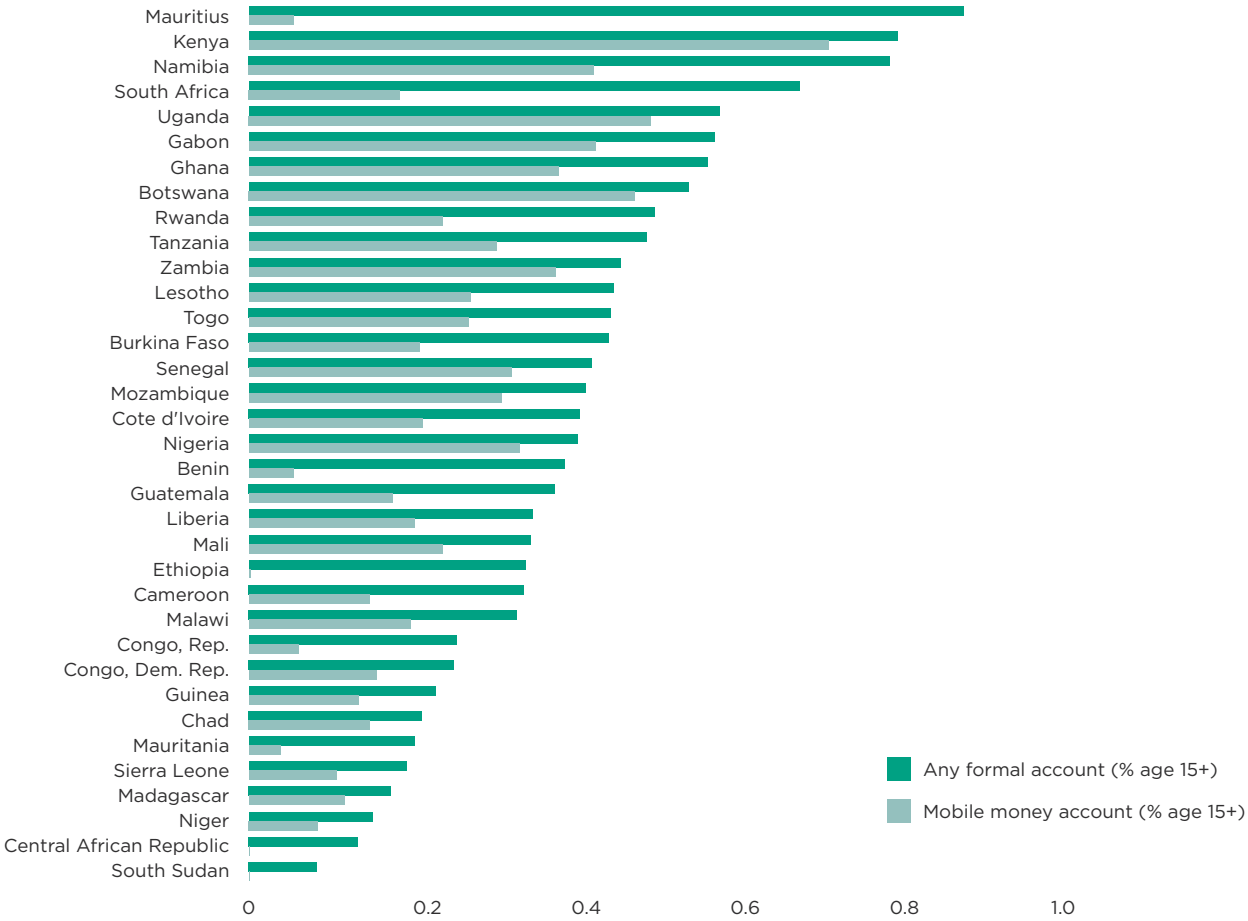
The importance of mobile money for financial inclusion

The impact of mobile money in expanding financial access to the world's poorest is well documented.[1] Due to the convenience, safety and affordability of transacting via mobile money over traditional financial institutions, the industry will continue to play a key role in bringing the 1.7 billion people who remain financially excluded into the formal financial sector.[2]

Mobile money continues to grow rapidly in low- and middle-income countries, especially in Sub-Saharan Africa which has established itself as the epicentre of mobile money. In several African countries including Kenya, Uganda, Zimbabwe, Gabon and Namibia, more than 40 per cent of the adult population have a mobile money account.[3] These gains were made possible by the rapid uptake of mobile phones in the developing world. The telecoms sector's role in financial inclusion is set to grow further, as around two-thirds of all unbanked adults globally (roughly 1.1. billion people) now have a mobile phone.[4]

Figure 1

Adults with a mobile money account or any formal financial account – Sub-Saharan Africa (Percentage of adults age 15+)



Source: World Bank Group (2018) Global Findex Database. 'Account (% Age 15+)' and 'Mobile Money Account (% Age 15+)'

The commercial and regulatory imperatives to know your customer

In the high-growth, fast-evolving context of financial services in developing markets, financial institutions must be able to identify their customers to ensure precise and accurate service provision, as well as to identify commercial opportunities. They also have commercial and regulatory incentives to prevent identity theft and fraud. Furthermore, in nearly all countries, financial institutions are required to comply with strict laws and regulations designed to counter money laundering and terrorist financing (ML/TF), as well as other forms of illicit finance, such as tax avoidance and proliferation financing.

At the international level, regulatory standards for anti-money laundering and countering the financing of terrorism (AML/CFT) regulations are set by the Financial Action Task Force (FATF), an international standard-setting body based in Paris. Over the past two decades, FATF's standards for AML/CFT regulations have been close to universally adopted.

Among other things, FATF's standards require financial institutions, including mobile money providers, to establish effective customer identification, verification, and due diligence procedures. These are often colloquially referred to as 'Know Your Customer', or KYC. This means that when mobile money providers onboard new customers, they must be able to positively identify them and collect sufficient information to assess the customer's risk of engaging in illicit finance. Providers must also conduct periodic reverification of existing customers, as their personal information and risk profiles can change over time.

Barriers to effective KYC for mobile money

Despite the success of mobile money and its potential for further growth, KYC requirements present a barrier for mobile money providers in many countries. Policymakers who wish to facilitate the expansion of digital finance can make it easier for financial institutions to meet their KYC requirements by addressing the following hurdles:

The lack of a clear regulatory framework

Mobile money providers need to know and understand the expectations of regulators, including activities that are permitted, required, and prohibited. As the Global Partnership for Financial Inclusion (GPFI), a G20 platform, has stated, "for digital financial services to flourish, there needs to be a legal and regulatory framework that is predictable, risk-based, and fair [...] and does not impose excessive, non-risk-based compliance costs."[5] China provides a good example of how clarifying regulatory expectations can boost market development. After the government issued clear regulatory guidelines for non-bank digital financial service providers in 2015, use of digital financial services in the country soared.[6]

Inflexible KYC requirements

Regulatory clarity should not be confused with taking an overly prescriptive approach, as unduly restrictive or burdensome regulations can hinder the development of innovative markets.

Instead, mobile money requires proportionate, risk-weighted regulatory flexibility.[7] This approach is enshrined in Principle 8 of the G20's "Principles for Innovative Financial Inclusion," which calls on policymakers to "build a policy and regulatory framework that is proportionate with the risks and benefits involved in such innovative products and services and is based on an understanding of the gaps and barriers in existing regulation."[8]

This principle is backed by evidence. The GSMA Mobile Money Regulatory Index indicates that countries with more proportional customer identification, verification, and KYC requirements tend to have higher levels of digital financial inclusion (see Figures 4a and 4b). Similarly, a 2015 study of 22 developing countries with mobile money services found that the eight countries where mobile money grew most rapidly had relatively light KYC requirements, whereas the eight countries where it failed generally had stringent regulations.[9]

Failure to keep pace with innovation

Regulators must be proactive in responding to fast-moving market and technological developments, as a slow regulatory reform process in a highly innovative world can inhibit the development of mobile money markets. Proactive engagement can be achieved through regular information-sharing exercises between regulators and industry representatives, as well as through more innovative approaches such as the establishment of 'regulatory sandboxes' which allow companies to experiment with new approaches to conducting KYC with fewer risks of sanction.[10] According to the Alliance for Financial Inclusion (AFI), more than 20 countries have implemented regulatory sandboxes. These proportionate regulatory approaches to fintech have been designed in line with emerging themes on digital KYC processes, biometric ID, blockchain, and regtech, among others. Mozambique, Kenya, Indonesia, Malaysia, Fiji and Sierra Leone are some of the countries that have implemented regulatory sandboxes.[11]

5. GPFI (Global Partnership for Financial Inclusion) (2017) Digital Financial Inclusion: Emerging Policy Approaches.
6. GPFI (2017) op. cit.
7. See, for example: Di Castri, S., Grossman, J., and Sihin, R. (2015) Proportional Risk-Based AML/CFT for Mobile Money: A Framework for Assessing Risk Factors and Mitigation Measures. GSMA.
8. G20 (2010) G20 Principles for Innovative Financial Inclusion
9. Evans, D., and Pirchio, A. (2015) An Empirical Examination of Why Mobile Money Schemes Ignite in Some Developing Countries but Flounder in Most
10. Ibid, pp. 11-12
11. Mohammad, A.G. (2018) Five Trailblazing DFS and FinTech Regulatory Trends Not to Miss in 2018

Lack of automation and digitisation

Automating KYC reporting requirements helps financial service providers to streamline their compliance efforts, thereby lowering the cost of onboarding and service provision. Today, regulators in many countries still rely on Excel- or paper-based reporting formats. Physical documentation during mobile money account registration is cumbersome, time-consuming, and error-prone.[12] Moreover, the storage and delivery of hard copies of customer registration documents incurs high costs. This could further be compounded by challenges related to manual authentication of the physical documents, thus negatively affecting mobile money adoption rates. It is therefore critical for regulators to consider the digitisation and automation of regulatory reporting and monitoring whenever possible.

