Financial Regulations for Improving Financial Inclusion

A CGD Task Force Report

Chairs:
Stijn Claessens
Liliana Rojas-Suarez

CENTER FOR GLOBAL DEVELOPMENT

Financial Regulations for Improving Financial Inclusion

A CGD Task Force Report

Chairs:
Stijn Claessens
Liliana Rojas-Suarez

Center for Global Development
2055 L Street NW, Floor 5
Washington DC 20036

www.cgdev.org

ISBN 978-1-933286-96-9

Cover photos, clockwise from top left: © Erik Hersman, CC BY 2.0; Arne Hoel/World Bank, CC BY-NC-ND 2.0; Tim Moffatt, CC BY 2.0; Meena Kadri, CC BY-NC-ND 2.0.

Editing, design, and production by Communications Development Incorporated, Washington, D.C.

Task force members

Chairs

Stijn Claessens
Liliana Rojas-Suarez

Task force members

Thorsten Beck, Professor, Cass Business School
Massimo Cirasino, Head of the Payment Systems Development Group, World Bank
Stijn Claessens, Senior Adviser, Federal Reserve Board
Asli Demirgüç-Kunt, Director of Research, Development Research Group, World Bank
Alan Gelb, Senior Fellow, Center for Global Development
James Hanson, Former Senior Financial Policy Advisor, World Bank
Ishrat Husain, Former Governor, Central Bank of Pakistan
Ben Leo, Senior Fellow, Center for Global Development
Nachiket Mor, Member of the Board, Reserve Bank of India
Mark Napier, Director, Financial Sector Deepening (FSD), Africa
Mthuli Ncube, Former Vice President, African Development Bank
Njuguna Ndung'u, Former Governor, Central Bank of Kenya
Lois Quinn, Senior Payment Systems Specialist, World Bank
Beth Rhyne, Managing Director, Center for Financial Inclusion
Liliana Rojas-Suarez, Senior Fellow, Center for Global Development
Lemma Senbet, Executive Director, African Economic Research Consortium
Tommaso Valletti, Professor, Imperial College London and University of Rome
Tarisa Watanagase, Former Governor, Bank of Thailand

The recommendations and views expressed in this report are those of the task force as a whole; not all recommendations are necessarily supported by all members. Affiliations are for identification purposes only. Task force members participate in their individual capacity, and the views expressed should not be attributed to the institutions listed.

Contents

Boxes

Glossary

See box 1.1 for definitions of other digital financial services providers and business models. An asterisk indicates that the definition was taken or adapted from World Bank (2012a).

agent network. A collection of independent businesses, such as retailers, with which a bank or other financial services provider contracts to serve as points of interaction with the provider's customers.

cash-in, cash-out. Transaction to convert a balance in a transaction account into cash, or incrementing a balance by paying in cash, often structured as a transfer between an agent's account and a customer's account, with the payer compensated in cash.

chip card. A plastic card in which is embedded a computer chip containing information about the cardholder's identity and account.

competition policy. The set of government policies that governs the state of market competition in an economy, including entry and exit rules, antitrust enforcement, contestability of infrastructure, and related issues.

contestability. The absence of barriers to the entry of new competitors in a market (market contestability) or to the use of infrastructures and other inputs necessary for participation in the market (input contestability).

digital (financial) services provider. A mobile network operator or other nonbank entity that offers various financial services but only by electronic means, for example, using a mobile phone or the Internet.

e-money.* A record of funds or value available to consumers that is stored on a payment device, such as a chip, a prepaid card, or a mobile phone, or on a computer system as a nontraditional account with a banking or a nonbanking entity. E-money products can be further differentiated into network money, mobile money, electronic purse, and electronic wallet (e-wallet).

e-wallet.* An e-money product for which the record of funds is stored on a specific device, typically a chip on a card or in a mobile phone.

ex ante regulation. Government rules and regulations that set prerequisites on financial services providers as conditions for their entry and continued participation in a market.

ex post regulation. Government regulatory intervention that occurs only after a problem or market failure has been identified.

float. The aggregate of funds that, for a short interval after a transaction, have been credited to the account of the recipient but not yet debited from the account of the sender.

functional approach. An approach to financial services regulation in which services of the same nature are regulated in the same way, rather than, for example, according to the type of provider.

interchange fee. A fee charged by one provider of payment services to another–for example, the fee charged by a merchant's bank (acquirer) to a cardholder's bank (issuer) to compensate the issuer for the benefits that merchants receive when they accept electronic payments.

interoperability.* A situation in which instruments belonging to a given scheme may be used in platforms developed by other schemes. Interoperability requires technical compatibility between systems, but it can take effect only when agreements have been concluded between the schemes concerned. In mobile money markets, interoperability implies the ability of users of one network to transact with users of another network, which can be achieved at different levels—at the customer level, at the agent level, or at the platform level.

know-your-customer regulation. Government rules and regulations that require a financial services provider to exercise due diligence in establishing the identity of its users, specifically, to ensure that the user is not engaged in money laundering or terrorist financing.

macroprudential regulation; microprudential regulation. See *prudential regulation*.

mobile money.* An e-money product for which the record of funds is stored on a mobile phone or a central computer system

and from which funds can be drawn down using specific payment instructions that are issued from the bearer's device.

mobile network operator. A provider of wireless communications services that owns or controls the infrastructure necessary to deliver those services.

narrow bank. A bank that invests its funds (typically deposits) in only the safest instruments, such as government bonds or a deposit account at another bank—subject to prudential limits —or number of banks.

network externality. The additional value that a network gains by increasing the number of participants with whom to transact.

off-network (off-net) transfer. The transfer of funds to a recipient who is registered with a different mobile network than the sender, or the conversion of funds to (or from) cash for a recipient who is not registered with a network.