The adoption of standardised reporting formats and definitions can facilitate the transition toward automated data sharing and analysis.[13] In Rwanda, for example, the central bank has established a new automated regulatory reporting system, with the aim of easing regulatory burdens on banks and non-bank financial institutions while also providing regulators with more accurate and detailed financial inclusion data.[14]

Overlapping regulations

Separate KYC requirements for SIM card registration and mobile money account opening create inefficiencies that exacerbate financial exclusion. While the KYC requirements for both processes are usually the same, in many countries mobile services and financial services are regulated by different entities. In many cases, mobile money, which is considered a value-added service by most mobile operators, can only be accessed through a different registration process. This presents a level of duplication considering SIM card registration is mandatory for a majority of countries with mobile money.[15] To reduce or eliminate redundancies in information provision, regulatory compliance and regulatory monitoring, policymakers should explore ways to streamline and standardise KYC requirements across different services to the greatest extent possible.[16]

Lack of a strong national ID system

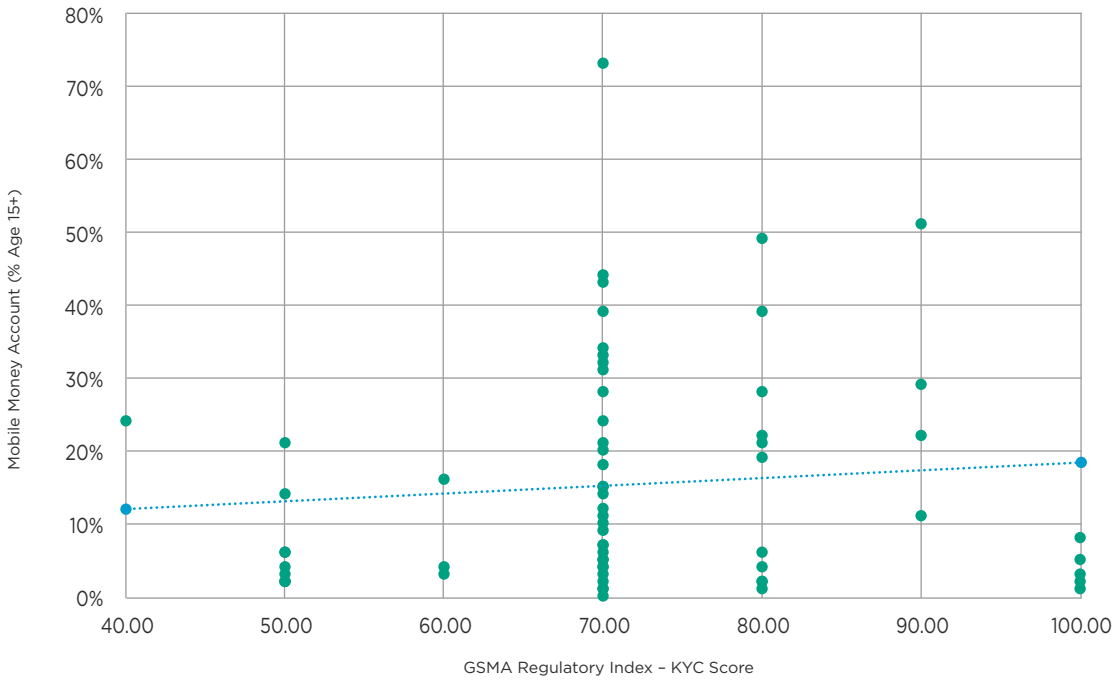
Finally, mobile money requires a supportive ID structure, since the challenge of conducting KYC is considerably greater in countries that lack a reliable digital ID system. Today, an estimated 1.1 billion people lack an officially-recognised ID and there is a significant overlap between this group and the 1.7 billion people worldwide who lack a financial account.[17] Most of the people in both categories live in Sub-Saharan Africa and Asia.

In the World Bank's 2017 Findex Survey, around 20 per cent of respondents reported that the lack of documentation was a barrier to having a financial account.[18] The challenge is more acute in some countries, such as Madagascar, where 50 per cent of financially-excluded adults cite lack of documentation as one reason they don't have an account, as well as Zimbabwe (49 per cent) and the Philippines (45 per cent).[19] Migrants and refugees are especially likely to lack officially-recognised ID.[20]

12. Puttanna, S. (2016) Digital KYC: A Key to Transform. *Finextra.*
13. GPFI (2017), op. cit.
14. Ibid
15. Theodorou, Y. and Yongo, E. (2018) Access to Mobile Services and Proof-of-Identity: Global Policy Trends, Dependencies and Risks. GSMA.
16. The GSMA has previously called for an enabling regulatory approach that includes "harmonising identity-related SIM registration requirements with the lowest tier of KYC requirements in countries where SIM registration is mandatory." See: GSMA (2018) Mobile Money Policy and Regulatory Handbook
17. The 1.1 billion figure is according to the World Bank's Identification for Development (ID4D) Program. This number is only a rough estimate of the global unidentified population. However, it provides a sense of the magnitude of the problem. For a detailed discussion of how the identity gap is defined and measured, see: Gelb, A. and Diofasi Metz, A. (2018) Identification Revolution: Can Digital ID Be Harnessed for Development? Center for Global Development.
18. It is possible that some unidentified individuals are able to obtain SIM cards through friends or relatives. In most cases, such individuals will still not be able to open their own mobile money accounts, however, as they would still not meet KYC requirements.
19. World Bank Group (2018) Global Findex Database
20. Gelb and Diofasi Metz argue that identity can be thought of as "layered." There are many different types of ID. People may lack a national ID or a birth certificate, but they may be registered for identification for access to specific programs. However, these IDs are not always as robust or secure, and may not engage in de-duplication. See: Gelb, A. and Diofasi Metz, A. (2018) Identification Revolution: Can Digital ID Be Harnessed for Development? Center for Global Development.

Figure 2a

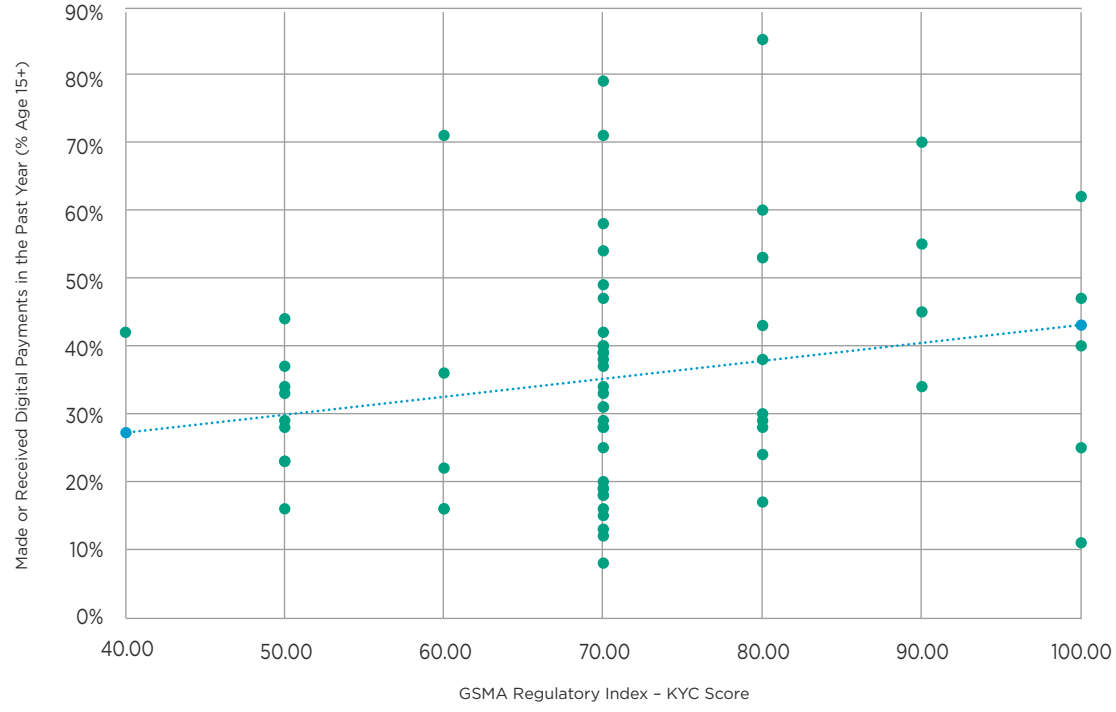
KYC regulations and digital financial inclusion: Adults with a mobile money account



Sources: GSMA (2018) Mobile Money Regulatory Index. 'KYC score'; World Bank Group (2018) Global Findex Database. 'Mobile Money Account (% Age 15+)'

Figure 2b

KYC regulations and digital financial inclusion: Adults who have made or received digital payments in the last year



Sources: GSMA (2018) Mobile Money Regulatory Index. 'KYC.'; World Bank Group (2018) Global Findex Database. 'Made or Received Digital Payments in the Past Year (% age 15+).'

Figure 3

Common mobile money KYC constraints and possible mitigations

Lack of ubiquitous ID	Allow MNOs to accept alternative forms of identification available in the country, such as student IDs and drivers' licences. Partner with MNOs to utilise their resources such as distribution channels to enrol people into the ID system.
Lack of a national ID database	Allow MNOs access to other available ID databases, such as election databases. Partner with global, regional and national stakeholders in addressing country specific identity needs.
Lack of a clear regulatory framework	Provide clear regulatory guidance on such issues as: KYC documents required to register for mobile money services; maximum number of mobile money accounts that can be registered under one customer; transaction and account limits and other related compliance checks.
High cost of storage and delivery of physical customer registration documents	Allow for electronic registration, which will eliminate the need for delivery of hard copies from remote places to the capital and related constraints while promoting efficiency.
Separate KYC requirements for SIM registration and mobile money	Allow MNOs to re-use customer information provided during SIM card registration as part of the mobile money onboarding process.

Two approaches to streamlining KYC requirements

The ability to conduct KYC efficiently and effectively is crucial in expanding access to mobile money. At present, there are two main approaches to addressing CDD-related impediments to financial inclusion. The first approach is to relax CDD requirements and compensate for the residual risk by restricting account functionality. This is referred to as simplified due diligence (SDD) or tiered know-your-customer (KYC). The second approach is to allow approved entities to query a national ID system to authenticate or verify customers' identities and, in some cases, to retrieve basic attributes about them. This is referred to as electronic KYC (e-KYC).

The approach a country should emphasise largely depends on the current scope and capabilities of its identification infrastructure, as well as the timeframe in which a solution is sought. SDD is most beneficial to countries or populations with low ID coverage. E-KYC, on the other hand, is best suited to countries with high levels of ID coverage and robust digital ID infrastructure, both of which take time to develop.