payment. The transfer of an item of value from one party (such as a person or company) to another in exchange for the provision of goods, services, or both, or to fulfill a legal obligation. In the context of this report, payments refer to digital transfers of value, thus excluding barter and cash payments.

person-to-person transfer. A transfer of funds directly from one person to another by electronic means rather than by cash or check.

point of sale. The time and place at which a retail transaction is completed by the customer making a payment to the merchant, using traditional or digital means, in exchange for goods or services.

principle of proportionality. See *risk-based approach.*

prudential regulation. Government rules and regulations that limit risk taking and some other behaviors of financial services providers to ensure the safety of an individual financial institution or of customers' funds (microprudential regulation) or to preserve the soundness of the financial system as a whole (macroprudential regulation).

risk-based approach. An approach to financial services regulation that follows the principle of proportionality, such that the stringency of regulation of an activity is commensurate with the risk that the activity poses to users and creditors or to the system as a whole.

safe assets. Government securities or other high-quality liquid assets. They may also include deposits in other banks but with tight limitations and provided that those banks are properly supervised.

safer corridor. An electronic payments channel between two countries in which only those individuals and entities previously determined to be trustworthy (that is, whose names appear on a list of approved participants) are permitted to conduct transactions.

SIM card. The removable chip within a smartphone or similar device that contains information about the phone, the user's identity, and possibly financial and other information.

store-of-value instrument. An account such as a deposit account, or an account on a device such as a magnetic card, that contains negotiable monetary value for a period longer than is necessary to complete a transaction.

tiered pricing. A schedule of prices for a service that varies, possibly with the value of the transaction(s), their volume, or the location, affluence, or other attributes of the customer.

Acknowledgments

This report was made possible by the knowledge, dedication, and effort of the members of a CGD Task Force. Their expertise, diverse experiences, and range of perspectives were invaluable in tackling the complex challenge of advancing recommendations for regulations needed to foster greater financial inclusion, especially those that enable innovations in digital finance to be adapted and adopted in order to benefit the vast majority of people. The recommendations in this report drew strength from the many engaging debates and conversations among Task Force members and from the three meetings held at CGD; however, not all members necessarily support all the recommendations.

We are also very grateful to Alan Gelb, Maria Chiara Malagutti, Peter Ondiege, Marc Bourreau, and Tommaso Valletti for writing working papers and producing background material that strongly supported the production of the report. Gelb and Valletti were also members of the Task Force. Gelb was also the main contributor for section 4 on know-your-customer policies.

This report also benefited from Task Force members' discussions with many individuals and organizations, whose feedback and active participation in CGD-sponsored meetings and events improved our ideas and recommendations. We would like to thank Tim Adams, Guillermo Babatz, Amar Bhattacharya, Marylin Choy, Louis de Koker, Eva Gutierrez, Yira Mascaro, Anand Sahasranaman, and Ratna Sahay. Particular thanks are due to experts from the Payment Systems Development Group of the World Bank Group's Finance and Markets Global Practice, who provided specific comments and suggestions on an earlier draft of the report.

Many thanks to our CGD colleagues for their feedback, especially Vijaya Ramachandran. Nancy Birdsall provided insightful comments that helped refine the final drafts. Rajesh Mirchandani, Kate Wathen, John Osterman, and Jocelyn West from CGD's communications team provided support with publication and outreach. We are thankful to Mike Treadway for his excellent editorial assistance. Brian Cevallos-Fujiy and Maryam Akmal provided outstanding research assistance.

Finally, we would like to thank the Bill & Melinda Gates Foundation for their generous financial support for this project and for their engagement throughout the process. Particular thanks are due to Rodger Voorhies, Sheila Miller, Rosita Najmi, and Sacha Polverini. We appreciate their commitment to broadening financial access among low-income populations.

Abbreviations

ATM	automatic teller machine
DSP	digital services provider
EU	European Union
FATF	Financial Action Task Force
G20	Group of 20
KYC	know your customer
ML/TF	money laundering/terrorist financing
MNO	mobile network operator
P2B	person to business
P2P	person to person
POS	point of sale
SIM	subscriber identity module
USSD	Unstructured Supplementary Service Data

Executive summary

As recently as 2011, only 42 percent of adult Kenyans had a financial account of any kind; by 2014, according to the Global Findex database (World Bank 2015), that number had risen to 75 percent, including 63 percent of the poorest two-fifths. In Sub-Saharan Africa as a whole, the share of adults with financial accounts, either a traditional bank account or a mobile account, rose by nearly half over the same period. Many countries in other developing regions have also recorded gains, if less dramatic ones, in access to the basic financial services that most people in richer countries take for granted. Much of this progress is being facilitated by the digital revolution of recent decades, which has led to the emergence of new financial services and new delivery channels.

Whereas payment services often are the entry point into using formal financial services, they are not the only financial services being delivered at far lower cost and more widely in recent years. Indeed, driven by advances in new digital payment services, small-scale credit is starting to be provided in several developing countries, and many providers are experimenting with new modes for delivering various insurance services. Digital (payment) records are being used to make decisions about provision of credit to small businesses or individuals who do not have traditional collateral or credit history to secure loans. Additionally, affordable mobile systems have led to the provision of new and innovative financial services, which would not be economically sustainable under the traditional brick-and-mortar model. Examples of those innovations include mobile-based crop microinsurance in Sub-Saharan Africa and pay-as-you-go energy delivery models for off-grid customers in India, Peru, and Tanzania.[1]

Increased access to basic financial services, especially payments services, by larger segments of the currently unbanked population reflects to a large extent the growing use and application of digital/mobile technologies in developing countries (which is leading to major changes in financial services provision in advanced countries as well). Also critical has been the adoption of proper policy and regulation based on country-specific opportunities, needs, and conditions. Kenya and India provide two examples. Kenya's recent success is partly explained by the restrained approach of its regulators, who preferred to set rules ex post, as services and their providers evolved, rather than impose a strict ex ante regime that might later prove a poor fit.