These two approaches are not necessarily mutually exclusive and in certain contexts can be deployed in combination. SDD may be utilised by countries with universal or near-universal ID coverage in order to address other CDD requirements, such as residential address verification or proof of income, which may still exclude certain populations.[21] In addition, by lowering the documentation required to open an account, SDD may also make it more convenient to open an account, therefore encouraging more customers to do so. There are, however, situations in which SDD is one of the only viable approaches, as is the case with refugees and other marginalised populations that lack any officially-recognised form of identification.

There are variations on these two approaches. For example, a promising form of SDD specific to mobile money is to allow customers to re-use the information they provided for SIM card registration, as is the case in Ghana. In addition, while e-KYC is often cited as a feature of foundational national ID systems, some countries may find that it is more viable to pursue a functional (or special-purpose) ID system.[22]

There is a growing consensus that this two-pronged approach represents the most viable path forward for addressing CDD-related financial inclusion challenges in developing countries a position that is supported by CGAP, the GPFI, ITU, among others.

21. Staschen, S. and Meagher, P. (2018) Basic Regulatory Enablers for Digital Financial Services. CGAP.
22. Mobile registration databases may also serve as effective functional ID systems, though they are not a substitute for a foundational national ID system. See: GSMA (2016) Mandatory Registration of Prepaid SIM Cards: Addressing Challenges Through Best Practice

Simplified due diligence (tiered KYC)

The first approach to addressing CDD-related impediments to financial inclusion is to simplify requirements for certain types of accounts. This approach recognises that, while ensuring universal ID coverage is a long-term endeavor, in the short-term a careful loosening of regulatory restrictions can bring more people into the formal financial system without substantially increasing the risk of abuse. Simplified due diligence has steadily gained acceptance over the past decade and has been adopted by many countries around the world. Tables 1a – c illustrate the application of tiered KYC requirements and account limitations.

The simplified due diligence (SDD) approach relaxes CDD requirements for customers and seeks to offset any residual risk created by restricting account balances or activities. FATF allows countries to offer SDD for customers, products, or market segments that regulators judge to be lower risk, and also allows CDD exemptions (as opposed to simplifications) for situations that are proven to be low-risk. In practice, however, these exemptions are quite rare. Countries such as Mexico permit a single type of SDD account, while others allow for a tiered approach, in which account functionality and CDD requirements increase progressively in line with one another, which means that as more KYC requirements are met, greater functionality is allowed. This is known as "tiered KYC" or "progressive KYC."

In simplified or tiered accounts, CDD requirements may be relaxed on such variables as the types of identification permitted, as well as the required information, documentation, levels of assurance (degree to which an identity claim is backed up), and records retention. In some countries, customer information provided during SIM card registration is enough to access basic mobile money services (See Tables 1a-1c).

Under the SDD approach, financial institutions offset any residual risk caused by gathering less information on their customers by placing restrictions on accounts that seek to limit their usefulness to money launderers and terrorist financiers. These restrictions can include what types of accounts a customer is eligible to open and the types of transactions they can make. Such accounts typically place limits on transaction value and volume, often on a per transaction basis, as well as on a daily, weekly, or monthly cumulative basis. Accounts may also be limited by the types of transactions customers can make, such as purchases, transfers, deposits, and withdrawals. Restrictions may also be geographic—customers may be limited to only making transfers domestically or, in the case of International Remittances, only to countries with low AML/CFT risk. Finally, customers may be restricted in terms of what devices or delivery channels they can utilise, including mobile phones.

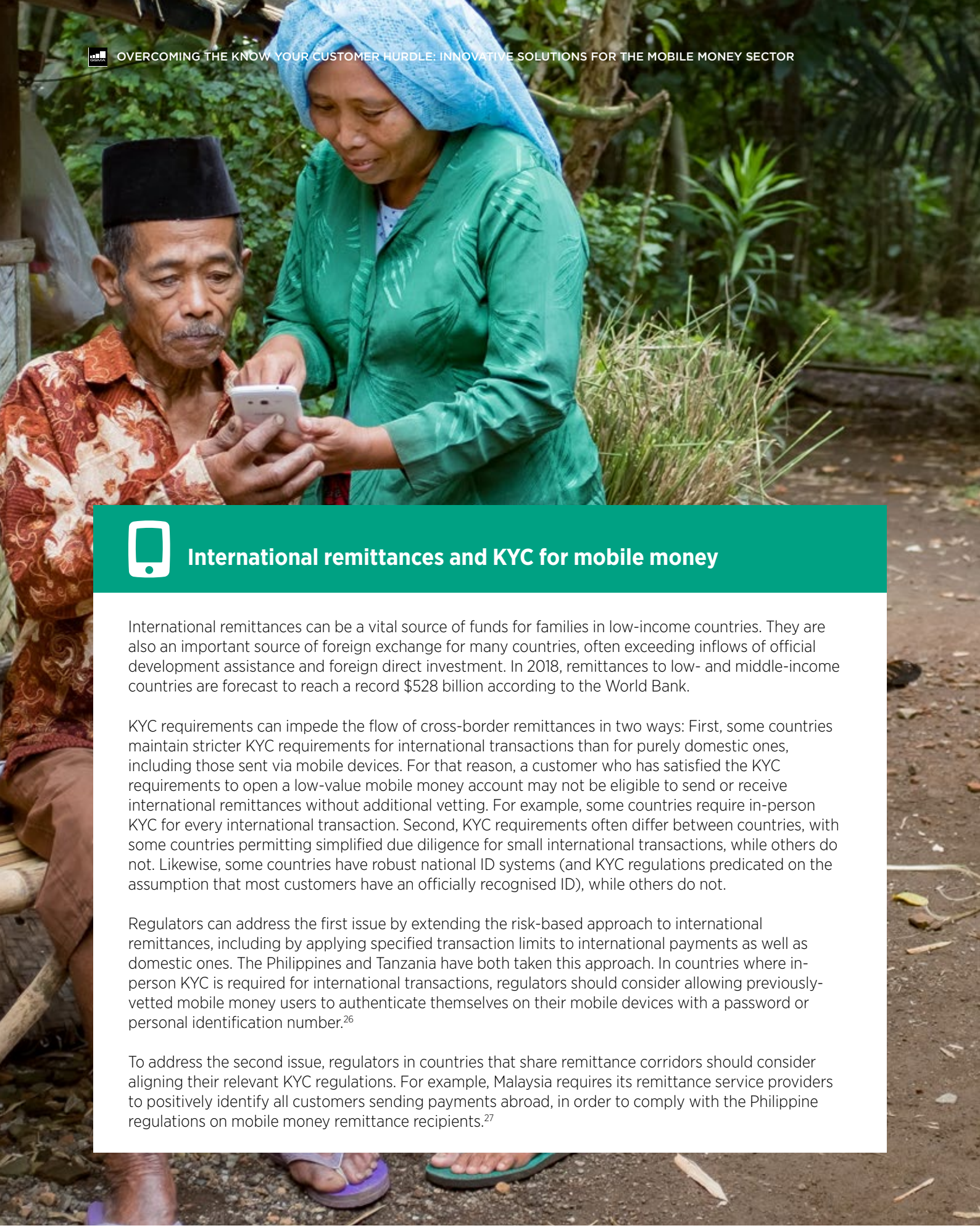
A growing number of countries have enacted SDD reforms in recent years, with at least 60 countries allowing exemptions or simplifications to CDD for certain types of customers or products.[23] In most countries, simplified or tiered CDD requirements are spelled out explicitly in regulation. In others, like South Africa, financial institutions are granted the discretion to determine their own policies. FATF permits both regulatory approaches.

Early evidence appears that such schemes can contribute to financial inclusion. For example, in the two years after Mexico introduced its tiered KYC scheme, the number of bank accounts increased by 9.1 million—a 14 per cent increase. Of these newly opened accounts, 77 per cent were accounts with simplified due diligence, with Level 1 accounts accounting for 50 per cent of the new accounts, and Level 2 and Level 3 accounts accounting for 23 per cent and 4 per cent, respectively.[24] However, more work needs to be done to evaluate the impact of these regulatory reforms on financial inclusion. Many schemes have been introduced in recent years, but as far as the authors are aware, no comprehensive assessment has been conducted of how many accounts have been opened under these new regulatory regimes.

Considerations for policymakers seeking to establish an SDD regime for mobile money

Countries that adopt SDD or tiered KYC must first consider the needs of the targeted population. For example in Brazil, the e-money regulatory framework allows customers to open a simplified account by only providing taxpayer's unique ID number and full name. The maximum account balance limit of BRL 5,000 (US $1,300) is the risk mitigation factor. In Mexico, authorities chose to limit deposits, rather than withdrawals or balances, to accommodate both transaction and savings accounts. The monthly deposit limit was set just above the average monthly household income in each of the lower economic segments of Mexico's population.[25] In the Philippines, regulators took the country's high reliance on remittances into account by extending its tiered KYC scheme to cover international as well as domestic transfers. (See "International Remittances and KYC for Mobile Money" for more detail).

23. World Bank Group (2017) Global Financial Inclusion and Consumer Protection Survey
24. Faz, X. (2013) Mexico's Tiered KYC: An Update on the Market Response
25. Ibid.



International remittances and KYC for mobile money

International remittances can be a vital source of funds for families in low-income countries. They are also an important source of foreign exchange for many countries, often exceeding inflows of official development assistance and foreign direct investment. In 2018, remittances to low- and middle-income countries are forecast to reach a record $528 billion according to the World Bank.

KYC requirements can impede the flow of cross-border remittances in two ways: First, some countries maintain stricter KYC requirements for international transactions than for purely domestic ones, including those sent via mobile devices. For that reason, a customer who has satisfied the KYC requirements to open a low-value mobile money account may not be eligible to send or receive international remittances without additional vetting. For example, some countries require in-person KYC for every international transaction. Second, KYC requirements often differ between countries, with some countries permitting simplified due diligence for small international transactions, while others do not. Likewise, some countries have robust national ID systems (and KYC regulations predicated on the assumption that most customers have an officially recognised ID), while others do not.