Taking a different approach, regulators in India have been reforming their institutional infrastructure to allow financial service providers to better serve the poor. In 2015, India witnessed the first in-principle approval of licenses for 11 payment banks, whose main aim is to enhance the (digital) provision of payment services to low-income populations. Institutions qualifying for these licenses were financial and nonfinancial firms, including digital service providers (DSPs). To strike a balance between fostering innovative approaches and ensuring safety, soundness, and consumer protection, the new payment banks may accept individual deposits up to a certain amount and engage in transfers and remittances. In contrast to regular banks, however, payment banks must not engage directly in lending; funds taken in must instead be invested only in certain explicitly permitted securities, thus guaranteeing the safety of the deposits.

As these and other examples show, the combination of innovation and sound regulation in financial services enables the private sector to improve economic opportunity and well-being for poor people in many countries. The examples also show that the paths leading to greater financial inclusion using the new digital technologies are multiple, evolving rapidly, and likely to be country-specific. The pace of progress is uneven, however, and from a global perspective, access to financial services remains limited. Again according to Global Findex, only 27.5 percent of the adult population in the world's low-income countries had a financial account in 2014; the figure for developed countries was 94 percent. Much further

1. These and other examples are documented in Queen Maxima of the Netherlands (2015); Tellez and others (2014); and Winiecki and Kumar (2014).

progress, including through more and better regulatory reforms, is needed to make efficient, safe, reliable financial services available to all who might benefit.

Poor regulation is a major obstacle to financial inclusion—but it is not the only one. Others include lack of good infrastructure, weak institutions, poor cooperation, and unstable economic and political conditions. However, this report focuses solely on regulatory issues for two main reasons. First, regulatory changes are often needed to enable the successful adoption and adaptation of innovations in digital finance, encourage their use, and increase competition among their providers, so that those new technologies can benefit the poor in particular. Second, progress in improving financial inclusion must be compatible with the traditional mandates of financial regulation and supervision—namely, safeguarding the stability of the financial system, maintaining its integrity, and protecting consumers.

Determining the best regulatory approach for finance in general is challenging, as the rules will have to reflect the features of each specific financial service and the risks entailed from alternative forms of financial service provision. This challenge is even greater for digital finance, given the many new forms of provision and providers. Put differently, in the new world, policies and regulations will have to vary in a number of dimensions to help ensure efficient service delivery that is also safe to the users and to the overall system.

To tackle these challenges, the approach to regulation for financial inclusion advocated in this report follows three principles commonly used to guide regulatory choices: similar regulation for similar functions, regulation based on risk, and balance between ex ante and ex post regulation. Relying on these principles, the report advances specific recommendations in three distinct regulatory areas—competition policy, leveling the playing field, and know-your-customer (KYC) rules—with a full section of the report devoted to each topic. A final section of the report discusses all three topics further as they apply specifically to the retail payments sector. A full list of the report's recommendations appears at the end of this summary.

Competition policy

Competition matters for financial inclusion, especially in developing countries, because a market open to fair competition leads to a greater variety of products and services, higher efficiencies, and lower costs, which ultimately means potential consumers currently on the sidelines will be more easily included. Competition policies tend to address the causes for inefficient outcomes resulting from the conduct and interactions among producers of financial services and between producers and consumers of financial services. Competition policies differ from initiatives aimed to level the playing field (see next section), as the latter address distortions derived from regulations applied to various products and services and the entities offering them. While the outcomes resulting from these inefficiencies and distortions may appear very similar, the underlying causes, market failures versus regulatory actions, are very different and thus require quite different solutions.[2]

Competition policy's main goal is to allow—and indeed, encourage—new providers to enter. Because of crucial differences in their overall nature and their activities, however, the rules of entry should most likely differ between traditional players, such as banks, and nonbank digital services providers (DSPs). For the former, entry should be conditional on standard fit-and-proper requirements. If they meet those requirements, and as long as strong regulatory, supervisory, and consumer protection frameworks are in place, banks should face no constraints on entry and minimal limits on the services offered (recommendation 1).[3]

For nonbank DSPs, entry rules should depend on the services they offer. Entry of DSPs that offer bank-like services (stores of value not fully backed by safe assets, credit, and so forth) should be conditional on fit-and-proper standards similar to those for banks, but otherwise liberal; failure to meet this recommendation would imply discriminatory practices vis-à-vis banks. For those providers that restrict their retail activities to (small) payments and transfers or that offer stores of value fully backed by safe assets (such as government securities or other highly liquid assets), standards should

2. For instance, a DSP could be prevented from offering mobile money services because either the license allowing it to issue electronic money is reserved according to regulation to banks only or because access to business critical technology such as the USSD channel is provided at high cost by competing entities. The first case is a level playing field issue that can be solved by reviewing the relevant regulation. The second case is a competition issue because the dominant position of the USSD provider constrains the ability of the newcomer to access the technology at fair prices and conditions and compete effectively in the market.

3. Numbers in parentheses refer to specific recommendations from the report, which are listed at the end of this summary.

be relatively minimal and entry should be liberal, as their activities would pose little risk to the customer and the overall financial system (recommendation 2). In all cases, licenses should be awarded only to providers with proven technical and financial capabilities to ensure the quality of the services offered. For all providers, laws and regulations must ensure that no-longer-viable providers exit the market (recommendation 3). Sound antitrust rules and procedures also are needed to avoid the emergence of entities with excessive market power and uncompetitive pricing (recommendations 4 and 22).

A goal to help achieve full financial inclusion is a fully interoperable financial system, in which any user of any digital network can transact with any other. The issue is whether (and if so, when) interoperability can be expected to emerge spontaneously, as a market solution, and if it cannot, whether (and when) it should be mandated through competition policy. Most often, regulators should not have to mandate interoperability, as they can allow the market to spontaneously develop and implement the proper arrangements to reach this objective. However, since there are situations where regulatory interventions may be warranted, the timing of these actions is key: imposing interoperability too early can inhibit innovation and the development of digital transaction markets, but acting too late can lead to system inefficiencies and entrenched monopolies. Regulators should thus only ensure today that digital services retain the capacity to become interoperable, while keeping the option open to mandate interoperability tomorrow should it become necessary (recommendations 5 and 23).

Taking into account choices made with respect to interoperability, the inputs required for the production and distribution of financial services (such as network services for payment and settlement, credit bureaus, and a functioning telecommunications system) must also be accessible to all providers wishing to use them, fairly priced and efficiently provided. For example, traditional banks entering the mobile payments market should have equal access to telecommunications networks, and DSPs offering credit services should have equal access to the information held by credit bureaus (recommendations 6 and 25).

Leveling the playing field

A level playing field in financial services is enabled by regulations ensuring that functionally similar services are treated equally as long as they pose similar risks to the consumers of the service or to the financial system as a whole. A level playing field for each service is critical to ensure that all providers compete on an equal basis. Equal treatment by service matters for financial inclusion because it allows more consistent consumer protection across service providers, because it can help expand the market frontier for financial services, and because the providers of the new, digital financial services on which greater inclusion depends often differ greatly from one another in their structure and business models. In addition, a level playing field reduces the scope for regulatory arbitrage and other distortions.

To operationalize this concept, regulators must first define each of the different services clearly and unambiguously (recommendation 7). On an "equal basis" refers to equality across providers of a given service. For example, to the extent possible, payment services must receive identical treatment, whether the provider is a bank or another kind of institution and whether it operates online or from a brick-and-mortar office (recommendations 8 and 24). Moreover, regulation should not discriminate among providers as to their rights, obligations, and entitlements for use of critical institutional infrastructure (recommendation 21).

Two important qualifications deserve particular attention. First, a level playing field does not mean that all types of financial services should be treated exactly the same with regard to regulations. Characteristics, including risks, vary across services—payment services differ greatly from insurance services. Therefore, regulatory requirements should vary by service, as the overall objectives (consumer protection and stability and security of the financial system) can be achieved only through different approaches. With a level playing field, providers, even if of a similar institutional form, could thus be regulated differently if they offer different sets of services. Second, even when providers deliver functionally the same service, a level playing field does not mean that regulatory approaches cannot vary across providers when risks—to the user and to the financial system—vary across providers. In these cases, providers may be subject to different risk-based requirements, even when all other regulatory requirements (such as those aimed at enhancing competition, consumer protection, or financial integrity) are the same for the specific services they offer.

To illustrate this concept, consider the activities of DSPs. DSPs that limit their provision to small transactions—whether payments, remittances, or transfers—and do not offer a store of value pose little risk. They can be subject to standard payment or money transfer

regulations only, whereby intraday settlement risks can be addressed within the payment system framework (recommendations 10 and 21). Only when DSPs go further and offer stores of value and engage in other bank-like activities does additional regulation become necessary, which will depend on how the DSP is set up. DSPs that offer stores of values that are fully backed by safe assets require little additional regulation, but DSPs that use their stores of values to fund credit or to provide other forms of intermediation must be subject to regulations similar to those that apply to deposit-taking commercial banks (recommendation 11). This last comparison shows how two providers offering the same service (store of value) are appropriately subject to different regulatory requirements, in this particular case because of differences in the risks involved in the use of the funds.

When DSPs offer stores of value not fully backed by safe assets, there are also important considerations about whether the provider needs to and can have insurance to protect customers' funds and the rules that accompany any insurance. Moreover, additional bank-like regulations are needed to protect the user—and, if applicable, the deposit insurance agency—from the risks entailed by the intermediation (recommendation 12). The bottom line is that the onerousness of regulations on any provider should be commensurate (level) with the risks that the provider's overall activities pose to customers and to the overall financial system.

An important recommendation for leveling the playing field is that all providers of financial services—banks, DSPs, and others—must be made subject to regulations aimed at protecting consumers from fraud and other identified harms and at preventing discrimination. Such regulations will have to be equivalent across all types of providers (recommendations 13 and 26) and will inherently foster greater inclusion.

Implementing these recommendations will require much detailed work. Thus, an important corollary recommendation is that the regulatory regime for all digital and nondigital forms of financial services provision, notably for payment services provision, is consistent across all regulatory agencies (recommendation 9). This task is challenging, especially when services are provided by MNOs and other DSPs that have their own regulatory and supervisory authorities (such as a telecommunications regulator). A complementary recommendation, therefore, is for greater coordination among all, both financial and nonfinancial, regulatory and supervisory agencies (recommendation 14). This effort can be helped by specifying clear mandates for all agencies involved, including a mandate to promote financial inclusion and one to ensure the agencies' accountability and independence, and by adopting memorandums of understanding that can create frameworks within which different regulatory authorities can interact and cooperate in areas of mutual interest.

Know-your-customer rules

Another task of financial regulation is to preserve the integrity of the financial system, in particular by combating money laundering and the financing of terrorism. Essential to this task is ensuring that financial institutions know who they are dealing with. A financial system in which customers have total anonymity is one that can be abused and corrupted, with potentially dangerous consequences for financial stability. Knowledge of one's customers also matters for financial inclusion because financial institutions that do not know their clients will be less willing to extend to clients their full range of services. Hence, strong KYC rules are indispensable for financial integrity and financial inclusion.

The financial integrity and financial inclusion goals, however, can at times conflict. Thus, the challenge in designing KYC rules, at both the national and the international levels, is to ensure that they are adequate for maintaining financial integrity yet do not create unnecessary barriers to inclusion, but rather, work to enhance it. This calls for a risk-based approach, following the principle of proportionality, as expressed by the Financial Action Task Force as well as the G20: "To strike the right balance, existing regulations should be carefully analyzed to establish whether their demands on service-providers are proportionate to the risk" (Global Partnership for Financial Inclusion 2011).