Regulators can address the first issue by extending the risk-based approach to international remittances, including by applying specified transaction limits to international payments as well as domestic ones. The Philippines and Tanzania have both taken this approach. In countries where in-person KYC is required for international transactions, regulators should consider allowing previously-vetted mobile money users to authenticate themselves on their mobile devices with a password or personal identification number.[26]

To address the second issue, regulators in countries that share remittance corridors should consider aligning their relevant KYC regulations. For example, Malaysia requires its remittance service providers to positively identify all customers sending payments abroad, in order to comply with the Philippine regulations on mobile money remittance recipients.[27]

26. Alliance for Financial Inclusion 2014, op. cit.
27. Alliance for Financial Inclusion 2014, op. cit.

Governments must also design restrictions that account for the risks inherent in products and the local environment, while maintaining a balance with financial inclusion policy objectives. For example, Mexico's lowest level offering is an anonymous pre-paid payment card that is restricted to domestic use and can only be used for paying for goods and services.[28] Mexican authorities decided against allowing the cards to be used to transfer funds because of the risk that they could be sent abroad to get around customs' detection of cash.[29]

If SDD regulations are not appropriately calibrated to the local context, they could either undermine the utility of such accounts (if they are overly restrictive) or fail to fully control for illicit-finance risk (if they do not have effective safeguards).

SDD and tiered KYC are likely to have the biggest impact on financial inclusion in countries that do not yet have universal ID coverage. In some circumstances, SDD may be one of the only viable approaches, as is the case with refugees and other marginalised populations that lack any officially-recognised form of identification. (See "Refugees and KYC for Mobile Money" for more detail).

However, they can also be useful in countries with universal or near-universal ID coverage in addressing other CDD requirements, such as residential address verification or proof of income, which may still exclude certain populations. In addition, by reducing the documentation required to open an account, SDD may make it more convenient, and therefore more attractive, to open an account, thereby bringing more people into the formal financial system. For example, in Cote d'ivoire one requires only either a national ID or valid passport to open a mobile money account as opposed to bank accounts which require national ID, proof of residence or business registration and an interview with a Payments Manager at BCEAO (Central Bank of West African States). SDD can also achieved by allowing a wide variety of identification documents to be used for mobile money account opening. In Mozambique, for instance, acceptable documents for mobile money account opening include the national ID, driver's licence, passport, residence permit, demobilisation card, military census card, voters card and refugee identification. This presents one of the best measures for mitigating financial exclusion on account of lack of identification.

28. FATF (Financial Action Task Force) and GAFILAT (Financial Action Task Force of Latin America) (2018) Anti-money Laundering and Counter-terrorist Financing Measures – Mexico
29. GPFI (2011) Mexico's Engagement with the Standard Setting Bodies and the Implications for Financial Inclusion

Refugees and KYC for mobile money

As of 2017, there were 25.4 million refugees around the world, many of whom consider mobile phones to be a "core survival tool," similar to food and shelter.[30] Mobile money can improve humanitarian assistance to refugees, including by facilitating cash transfers and improving their "traceability, GSMA (2017) efficiency, timeliness, and cost-effective[ness]."[31]

But conducting KYC for refugees can be difficult because most lack the documentation needed to prove their identities. In addition, many countries do not accept humanitarian IDs, such as those issued by the United Nations High Commissioner for Refugees (UNHCR) or by non-governmental organisations, for either SIM card registration or for mobile money accounts. Instead, many countries with large refugee populations, including Kenya and Turkey, require a government ID, which in turn depends on official recognition of refugee status—a process that can take months or years to complete.[32]

One way to address this issue is to explicitly recognise the validity of humanitarian IDs for KYC purposes. For example, in Jordan, which has a large Syrian refugee population, KYC regulations for mobile money allow refugees to use their UN-issued ID numbers.[33] This approach can be incorporated into a country's tiered KYC system, if it has one. For example, in Iraq, refugees that have registered with the UNHCR's Biometric Identity Management System and possess a registration certificate can open a mobile money account with restricted functionality.[34]

Another solution is to establish a closed-loop payment system designed specifically for refugees. In Kenya, which has large Somali and Sudanese refugee populations, the World Food Program (WFP) partnered with Safaricom to introduce the Bamba Chakula Initiative to distribute electronic food vouchers to refugees via mobile devices.[35] Within that closed-loop, refugees can use SIM cards with limited functionality to receive food vouchers from the WFP and then redeem those vouchers at approved vendors in the refugee camps. Refugees cannot, however, use their SIM cards to make calls, send texts, or use outside mobile money services. The WFP and the UN are responsible for verifying the identities of refugees that use the service.

30. This number includes 19.9 million refugees under the UNHCR's mandate and 5.4 million Palestinian refugees. UNHCR (2017) Global Trends 2017
31. GSMA (2017) Landscape Report: Mobile Money, Humanitarian Cash Transfers, and Displaced Populations.
32. GSMA (2017), Refugees and Identity: Considerations for Mobile-Enabled Registration
33. Claire, S. and Nautiyal, A. (2016) The Long Road to Interoperability in Jordan: Lessons for the Wider Industry
34. GSMA (2017), Refugees and Identity: Considerations for Mobile-Enabled Registration
35. Ibid

Table 1a

Tiered KYC requirements and account restrictions – Ghana[36]

Account Type	Single transaction limit	Cumulative daily transaction limit	Cumulative monthly transaction limit	Maximum account balance	KYC requirements for opening a mobile money account
All accounts	GH¢500 (US$102) (OTC only, with acceptable ID)				**Re-use of SIM card registration information:** E-money issuers that have collected and retained customer ID information previously, e.g. during registration of SIM cards or bank accounts, are allowed to use this information to satisfy relevant CDD requirements across the various account tiers without requiring the presentation of the same documentation again. In cases relying on information from SIM registration, EMIs need to validate the data against the database of the National Communications Authority within 48 hours of account opening.
Level 1: Minimum KYC account		GH¢300 (US$61)	GHS¢3,000 (US$612)	GH¢1,000 (US$204)	• **Acceptable means of identification:** Any type of photo ID that can reliably identify the customer • **Required information:** Name; Date of birth; Residential address (proof of address not required); Telephone number
Level 2: Medium KYC account		GH¢ 2,000 (US$408)	GH¢20,000 (US$4,077)	GH¢ 10,000 (US$2,039)	• **Acceptable means of identification include** National ID; Voter ID; Driver's License; NHIS (National Health Insurance Scheme) ID; SSNIT (Social Security and National Insurance Trust) ID; Passport • **Required information:** Same as Level
Level 3: Enhanced KYC account		GH¢5,000 (US$1,019)	GH¢ 50,000 (US$10,193)	GH¢ 20,000 (US$4,077)	• **Acceptable means of identification:** Same as Level 2 • **Required information:** Same as Levels 1 and 2, plus at least one of the following (to be validated by the mobile money operator): Tenancy agreement; Utility bill; Income tax certificate; Other banks' statements; Reference letter; Employer's reference letter

36. This table presents a summary of the relevant regulatory requirements. To read the regulations in their entirety, see: Bank of Ghana (2015) Guidelines for E-Money Issuers in Ghana

Table 1b

Tiered KYC requirements and account restrictions – Liberia[37, 38]

Account Type	Single transaction limit	Cumulative daily transaction limit	Cumulative monthly transaction limit	Maximum account balance	KYC requirements for opening a mobile money account
All accounts	US$100 (OTC only)				• **SIM Number**
Level 1: Entry level accounts		US$250	US$2,000	US$1,000	• **Accepted means of identification:** Authorised institutions must have written policies on the identification of people without a formal ID , listing documents acceptable for their identification, for example allowing a third party (such as clergymen, village/clan head/chief, etc. with acceptable means of identity) to act as referees.
Level 2: Accounts with full KYC		US$1,000	US$8,000	US$4,000	• **Accepted means of identification include:** Driver's license; Passport; Voter identification • **Required Information: Name;** Address; Telephone number
Level 3: Accounts with enhanced KYC		US$2,000	US$20,000	US$10,000	• **Accepted means of identification include:** Same as Level 2 • **Required information:** Same as Level 2, plus one of the following: Utility bill; Income tax certificate; Bank statement

37. This table presents a summary of the relevant regulatory requirements. To read the regulations in their entirety, see: Central Bank of Liberia (2014) Mobile Money Regulations
38. The regulations present monetary amounts in U.S. dollars or their "equivalent in Liberian dollars."

Table 1c

Tiered KYC requirements and account restrictions – Nigeria[39]

Account Type	Cumulative daily transaction limit	Maximum account balance	Other restrictions	KYC requirements for opening a mobile money account
Level 1: Low-value accounts	N50,000 (US$137)	N300,000 (US$822)	• International funds transfer prohibited.	• **Accepted means of identification:** Passport photograph • **Required information includes:** Name; Place and date of birth; Gender; Address; Telephone number • **Not required:** Bank Verification Number (BVN); evidence/verification of information provided by the customer
Level 2 Medium-value accounts	N200,000 (US$548)	N500,000 (US$1,370)	• International funds transfer prohibited.	• **Accepted means of identification:** Passport photograph • **Required information includes:** Name; place and date of birth; bender; BVN • Evidence of basic customer information is required. ID verification is required.
Level 3 High-value accounts	N5,000,000 (US$13,700)	Unlimited		• Customers are required to comply with all KYC requirements contained in CBN AML/CFT Regulation, 2009 (as amended). • BVN required.

39. This table presents a summary of the relevant regulatory requirements. To read the regulations in their entirety, see:
    1.) Central Bank of Nigeria (2013) Introduction of Three-Tiered Know Your Customer (KYC) Requirements
    2.) Central Bank of Nigeria. (2017) Review of Daily Mobile Money Wallet Transaction and Balance Limit and Bank Verification Numbers (BVN) Requirement for Mobile Money Wallet Holders

Innovative approaches to SDD

SIM card registration and remote onboarding

SIM registration for mobile money KYC

One approach to SDD that is specific to mobile money is to re-use the information customers submit when registering their SIM cards or to simply rely on the KYC that mobile network operators conduct during the SIM card registration process.[40, 41] To the extent that KYC requirements for SIM registration and mobile money overlap, this approach can eliminate redundancies by consolidating information across different mobile platforms and services.