In line with this approach, KYC rules should recognize the minimal risks that small value transactions pose to the system. One way is by allowing for restricted and graduated accounts (recommendation 16)—specially designated accounts, with limits on their balances and size of transactions, to which less onerous KYC rules apply. This would be the first level of a tiered KYC regime, which would increase the customer due diligence requirements in line with the volume, size, and nature of customers' transactions.

Also, to support a level playing field, KYC rules must be similar across mobile and brick-and-mortar providers of the same service. In line with the principle of proportionality, rules and penalties for violation should be set according to what are regarded as more and less serious failures of KYC processes (recommendation 18).

Penalties should be set on a graduated basis, increasing as the failure of compliance with KYC requirements becomes more severe and regular. For small accounts and limited transactions, penalties should be imposed according to failures to comply with KYC requirements rather than on the number of infractions that have taken place.

As with other regulations, KYC rules should be applied, as much as possible, uniformly across countries and, within countries, across supervisory agencies. Such enforcement will require greater coordination at both the national and the international levels (recommendation 15). To facilitate compliance with KYC rules for banks and DSPs and to support cross-border KYC applications, national identification systems may have to be strengthened (recommendation 17). At the international level, regulation should encourage a shift from cash-to-cash wire transfers toward direct transactions between identified account holders (recommendation 19). Finally, as an interim solution for countries deemed to pose particularly severe risks to global financial integrity, a special transfer system for transactions to and from those countries might be set up as a "safer corridor," available only to those local financial intermediaries and transfer recipients included on a preapproved positive list (recommendation 20).

The audience for this report

This report builds on an earlier one by the Center for Global Development[4] and distinguishes itself from other recent publications about financial inclusion in that its focus is largely on regulatory principles and related reforms.[5] Its recommendations concern the behavior of a wide range of actors—in particular the regulators and supervisors of financial services providers (traditional and new), but also donors, multilateral organizations, other policy advisers, private sector actors, and the various standards-setting bodies for the financial sector. Within these groups the recommendations are directed primarily at policy makers charged with improving financial inclusion through regulations.

The recommendations, however, also are relevant to a much larger range of policy makers whose policies and actions can influence inclusion. Those policy makers include the antitrust, prudential, market conduct, and consumer protection regulators of banks, other financial intermediaries, and financial markets; regulators of the telecommunications sector; licensing authorities; and the ministries and agencies concerned with policies to combat money laundering and terrorist financing. The recommendations are also addressed to the aforementioned standards-setting bodies and to the multilateral organizations and donors that play a central role in designing, advocating, and, often, financially supporting policy initiatives. Although the recommendations are not addressed directly to financial services providers, they are based on the philosophy—which is strongly supported by empirical evidence—that private financial services provision is key to sustainable financial inclusion.

4. See Claessens, Honohan, and Rojas-Suarez (2009).

5. For example, the recommendations on payments systems in this report complement those advanced by the Committee on Payments and Market Infrastructures and the World Bank Group (2015). The scope of the latter is much broader, however, and goes well beyond legal and regulatory issues in payments systems.

Recommendations

Competition policy

1. Provided that strong regulatory and supervisory institutions and solid consumer protection frameworks are in place, entry of "fit and proper" banks and other traditional providers into the financial services market must be facilitated, with the fewest and least intrusive regulatory barriers possible. Limits on the products and services these providers offer and on the inputs they use to produce and deliver services should be minimal.
2. Entry of DSPs that restrict their retail activities to (small) payments and transfers, or that offer stores of value fully backed by safe assets, should be relatively liberal. In contrast, higher entry standards, including "fit and proper" entry rules and

Recommendations

tests, should apply to DSPs that, in providing their services, pose risks to consumers and to financial system stability, such as those providing stores of value not fully backed by safe assets, credit, or insurance.

3. For DSPs active in services beyond payments and fully backed store-of-value services, the rules governing exit from the market must be as well specified, on an ex ante basis, as they are for banks and should typically extend beyond those in the bankruptcy laws governing commercial businesses. Exit rules for DSPs that restrict their activities to small payments and transfers and fully backed stores of value, with no or limited (intraday) exposure to loss and small overall transaction volumes, can largely follow commercial bankruptcy laws and procedures—but with the option for ex post regulation—provided appropriate safeguards to protect customers' funds are in place.
4. Sound antitrust rules and procedures are needed in the financial sector to avoid the emergence of entities with excessive market power. The antitrust regulators must have adequate tools and resources at their disposal to analyze the current state of competition, and they must have the authority to break up monopolies and oligopolies, penalize collusive behavior, and challenge uncompetitive pricing structures.
5. Interoperability among DSPs, and between them and traditional financial services providers—including through open (nonproprietary) technical standards—is essential for effective competition and for financial inclusion. Interoperability ideally emerges as a market solution, and if not, should be encouraged. If regulatory intervention is, however, needed, timing is key: interoperability should not be mandated either too early or too late.
6. Taking into account choices made with respect to interoperability, except where consumer protection and financial stability may be compromised, inputs required for the production and distribution of financial services must be accessible to all providers interested in using them, be fairly priced, and be efficiently provided. Codes and standards can help toward this objective, but direct (ex post) government intervention to eliminate access barriers and address discriminatory pricing might be necessary at times.

Leveling the playing field

7. Leveling the playing field for financial services starts with regulatory agencies clearly distinguishing the various services from one another.
8. To the extent possible and applicable, identical rules should apply to functionally identical services, regardless of the institutional form of the provider.
9. A consistent regime for regulating all forms of payment services provision is preferable, and the rules should ensure a level playing field in the delivery of various payment services.
10. Risks to users and general financial stability concerns arising from payment services, such as intraday settlement risks and other (systemic) risks, should be addressed within the payment system framework and should not differentiate by type of provider. MNOs and other DSPs that limit their provision of retail financial services to payments should be subject to payment regulations only.
11. For MNOs and other DSPs whose services go beyond simple payment transactions, additional regulation and supervision should apply. Those regulations may include restrictions on the use of the funds. For those store-of-value instruments that are not fully backed with safe assets, regulations should typically be similar to those that apply to deposit-taking institutions ("banks"). They can include, if applicable, insurance and related requirements.
12. To the extent that the DSPs uses stored values to fund the credit it extends, additional requirements will have to come into play, typically similar to those applied to banks to protect the individual saver, the insurance provider (if the stored values are insured), and the stability of the overall financial system.
13. All providers of financial services—banks, MNOs and other DSPs, and others—must be made subject to regulations aimed at protecting consumers from fraud, abuse, and discrimination. For any given service, these regulations should be equivalent across all types of providers of that service.
14. Coordination among supervisory agencies is as essential for digital financial services as for traditional ones. Coordination problems can be minimized by specifying clear mandates for all agencies involved and by ensuring their adequate accountability and independence. Memorandums of understanding can further help improve coordination.

Recommendations

Know-your-customer rules

15. An urgent need exists for greater coordination of efforts toward a sound global KYC regime, both among the national authorities of different countries and—within some countries—across individual agencies. Clearer guidance from the FATF could be useful in both cases.

16. In line with the risk-based approach, KYC rules should recognize the minimal risks posed by customers undertaking small transactions by allowing for restricted and graduated accounts. Less onerous KYC measures should be required for certain types of basic 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 DSPs: the rules must be similar for all providers of the same service.

17. National identification systems must be strengthened, both to facilitate compliance with KYC rules for banks and DSPs and to support the effectiveness of the preceding recommendations as they apply to cross-border transactions.

18. In keeping with the principle of proportionality, regulators must articulate what they regard as more and less serious failures of KYC processes and set rules and penalties accordingly. For small accounts and limited transactions, penalties should be set according to failures to comply with KYC requirements rather than on whether or how many infractions have taken place. Penalties should also be set on a graduated basis, increasing as the failure of compliance becomes more severe and regular.

19. Regulation should encourage a shift from cash-to-cash wire transfers toward direct international transactions between identified holders of bank accounts or e-money.

20. In cases in which 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, or positive, list.

The retail payments system

21. In principle, regulation should not impose on payment services providers, users, or other network participants any of the following: rules that discriminate between authorized payment services providers as to the rights, obligations, and entitlements of participants; restrictions on the basis of institutional status; or restrictive rules for effective participation in other systems.

22. As a general principle, and consistent with this report's general recommendations on competition, pricing of payment services can be left to the market. In some circumstances, however, interventions may be needed to ensure that pricing policies are in line with the provider's actual costs. Such interventions may include, for example, limits on interchange fees. Ensuring near-universal access may also require other types of interventions.

23. Consistent with recommendations in section 2, regulatory intervention to ensure interoperability of payment systems should be undertaken mostly ex post—and then only when necessary. If intervention is required, regulators should be mindful not to mandate interoperability of payment systems either too early or too late; the former can dampen innovation and market development, whereas the latter can allow one or more dominant players to accumulate too much market power.

24. Merchants should be free to choose which payment channel or channels they will use, but they should be discouraged from signing exclusivity arrangements. Customers should not be forced to use, or to pay more for, one means of payment when more than one are available. Regulation should be technology neutral, and standards should be based on functionality.

25. The operation of infrastructures for the processing, clearing, and settlement of payments is best left to the market, with retail payment instruments fully integrated. As a general principle, the public sector should be involved only as a regulator of infrastructure but, in exceptional cases, could serve as an operator of the infrastructure.

26. A solid institutional framework requires disclosure of fees charged—in ways that make them easily comparable across providers and products—and the provision of adequate customer recourse and dispute resolution mechanisms. The objective of financial system integrity should be balanced with that of not unnecessarily hindering access to payment services.

Chapter 1
Introduction

The opportunities of greater financial inclusion

The improvements in economic opportunity and well-being that the increased use of financial services can bring to poor people around the world are increasingly being recognized. Access to those services, however—from simple payments and money transfer services to deposit accounts, credit, insurance, and others—remains limited for many people in many developing countries. According to Global Findex (World Bank 2015), only 27.5 percent of the adult population living in low-income countries has either an account in a bank or other formal financial institution or a mobile money account; the comparable figure in developed countries is 94 percent.[1] Although the private sector, international organizations, donors, governments, and international forums such as the G20 have begun to target financial inclusion and to act to improve it, with the goal that all eligible individuals and businesses should be able to have and use at least one transaction account, various challenges remain.

The digital revolution of the past decade has led to the emergence of new financial services and products and new delivery channels. These have the potential to contribute enormously to the three key elements of financial inclusion: the expansion of financial services to serve the vast majority of the population (availability), at low cost (affordability), and in efficient, safe, reliable forms that meet their needs (quality). Ongoing technological innovations have already brought about the emergence and rapid growth of new markets, such as those for mobile money and other forms of e-money, and more are on the way. These new technologies can be especially useful for many low-income populations in developing countries because they offer a chance to leapfrog outdated financial systems. Consequently, people not only get services better suited to their needs but also escape the often crippling costs, especially of traditional payment services.

So far, however, the application of these new technologies has been confined to a relatively small (albeit increasing) number of countries and for the most part has been limited to payments and transfers, with limited penetration in the markets for other important financial services: store of value, credit, and insurance. As a result, those people fortunate enough to live in countries where mobile money or other forms of e-money are flourishing have benefited in several ways, in particular from a reduced need to carry cash and an increased ability to send and receive remittances and make payments.[2] Improvements in this aspect of financial inclusion in other countries, however, and in other dimensions of financial inclusion––deposits, credit, insurance, and other financial services––in virtually all developing countries, remain limited.