Most countries now require customers to identify themselves and submit personal information when purchasing a mobile phone or pre-paid SIM card. Some countries, like Pakistan, require mobile money providers to capture their customers' IDs and biometric data and verify that information against the national ID registry. Others, such as Ecuador and Rwanda, require providers to verify their customers' identity against the national ID registry, but do not require the capture of biometric data. A few countries, such as Nigeria, require operators to capture their customers' information and forward it to the government, but without first verifying it against the government's registry.[42]

KYC requirements for AML/CFT are typically enforced by financial-sector regulators. In most countries, this is either the central bank or the ministry of finance. KYC requirements for SIM card regulation, on the other hand, are typically enforced by the telecom-sector regulators.[43] Under these circumstances, mobile money providers must comply with two different sets of KYC requirements. Likewise, mobile phone owners who wish to open a mobile money account must go through the KYC process twice.[44] This may be merely an inconvenience for those who have an officially-recognised ID, but for those without such an ID it raises the dual risk of being both digitally and financially excluded.[45]

Country examples of SIM registration for mobile money KYC

Several countries already allow mobile money providers to use information provided during SIM registration for their own KYC purposes. The Bank of Pakistan has allowed Telenor, the mobile network operator that runs Easypaisa, to treat SIM registration information verified against the country's national ID registry CNIC as sufficient for mobile money KYC. This has reduced onboarding time and allowed the company to offer mobile money services to customers at the point of SIM registration.[46] Telenor officials report that Easypaisa doubled its customer base in the year following the change.

In Ghana, mobile money providers may rely on the information provided during SIM card registration, as long as they validate that information with the National Communications Authority within 48 hours of account opening,[47] while in Haiti, mobile money customers can make transactions of up to 2,500 Gourdes (roughly $44) without providing additional KYC information. In Sri Lanka, the identification provided during SIM card registration can be used to open a basic mobile money account. These accounts may hold balances up to 10,000 rupees ($877) and allow transfers of up to 5,000 rupees.[48]

40. Gelb (2016) Balancing Financial Integrity with Financial Inclusion: The Risk-Based Approach to 'Know Your Customer
41. GSMA (2016) Mandatory Registration of Prepaid SIM Cards: Addressing Challenges Through Best Practice
42. Theodorou, Y. and Yongo, E. (2018) Access to Mobile Services and Proof-of-Identity: Global Policy Trends, Dependencies and Risks. GSMA.
43. GSMA (2018) 'GSMA Mobile Money Policy and Regulatory Handbook'.
44. Ibid
45. Theodorou, Y. and Yongo, E. (2018) op.cit.
46. Lowmaster, K. and Cherepennikova, D. (2018) Private Sector Economic Impacts from Identification Systems. World Bank Group.
47. Bank of Ghana (2015) Guidelines for E-Money Issuers in Ghana
48. Gelb (2016), op. cit.

Remote onboarding

Another approach that is used to support SDD is remote onboarding. Instead of visiting an agent in person to open an account, customers may instead do so by phone or on a computer. Paraguay now allows customers to register by taking a picture of their ID card and a picture of themselves and sending the two in together. Thailand introduced regulations in 2016 for remote customer onboarding, which have been interpreted to include registering via videoconference. In Mexico, customers can open Level 1 and Level 2 accounts either via mobile phone or online, subject to additional ID verification and monitoring procedures by providers, which must be authorised by their supervisory authority with feedback from the Ministry of Finance.[49] Finally, Malaysia's central bank, Bank Negara Malaysia, has laid the regulatory groundwork for e-KYC services for the money services business (MSB) industry, with a particular view toward streamlining the KYC process for users of online and mobile remittance services.[50] The regulations permit the MSB industry to conduct remote onboarding of users through the use of video calls and 'selfie' photos (using facial recognition technology).[51]

Lessons learned for policymakers seeking to use SIM card registration or remote onboarding for mobile money KYC

Harmonising KYC requirements for SIM cards and lower-tier mobile money accounts can foster financial inclusion by reducing redundant regulations and allowing mobile phone penetration and mobile money penetration to proceed in greater alignment.[52] And it can do so at relatively low cost. The key hurdle is interagency coordination. Getting financial regulators to coordinate telecom regulators will in most cases require a top-down effort from the highest levels of government making this a priority.

Policymakers and regulators need to clarify under what circumstances remote onboarding is allowed, as well as what technologies or intermediaries may be used. They may specify that risk controls be boosted in other areas, such as in transactions monitoring.

49. FATF (Financial Action Task Force) (2013-2017) FATF Guidance: Anti–Money Laundering and Terrorist Financing Measures and Financial Inclusion
50. Bank Negara Malaysia (2017) Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) - Money Services Business (Sector 3) (Supplementary Document No. 1)
51. Bank Negara Malaysia. (2017) Implementation Guidance on e-KYC by MSB Industry Frequently Asked Questions and Answers (FAQs)
52. GSMA (2018) GSMA Mobile Money and Regulatory Policy Handbook. See also: Theodorou, Y. and Yongo, E. (2018) op. cit.

Digital ID and queriable ID systems for e-KYC

While simplified due diligence is an effective way to improve financial access for populations that would otherwise lack the requisite documentation, queryable digital ID systems offer greater promise over the long term.

The World Bank defines digital ID as "a collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and is used for electronic transactions. It provides remote assurance that the person is who they purport to be." As economic and social activity has migrated online and become increasingly mediated by mobile devices, digital ID platforms have become critically important to being able to access services and an essential element of modern infrastructure.[53,54]

Digital ID can improve the onboarding process by reducing or eliminating paper-based procedures and record-keeping. This reduces operational costs, which, in turn, should improve the profitability of mobile money providers with respect to servicing low-income and rural customers. Cost savings can also be passed on to consumers through more affordable transaction charges. Digital ID can also link systems together to facilitate the transmittal of information and make identity verification more automatic and secure. Finally, digital ID systems with broad coverage and easy accessibility reduce the need for service providers to accept a wide range of credentials and can replace the need for SDD, as has been the case (until recently) in India.

E-KYC has other advantages over SDD, especially paper-based SDD. While simplifying SDD offers flexibility in accepted documentation, it does not resolve the physical documentation risks and associated costs which paper-based ID inevitably entails. Digital ID solves both the issue of cost as well as responding to security and reliability concerns. Further, efforts to increase flexibility on who can open an account (and where) can be accelerated with a reliable digital ID system.[55]

The role of biometrics in digital ID systems

Biometric authenticators use distinctive physiological or behavioural characteristics to uniquely identify users. A number of characteristics can be used, the most common of which are fingerprints, iris patterns, and facial geometry. Voice recognition technology is also being widely adopted for certain business applications, such as call centres.[56]

Though biometrics are often discussed in conjunction with digital ID systems, they are not synonymous. One of the world's most successful digital ID systems, Estonia's eID, does not use biometrics, but instead employs a chip card (also called a smart card) and a personal identification number (PIN).[57] Kenya's ID system also relies on PINs.

However, biometrics are an increasingly common feature of digital ID systems. Most new digital ID systems use biometrics, and many legacy systems are being reconfigured to support this technology. This is for a few reasons. First, biometrics are generally considered to be more secure and easier to use, in comparison to other authentication factors, such as passwords, PINs, and cards. Biometric fraud requires illicit actors to obtain and replicate the user's biometric trait—this is not impossible, but it is difficult. Also, unlike passwords, PINs, and cards, biometric features cannot be lost, stolen, or forgotten.

53. World Bank Group and GPFI (2018) G20 Digital Identity Onboarding
54. Atick, J.. and Safdar, Z. (2014) Digital Identity Toolkit: A Guide for Stakeholders in Africa. World Bank Group.
55. World Bank Group and GPFI (2018) op. cit.
56. See, for example, Safaricom's Jitambulishe service
57. Atick, J.. and Safdar, Z. (2014), op.cit.

Biometrics are now an affordable, mature, and widely used technology—so much so that they are increasingly viewed as a commodity product.[58] According to a recent report to UK Financial Conduct Authority (FCA), biometrics are now regarded as one of the most mature and instantly useful elements of technology in AML.[59]

Biometric digital ID systems may be especially useful in developing countries that lack a strong civil registry. Developed countries such as Estonia can afford to rely on PINs and smart cards, because their systems are backed by a strong pre-existing civil registry.

Foundational vs. functional digital ID systems

ID systems are often referred to as foundational or functional.[60] Foundational systems are general purpose systems that supply users with an ID that can be used across different services and platforms. Functional systems are special-purpose systems that supply users with an ID that can be used to access a particular platform or service. Civil registries (e.g., birth certificates) and national ID systems are foundational systems. Drivers' licenses, ration cards, pension cards, passports, and voter IDs are all functional IDs. Foundational IDs are almost always issued by the central government, whereas functional IDs may be issued by government agencies, the private sector, or through a public-private partnership. Private-sector functional IDs may be considered a form of legal ID if governments recognise them as such.

In general, foundational ID systems are considered better investments for governments, but both approaches contain potential trade-offs, especially in a developing-country context. A foundational ID system has the potential to produce greater economic and societal returns over the long run, since it can serve as a platform for a variety of applications and services, possibly including some that were not conceived when the system was first established. However, because foundational systems may initially lack a clear and specific purpose, they can languish if the political and organisational will to see them through is weak or unsustainable. For that reason, most ID systems in Africa are underfunded and under-resourced as per a recent survey by the World Bank Group.[61] Moreover, foundational ID systems can exclude the poor, migrants, refugees, and other marginalised groups if the systems are built around proof of citizenship or legal residence.

Functional ID systems have the opposite problem. While they benefit in the short run from having a clear purpose — which can make it easier for governments to gain political support and justify investment — they also can be difficult to use beyond their original role and integrate into other systems. A country with multiple functional ID systems may find that it has spread its resources too thin, and thus may have a hard time sustaining such systems over time.

National ID systems for e-KYC

In most developing countries, national ID systems represent the most viable opportunity for reducing their undocumented populations. The feasibility of using e-KYC for mobile money, however, depends on the broader ID ecosystem in a country. Hence, questions related to the design and use of digital ID for mobile money overlap, to a large degree, with broader issues related to the coverage, functionality, and accessibility of the national ID system.