In many developing countries, the opportunities that digital finance offers are largely spurred by the entry of nontraditional players in financial services. Traditional banks in a number of these countries have made some progress in reaching underserved populations by building networks of nonbank agents, such as small retailers, to deliver their services. Coverage of poorer and more remote populations remains limited, however, and issues persist regarding the costs and quality of these agents' services and of the digital connections used to link to them. Progress in adopting the new digital technologies to enhance inclusion also has been limited by existing market structures, which are often dominated by entrenched insiders reluctant to innovate, and by various forms of regulatory capture. Telecommunications companies, consumer electronics producers, and online retailers—both existing organizations (such as Safaricom, Millicom, Apple, Amazon, and Google) and rapidly growing new innovators (such as Venmo and bKash)—are beginning to break through these barriers in developed and developing countries and forcing existing players to innovate, but

1. See World Bank (2014) for further discussion of the various aspects of financial inclusion.

2. In developing countries, e-money has mostly taken the form of mobile money. In the more developed countries, a broader range of e-money is developing, although overall uptake is still relatively low.

again, their effect so far has mainly been limited to the area of payment services.

The future of financial services provision in general is hard to predict, and that of financial inclusion achieved through digital means is even more so. What is certain, however, is that market structures will continue to change with the entrance of new players and the adoption and adaptation of new technologies. The most likely future scenario will involve a more diverse landscape, with both new and traditional providers and a variety of delivery channels. Providers of different types and from different industries are discovering new opportunities for cooperation, continuously developing new business models that combine institutions and modalities of operation (box 1.1). Each entity brings something to the table. Mobile network operators (MNOs) and other nonbank digital services providers (DSPs) bring the low-cost technology required to handle (small) transactions over distance, avoiding the need for automatic teller machines (ATMs) and brick-and-mortar offices in every village. Commercial banks and other traditional services providers bring their existing institutional setups and established processes, both of which are likely needed to deliver the complete menu of financial services—including deposits, credit, and insurance—on which full financial inclusion depends.

However, combining the best elements of these nonbank DSP-led and bank-led models and achieving a fully functional digital finance ecosystem are today just a vision statement. No country, developed or developing, has all the necessary features in place yet; parts of the mosaic remain to be filled in. Presumably, countries will follow many different paths to this final goal, at different speeds, depending on (among other things) their existing complement of MNOs and other DSPs, banks, and other financial institutions and on their unique legal history and institutional environment.

Purpose, approach, and scope of the report: the role for regulation

Despite the great promise of the new technologies for achieving greater financial inclusion, many obstacles stand in the way. Those obstacles constrain the use of traditional financial services, the pace of development of new digital financial markets and the breadth and depth they can achieve, and the ability of the poor to access financial services. The obstacles range from lack of adequate infrastructure (hardware, software, or both), to weak institutional frameworks that discourage private investment, to unstable economic and political conditions that reduce the demand for financial services, to inadequate financial regulation and subsequent legal uncertainty. Fulfilling the goals of financial inclusion therefore means advancing on multiple fronts simultaneously to overcome the constraints, which also are likely to vary greatly in intensity and importance from country to country. Striking the best balance in the choice and sequence of reforms in each country represents a major policy challenge in its own right (and has been analyzed in detail in World Bank [2008, 2014]).

Recognizing the opportunities that the new technologies offer for greater financial inclusion—but also the uncertainties and constraints—this report focuses on a number of specific regulatory issues. Addressing financial inclusion through changes in regulation is necessary for two main reasons. First, regulatory changes often are needed to enable the successful adoption and adaptation of innovations in digital finance, encourage their use, and increase competition among their providers, so that those new technologies can benefit, especially, the poor. Second, progress in improving financial inclusion must be compatible with the traditional mandates of financial regulation and supervision, namely, safeguarding the stability of the financial system, maintaining its integrity, and protecting consumers.

Recognizing the possible synergies is important: financial inclusion, especially when driven by novel technology, is likely to enhance financial stability, increase its integrity, and allow for greater protection of consumers. Financial stability will be enhanced if greater financial inclusion broadens the system's customer base, allowing financial services providers to diversify their risks beyond the large corporations and state enterprises to which, in many developing countries, they often lend. Greater digital financial services provision can increase financial integrity, as it provides traceable records of transactions. Also, the transition to formal means of financial services provision can afford consumers greater protection than they may receive when they use informal money lenders and the like.

Those favorable synergies and outcomes are not guaranteed, however. Financial inclusion could be a source of system instability if the entry of new providers, using untested technological innovations and modalities, compromises overall soundness of the system. For that very reason, regulators are often wary of allowing nonbank DSPs access to the retail payments system shared by banks. Another concern for financial stability and consumer protection is that the

Box 1.1 A scorecard of the players and evolving business models in digital finance

New business models for financial services provision, often involving cooperative ventures among companies of different types from different industries, are rapidly expanding in developing countries and elsewhere. Often what distinguish these models from one another are differences in the degree of cooperation among the players. This box identifies the key players that interface with customers in this evolution and, following Bourreau and Valletti (2015), five types of cooperative business models for financial services, ranked approximately by degree of cooperation among players.

Key players

- Traditional full-service banks offer a range of financial services, such as deposit and savings accounts and loans; some of these services can be offered digitally.
- Credit unions and microfinance institutions provide services similar to those of traditional banks but have more limited charters.
- Specialized payment banks differ from traditional full-service banks in that they have a much more limited charter: they may not engage in lending and may accept individual deposits only up to a certain amount. India, for example, licensed 11 such payment banks in August 2015 to improve financial access in low-income communities.
- Digital services providers (DSPs) include mobile network operators and other nonbank DSPs.
  - MNOs are telecommunications services providers that may also offer a limited set of mobile financial services, possibly including digital wallets; an example is Safaricom's M-Pesa in Kenya.
  - Other nonbank DSPs include the following:
    - Money transfer operators, such as Western Union and MoneyGram;
    - Payment card services providers, such as MasterCard, Visa, and other card providers;
    - Payments providers, such as Venmo, Apple Pay, and PayPal; and
    - E-wallet and other services providers, such as Amazon and Google (Google Wallet).