Most countries now have a form of national ID system in place and many of these systems are digitised and employ biometrics to authenticate their users' identities. In 2017, the World Bank reported that 175 countries (out of 196 surveyed) had some type of national ID system in place.[62] Of these, 161 were digitised and 83 collected biometric features. Few of these yet allow third parties to access them to validate the identities of customers.[63]

A digital national ID system is a platform upon which a variety of services can be built. Increasingly, national ID systems are being linked to third-party functions and services, both public and private.[64] These include elections, financial services, healthcare, and security, among others. The ability of third-party service providers to query digital ID systems may confer a number of public benefits. These can include a reduction in the cost of transactions that require identification; the development of new services that depend on automatic and inexpensive identification; and a reduction in the need for private companies

58. Gelb, A. and Diofasi Metz, A. (2018), op. cit.
59. PA Consulting Group (2017) New Technologies and Anti–Money Laundering Compliance
60. Gelb and Diofasi Metz suggest that India's Aadhar system may require the creation of a third category—one that is truly "ID first," and is not linked to citizenship or even residence. See: Gelb, A. and Diofasi Metz, A. (2018), op. cit. 61. World Bank Group (2017) The State of Identification Systems in Africa: A Synthesis of Country Assessments
62. World Bank Group (2018)c. Identification for Development (ID4D) Global Dataset
63. The GSMA identifies 16 countries that allow mobile network operators to validate customers identities' against a database when those customers register a SIM card. See: Theodorou, Y. and Yongo, E. (2018) op. cit.
64. Lowmaster, K. and Cherepennikova, D. (2018) Private Sector Economic Impacts from Identification Systems. World Bank Group.
65. Lowmaster, K. and Cherepennikova, D. (2018), op. cit.

to collect and store customers' personal information themselves.[65] Moreover, the utilisation of the national ID system by third-party service providers may produce a positive feedback loop, insofar as it encourages people to enroll in the system and keep their personal information current and accurate. For these reasons, the International Telecommunications Union (ITU) has recommended that "countries with a national identity system, or another similar market-wide identity system, should recognise this as a public resource. Access to this directory, and use of it, should be open to all regulated digital financial services providers at a reasonable cost."

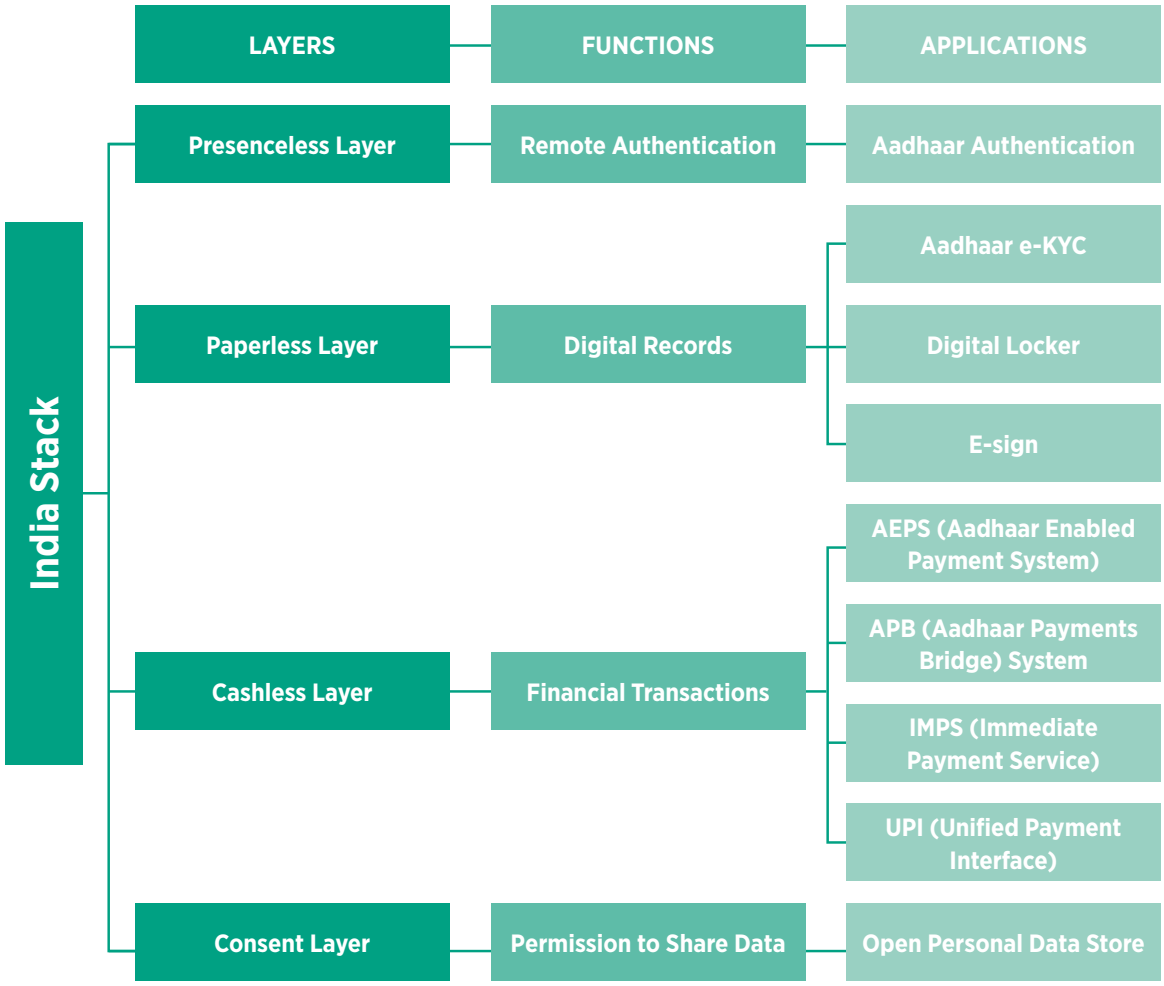
The case of India

India's unique identity or Aadhaar program has rightly captured the world's attention for its innovativeness, sophistication, rapid growth, and sheer scale. The program assigns each registrant a unique 12-digit ID number that is linked to minimal personal information (including name, gender, date of birth, and a digital photo) and biometric information (fingerprints and iris scans) that can be used for authentication.[66] Since the first Aadhaar ID number was issued in 2010, more than 1.2 billion people (nearly 90 per cent of the population in India) have enrolled in the program.

The original stated purpose of Aadhaar was to reduce leakage and fraud in the government's sprawling subsidy program by removing "ghost beneficiaries" and duplicate entries on its rolls. However, use of the ID quickly spilled over to other areas, including filing income tax returns, authenticating payments, and digitally signing documents. The government helped to expand the system's functionality by building out the country's digital infrastructure and working with tech experts to create a collection of open APIs (application programming interfaces) called "India Stack," which government agencies, businesses, and developers can use to connect to the system.[67]

Figure 4

The four layers of India stack



66. Clark, J. (2018) Public Sector Savings and Revenue from Identification Systems: Opportunities and Constraints. World Bank Group.
67. Indiastack.org

Using Aadhaar-based e-KYC, customers can electronically provide their demographic and personal information - including proof of identity, proof of address, date of birth, and gender - to financial providers, who verify this information using Aadhaar authentication in real time, reducing both the paperwork required and time spent.[68] A recent World Bank report cites an estimate that moving to e-KYC reduces the average cost of verifying customers from $15 to $.0.50.[69] Similarly, most estimates suggest that customer verification can be done in seconds using e-KYC compared to 5-7 days when done manually. The use of Aadhaar for KYC has, however, raised privacy concerns. For example, using the tool for KYC authentication provides financial service providers with additional personal information about their customers, which poses a potential data privacy risk. One means of mitigating this is to only share the minimum relevant information necessary with third parties, without exposing customers' personal information, as implemented by the UIDAI.[70]

Other examples of national ID systems with mobile money capabilities

In **Kenya**, mobile money operators can verify onboarded customers against the government database in real-time, creating efficiencies and assurances of data accuracy. A fee is charged to validate against the database, which adds to the cost of customer acquisition.[71] Depositors in Kenya who use the M-Shwari mobile savings account can use their national IDs to verify their identities, in turn receiving higher balance limits on their savings accounts, as well as access to credit. (The first tier of Kenya's KYC regulations allows mobile money customers to use their SIM cards to identify themselves.) Kenya has also built an Integrated Population Registration System (IPRS) to verify the identity of citizens and residents. Commercial banks, mobile money providers and other financial service providers are able to access this database to authenticate the identity of customers during the onboarding process. **Tanzania** is also in the process of rolling out a national ID system with e-KYC capabilities.

The Philippines is in the initial stages of developing a digital national ID system, which may have e-KYC capabilities. In 2018, the Filipino government enacted legislation establishing a new biometric-based foundational national ID system—the Philippine Identification System (PhilSys). The Central Bank of the Philippines (Bangko Sentral ng Pilipinas or BSP) has issued regulations on technology-enabled KYC rules. The BSP identifies the system as a crucial enabler for financial inclusion, with its potential to address persistent onboarding issues due to the lack of verifiable IDs and the inefficient paper-based KYC processes which make serving small-value customers unattractive.[72] SingPass in **Singapore** can be used to facilitate direct payments without the need to reference taccount numbers of the payment originators and beneficiaries. SingPass has a component called MyInfo that pulls basic user information (such as names and addresses) from government databases. The Monetary Authority of Singapore is in the process of developing a KYC platform that will allow participating financial institutions to access customers' MyInfo data in order to fulfil basic KYC requirements.

68. http://indiastack.org/ekyc/
79. Clark, J (2018), op. cit.
70. UIDAI (Unique Identification Authority of India) (2018) Enhancing Privacy of Aadhaar Holders – Implementation of Virtual ID, UID Token and Limited KYC
71. Interview with Safaricom
72. Central Bank of the Philippines (2017) Financial Inclusion Initiatives 2017

Functional ID systems for e-KYC

Although they lack the versatility of foundational ID systems, functional ID systems built for use in a specific sector or for a specific service may be appropriate in certain circumstances, such as when a country lacks the resources, organisation, or political will to develop a national ID system. Such ID systems may be developed by government ministries or agencies, individual financial institutions or industry consortia, or some combination of these. Governments with national ID systems which do not meet identification needs are most likely to establish a functional system, but this is not always the case. Sweden's BankID is an example of a functional ID that was successfully developed despite the existence of a well-functioning national ID system.[73]

Public-private partnerships: Nigeria's bank verification number

In 2014, the Central Bank of Nigeria (CBN) partnered with the Bankers Committee, an industry body, to launch the Bank Verification Number (BVN), a functional biometric verification system for Nigerian banking customers. The system captures biometric data (fingerprints and facial images) and issues customers an 11-digit ID number. It is used to identify and verify customers who have accounts with Nigerian financial institutions and to track their credit histories in order to prevent identity theft and reduce the incidence of non-performing loans.

The BVN system is run by the Nigeria Inter-Bank Settlement System (NIBSS), a financial market infrastructure collectively owned by all licensed Nigerian banks, along with the CBN. The NIBSS maintains the ID database and performs verification services for its member banks. The BVN system is separate from Nigeria's foundational national ID system, the National Identification Number (NIN), which is run by the National Identity Management Commission.[74] There are ongoing efforts to integrate the BVN with the NIN and the national e-ID card. In 2015, the CBN made the BVN mandatory for carrying out financial transactions in Nigeria. Under Nigeria's tiered KYC regulations, the BVN is not required for Level 1 (low-value) mobile money wallets but is required for Level 2 (medium-value) and Level 3 (high-value) mobile money wallets.[75] By the end of 2017, more than 31 million Nigerians had obtained a BVN.

Individual financial institutions: Mexico's biometric verification system

In Mexico, Banco Azteca introduced biometrics in 2001. Customers could register using their fingerprints and use these to authenticate themselves. Banco Azteca registered over 8 million customers biometrically in the first five years and was processing over 200,000 fingerprint matches per day as early as 2006.[76] The bank asserts that the use of biometrics has allowed it to provide access to financial services to customers without reliable official identification.

Other banks in developing countries that have established their own biometric enrolment programs include PRODEM in Bolivia, Opportunity Bank International (which operates in multiple countries), and Siddhart and Everest Banks in Nepal.[77]

73. BankID (2018) This is BankID
74. The NIMC is embarking on an ambitious digital ID enrollment campaign and is enlisting private-sector entities, including mobile network operators, to help it enroll hard-to-reach Nigerians. See, for example: Adeyemi, A. (2018) NIMC, Operators Strategize on January 2019 NIN Deadline. The Guardian (Nigeria).
75. Central Bank of Nigeria (2017) Review of Daily Mobile Money Wallet Transaction and Balance Limit and Bank Verification Numbers (BVN) Requirement for Mobile Money Wallet Holders
76. Gelb, A. and Diofasi Metz, A. (2018), op. cit.
77. Gelb, A. and Diofasi Metz, A. (2018), op. cit.

Lessons for policymakers and mobile money providers seeking to create e-KYC capabilities

Countries that already have universal or near-universal ID systems should work to make those systems accessible to third-party service providers, including mobile money providers, for the purpose of authenticating customers. Countries that do not yet have universal ID systems can also improve the accessibility of their systems, while, over the long term, focusing on expanding the coverage and capabilities of their systems.

In this section, we consider the prerequisites and policies that countries must have in place in order to effectively implement an e-KYC service, including the regulatory framework, ID infrastructure and coverage, and the technical capacity of public- and private-sector stakeholders.

Design, infrastructure, funding, and maintenance

Several lessons can be drawn from the experiences of countries that have developed e-KYC capabilities for their national ID systems.

Population coverage: It is important that the ID system covers a majority of the population. For mobile money providers to be incentivised to make investments in connecting their systems to the national ID system, and to have the technology to authenticate users, a sufficient number of customers need to be linked to the system in the first place.

Quality controls: It is essential that the appropriate quality controls be in place during initial registration. The sophistication of the system cannot compensate for poor or unreliable data quality with respect to people's unique identification and personal information. It is equally important that the accuracy of individuals' personal information be maintained over time. One way to accomplish this is by linking databases across the public sector.[78]

Offline capability: It is important to have offline capabilities in place, which give service providers the option of authenticating users against a smart card using a mobile application or point of sale device when connectivity is limited. Offline capabilities are essential in areas with poor or unreliable internet or electricity. In addition, consideration has to be given as to how biometric devices will be maintained—if, for example, a biometric scanner breaks down in a rural area, it may be difficult to repair or replace.

Budgeting: Careful consideration must be given to how the ID system is funded. In most of Sub-Saharan Africa, national ID registries are funded as a budget line item. The World Bank also provides substantial support for national identification and civil registration programmes.[79] This runs the risk of underfunding, which has happened in several cases. Some governments have opted to make their ID systems self-sustaining, allowing them to charge access fees, as is the case in Rwanda and Pakistan. However, the use of fees also risks discouraging third parties from utilising the ID system.

Technical capability: Careful consideration must be given to the technical capacity of various stakeholders, including government agencies and individual users. In particular, the cost and complexity of maintaining the system and the devices that interact with it must be realistically assessed.[81] Policymakers must consider not only the upfront cost of registering the users, but also the need to invest, maintain, and occasionally upgrade the supporting infrastructure, which may include cards, scanners, micro-ATMs and other point-of-sale devices. Some newer generation smartphones have built-in biometric scanners, but older smartphones and feature phones do not.

Design standards and interfaces: Open design standards and open interfaces should be used wherever possible to promote interoperability and to discourage favoritism.

Governance: It is important to have a strong legal backing in place, as well as robust governance and oversight procedures.

Safety, security, and privacy

The safety, security, and privacy of digital ID systems is critically important, particularly if those systems are online and accessible to outside parties. Digital ID systems pose a risk to privacy because they typically aggregate sensitive personal information in one place.[82] Furthermore, since centralised

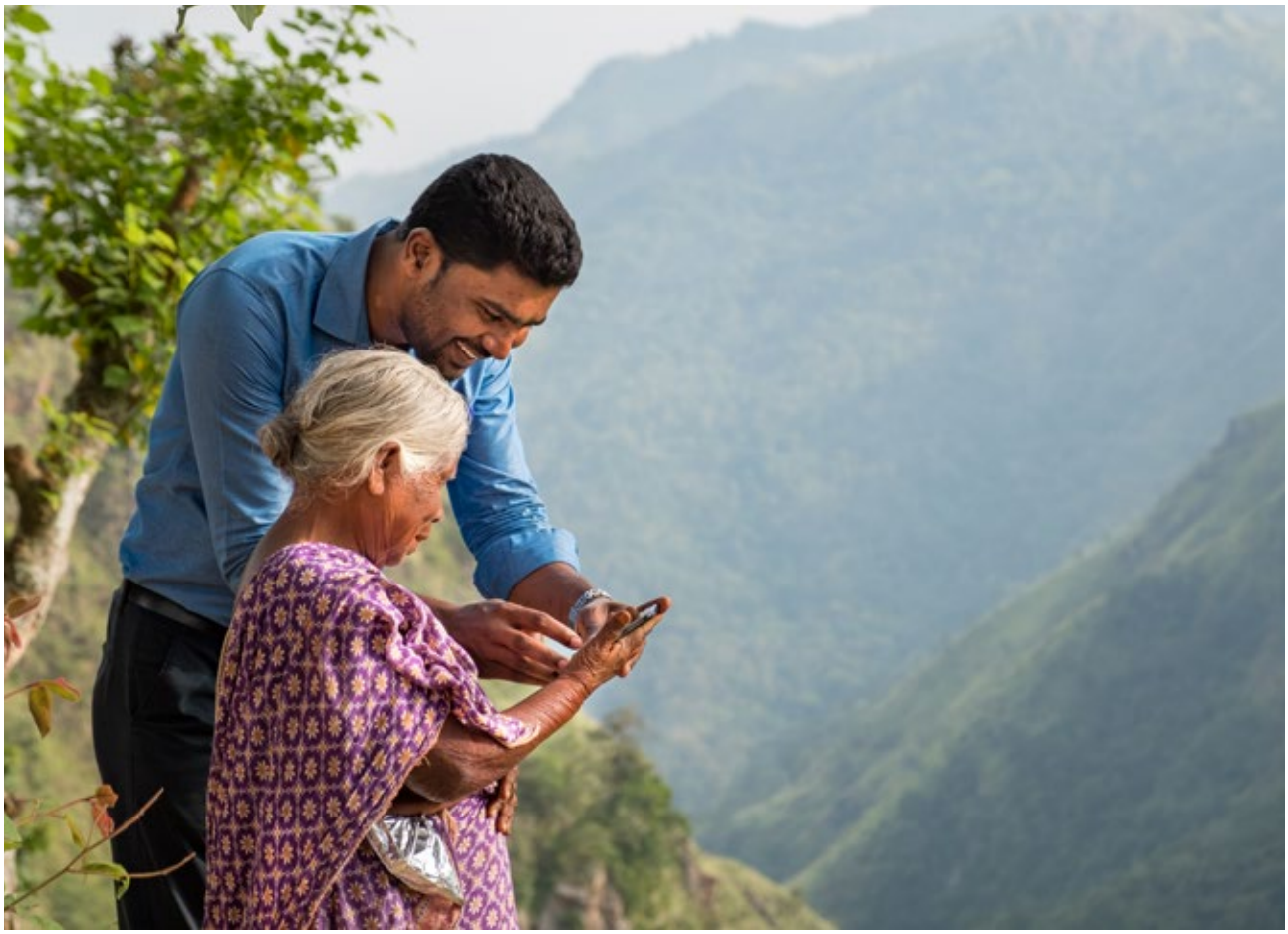
78. Lowmaster, K. and Cherepennikova, D. (2018), op. cit.
79. World Bank Group (2017) Identification for Development 2017 Annual Report
80. Clark, J. (2018), op. cit.
81. World Bank Group and GPFI (2018), op. cit.
82. ID systems are not always centralised. In Sub-Saharan Africa, civil registries are usually decentralised, while national ID systems tend to be more centralised. However, in most African countries, even national ID systems are "horizontally decentralised" to some extent, meaning that different government agencies maintain separate databases for the administration of different programs. See: World Bank Group (2017) The State of Identification Systems in Africa: A Synthesis of Country Assessments

databases present an attractive target for hackers, government databases must have strong cybersecurity measures in place.[83]

These risks depend to a great extent on what information third parties can access. A digital ID system with strong privacy safeguards will only allow access to the personal information required for the task at hand, require the user to grant permission for the information to be shared, and may, where possible, answer queries with a simple "yes" or "no" without providing access to the underlying information.[84]

Data privacy laws are critical to ensuring that citizens' data is safeguarded in the use of digital ID systems. However, the effectiveness of data privacy laws depends on the technical and institutional capacity to enforce these digital ID systems, as well as the overall respect for the rule of law in a country. Countries that lack the technical capacity to manage these systems themselves may need to rely on outside vendors, which can pose risks if the vendors are not well-supervised and if the countries become dependent on them.[85] Moreover, most developing countries still lack comprehensive legal frameworks for protecting mobile users' privacy, which may impact the adoption of these digital ID systems.

Where institutional capacity is low, it is important to build safeguards directly into the system, applying the principle of privacy by design. This will be geared towards keeping the amount of personal data collected to the minimum necessary, while proscribing data that is extraneous to the purpose of the ID system and that might be dangerous in the wrong hands. For example, Rwanda's ID system does not collect data on ethnicity.[86] Another option is to assign "dumb" random numbers that do not include information about the user in their code.[87] Yet another is to create multiple identifiers for a single unique identity, or to use cryptography to ensure that a single ID cannot be matched across different database (as Austria does) or to use a single ID but separate databases for different functions (as Estonia does).[88]



84. Gelb, A. and Diofasi Metz, A. (2018), op. cit.
85. Gelb, A. and Diofasi Metz, A. (2018), op. cit.
86. Ibid
87. Ibid
88. Ibid

Blockchain for digital identity and KYC

Blockchain or distributed ledger technology (DLT) is a method for securely managing, sharing, and updating data across a peer-to-peer (P2P) network of computers. Many believe that the technology can expand opportunities for economic exchange and collaboration by reducing the need to rely on intermediaries and the frictions associated with them.

Several firms are focused on using blockchain as the basis of "user-centric" or "self-sovereign" ID systems.[89] These systems aim to shift control to individuals by allowing them to "store their own identity data on their own devices, and provide it efficiently to those who need to validate it, without relying on a central repository of identity data."[90] Under this model, users would store certified documents and other personal information in an "identity wallet" on their mobile phones, and grant permission to specific third-parties to access particular documents or other pieces of information.

Using blockchain technology to help individuals manage and share their personal data could confer several benefits including: privacy, since users could control both who they share their personal information with and how much information they share; security, since the absence of a centralised database eliminates single point of failure risk; and convenience, since users could provide verified information with the touch of a button rather than through multiple physical documents.

Despite this potential, at present few, if any, applications of a user-centric ID model have scaled. And while the benefits of such an approach are obvious in theory, shifting from a centralised to a decentralised ID model raises several legal and regulatory challenges. In the first instance, companies interested in using the technology must determine if, and how, they can comply with existing data security and privacy laws. In the second, policymakers must consider whether to change existing laws to facilitate the use of decentralised models.

Moreover, although blockchain may provide a secure means of storing and sharing ID information, it does not resolve the issue of initial identity proofing at the point of entry into a system. A blockchain-based identity may be more secure once it is established, but that does not necessarily mean it is accurate. As the World Bank and the GPFI noted with respect to an Emirati blockchain ID initiative, "in actuality, what will be stored in the distributed ledger is not identity itself but an identity 'transaction' or attestation of an identity."[91]

Blockchain is still an emerging technology. Policymakers who wish to explore its use for digital identity and KYC should permit banks and mobile money providers to experiment with proofs-of-concept and pilot projects. They may also wish to consider how data sharing and privacy laws might affect the legal viability of blockchain-based solutions. Finally, they should encourage coordination among different stakeholders with a view toward ensuring interoperability between different institutions and blockchain arrangements, so that they can integrate as initiatives are scaled up.

89. See for example, Sovrin and SecureKey
90. Antony, L (2016) A Gentle Introduction to Immutability of Blockchains. Bits on Blocks.
91. World Bank Group and GPFI (2018) op. cit.

The potential for e-KYC in Sub-Saharan Africa, Latin America and South Asia

In this section, we examine the extent to which countries in Sub-Saharan Africa meet the policy, regulatory, and technological prerequisites for the e-KYC solutions described above.

In a recent survey of African ID systems, the World Bank Group found "a wide range of identity system types and levels of development."[92] Of the 17 countries included in the survey, the World Bank determined that a few countries (such as Kenya) have "relatively advanced" systems, while many others (such as Tanzania) are at the "intermediate stage of development." Finally, a few countries (such as the Democratic Republic of the Congo) lack ID systems altogether or are in nascent stages of developing one.[93] Overall, the World Bank found that in most countries, access to ID systems and related services was limited.[94] Few countries allow external service providers to authenticate their users' identities against the central database. Moreover, verification is often manual, and most countries cannot securely authenticate individuals' identities, even those with ID systems that issue smartcards.

In much of Africa, there are basic prerequisites for such systems to be valuable to mobile money providers and other financial institutions. First, many African countries still have significant coverage gaps. Second, in many African countries, the power and telecommunications infrastructure is unreliable, meaning that e-KYC services accessed via the internet will not always be reliable, necessitating offline as well as online means of verification.[95] Third, many ID systems require manual authentication. Even when this is possible, it cannot always be done securely. Finally, few ID systems across the continent are accessible to third-party service providers.

Most African countries therefore need to focus on improving the general coverage, functionality, and reliability of their ID systems. This includes expanding population coverage while maintaining or improving data quality. It also includes making their power and telecommunications infrastructure more robust—an important development goal for the continent. Various ID stakeholders, including telecoms and mobile money providers, financial

92. World Bank Group (2017) The State of Identification Systems in Africa: A Synthesis of Country Assessments
93. Ibid
94. Ibid
95. Email correspondence, Safaricom, October 31, 2018.
96. Interview with Daniel Barrientos and Jose Manuel Ayala Marti, Tigo El Salvador, November 9, 2018.
97. World Bank Group (2018) Identification for Development (ID4D) Global Dataset
98. GSMA (2018) Mobile Money Regulatory Index

sector and telecoms regulators, and others, should to coordinate to ensure that the system and its interface meet the needs of all users. Finally, it is important to have strong legal foundations, governance procedures and oversight in place, and to ensure sufficient funding for ID systems.

In some countries, the next steps are more particular. For example, Nigeria must navigate how to integrate the various ID systems it has in place, in particular the BVN and the national ID system. Kenya is in the process of transitioning from a universal but paper-based ID system to one that is digitised and based on biometrics. Some countries, such as the DRC, require sustained and fundamental reform. In the short term, they need to expand the use of SDD by allowing alternative forms of ID and to allow financial service providers to digitise their KYC records. Over the longer term, the country needs to develop a national ID system, taking advantage of the assistance provided by the World Bank Group and other donors.

In Latin America and South Asia, the challenges are different. In these regions, ID coverage tends to be better, on average, and the ID infrastructure is generally more robust. Some countries need to focus on enrolling their remaining unregistered populations, but in many countries in these regions, the priority should be to further develop their ID infrastructure and to make it more accessible to third-party service providers, including mobile money providers. For example, in El Salvador, the national ID system is unable to respond to many queries simultaneously. This is a hindrance for mobile operators in the country, who may register upwards of 1,000 customers per day.[96]

In Latin America and the Caribbean, nearly all countries have a digital national ID system. Many of these systems collect biometric information, with some notable exceptions, including Brazil and Mexico. Few countries have large uncovered populations.[97] The GSMA has identified several countries that have established ID verification infrastructure for mobile money, including Bolivia, Brazil, Columbia, and Peru.[98]

Similarly, all countries in South Asia have a digital national ID system that collects biometric information. ID coverage ranges from 68 per cent in Bhutan to 100 per cent in Sri Lanka; the larger countries, including Bangladesh, India, and Pakistan, all have adult coverage rates above 80 per cent.[99] India and Pakistan have established e-KYC capabilities for mobile money and Bangladesh is developing them.[100]

99. World Bank Group (2018) Identification for Development (ID4D) Global Dataset
100. GSMA (2018) Mobile Money Regulatory Index and Perlman, L. and Gurung, N. (2018) The Use of eIDs and eKYC for Customer Identity and Verification in Developing Countries: Progress and Challenges

Conclusions and policy recommendations

Among developing countries in general, and Sub-Saharan African countries in particular, there is wide variation in their ID systems' level of coverage, accessibility, and functionality. Some countries, such as Kenya, have ID systems that already offer e-KYC, and a few more are well-positioned to offer such services. For many other countries, more fundamental investments in their ID systems would be useful to expand coverage and improve reliability and accessibility.

For countries in Sub-Saharan Africa, the policy options depend to a certain extent on whether countries have high or low levels of ID coverage, though they overlap in certain respects: Countries with a high-degree of ID coverage should focus on building up the capability of their ID systems, making them into digital platforms that can support a range of digital activities, including e-KYC. These countries may also use simplified due diligence, though it may not have as much of an impact on the market.

Countries with lower levels of ID coverage should focus in the short term on finding a workable, simplified due diligence regulatory regime. If possible, they should seek to build or expand upon a viable foundational national ID system, but if that is not a viable option in the short to medium term, they may wish to look at functional ID systems. In addition, the governments of these countries could explore areas of collaboration with the private sector and/or development partners in the provision of IDs.

Countries in Latin America and South Asia, which tend to have higher levels of ID coverage, should in general focus more on developing the technical capabilities of their systems, and on establishing or revising the legal and regulatory basis for third-party access. All countries may wish to explore the option of merging KYC requirements for different mobile services, and allowing those who have already registered their information for a SIM card to use the same credentials for a basic mobile money account.

Regulators should aim to have clear, predictable and effective regulatory frameworks that are flexible enough to adapt to market developments. Constant dialogue between operators and regulators should be encouraged to resolve any regulatory areas that require clarification with immediate action. Innovation should not be viewed as solely market-led, but also as a regulator-led initiative. These efforts should be in line with the Financial Action Task Force (FATF) recommendations which state that regulatory frameworks ought to strike the balance between financial integrity and financial inclusion. This will ensure that KYC requirements are complementary to the continued responsible growth of mobile money services in emerging markets, rather than a barrier to that goal.

gsma.com/mobilemoney

For more information, please visit
gsma.com/mobilemoney

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601