Models of cooperation

- The light model involves minimal cooperation among providers, which may include banks, MNOs, and other digital payment services providers, such as PayPal.
- In the mobile-centric model, the mobile payments service is MNO led, and limited cooperation exists with banks and other players; examples include Tigo Pesa in Tanzania and MTN in Uganda.
- In the bank-centric model, the service is bank led, and little or limited cooperation exists with MNOs and other players; examples include Chase QuickPay in the United States and the mobile payment services offered by Stanbic IBTC Bank in Nigeria.
- The partial-integration model is characterized by strong cooperation between banks and MNOs but little cooperation between them and other digital payment services players. An example is Orange Money, a service that has partnered with local banks in parts of Africa.
- In the full-integration model, strong cooperation exists among players of all types. The emerging Peruvian model may become an example, as it promises to bring together the banking and telecommunications sectors, along with other stakeholders, to create a single, open, interoperable platform for digital financial services.

expansion of credit to previously unserved low-income households and small firms could result in excessive credit growth, leading to overindebtedness, high rates of default, and, ultimately—through the financial system's many interconnections—to systemwide risks. To avoid potential trade-offs between financial inclusion on one hand and financial stability, financial integrity, and consumer protection on the other, and to make inclusion even more likely, appropriate regulations and supervisory practices need to be in place. Thus, a sound regulatory framework needs to address new and evolving sources of risk related to the entrance of new market

participants, new technologies, and new modalities in the provision of financial services.

Before proceeding, therefore, an important step is to specify some necessary qualifications for the recommendations in this report to be effective. First, as a precondition, some critical elements of the regulatory framework must already be well established or pursued alongside these recommendations. Adequate solvency, liquidity, and other microprudential laws and regulations, matched by well-equipped supervisory institutions, must be in place for all formally chartered financial institutions and permitted financial activities, complemented by macroprudential tools and systemic oversight. Adequate consumer protection rules must be in place and be well enforced.[3] Second, efforts to increase financial literacy often will be needed, to educate underserved populations about the benefits of having access to financial services, how to obtain and use them, how to minimize risks in using them, and how to use the new technologies to access them. Third, each of the report's recommendations will have to be tailored to the institutional capacity of the country charged with financial oversight (which could be a foreign country). That does not mean that a country's initial institutional capacity must be assumed to be static and unchangeable. Deficiencies in any country's oversight capacity must be addressed. Failure to do so could prevent the implementation of important reforms that would allow greater market dynamism and greater financial inclusion without endangering consumer protection and overall financial stability.

An adequate regulatory framework that enables new developments in financial inclusion yet takes into account the traditional financial regulatory mandates is therefore the appropriate goal. To that end, this report's recommendations aim to support the development of markets for financial services suitable to the needs of the poor by encouraging entry of a large variety of providers and promoting balanced innovation and experimentation while avoiding creating incentives for financial instability and consumer abuse.

The approach to regulation for financial inclusion advocated in this report follows from the following three principles commonly used to guide regulatory choices (box 1.2; see also annex 1): similar regulation for similar functions, regulation based on risks, and balance between ex ante and ex post regulation. The combination of the first two principles implies that regulations should ensure that functionally similar services are treated equally as long as they pose similar risks to the consumers of the service or to the financial system as a whole. Differences in risks, and thus regulations, will largely arise because functionally equivalent services can be provided by different entities, as described in box 1.1. For example, as will be fully explained in the following sections, regulations for store-of-value services may differ between some DSPs and banks. Specifically, DSPs that fully invest the store-of-value funds they raise in safe and liquid assets (such as government bonds) and do not engage

Box 1.2 The approach of the report: Three principles for pro-inclusive regulation

1. *Similar regulation for similar functions.* Financial inclusion will be best served when regulation follows a functional approach—that is, when financial services providing essentially the same functions are regulated in essentially the same way, whether the provider is a traditional bank, some other type of financial institution, or even an entity whose primary business is not financial services at all (for example, an MNO).
2. *Regulation based on risk.* Regulation should also follow a risk-based approach, in which the stringency of regulatory requirements on any financial activity is commensurate with the risk that that activity poses to the individual participant (whether the consumer or the provider) and to the stability and integrity of the overall financial system.
3. *Balance between ex ante and ex post regulation.* Regulation should be sufficiently well specified ex ante to give providers clear rules of the game and enable competition for the market, but regulators should also have the authority to intervene ex post as the financial system evolves and regulatory or market development issues emerge. The challenge is to strike an adequate balance between these two approaches (see annex 2 for examples of this principle as applied by the European Union, Australia, and Kenya).

3. Good practices for financial consumer protection can be found in World Bank (2012b). Also, see the recommendations advanced by the Smart Campaign www.smartcampaign.org and DLA Piper/New Perimeter and the Microfinance CEO Working Group (2015).

in financial intermediation do not have to be subject to the type of regulations imposed on banks. Banks also offer stores-of-value—deposits—but by definition of their franchise, they offer deposits so that they can undertake financial intermediation through lending; thus, banks' deposit-taking activities are riskier. If, however, DSPs engage in financial intermediation activities, then the risk-based regulations should be similar to those imposed on banks. As the example shows, different providers offering a functionally equivalent service may be subject to different risk-based requirements. No such differentiation should exist with respect to other regulations, however, such as those to enhance competition, consumer protection, or financial integrity.

Determining the best regulatory approach for finance in general is challenging, as the rules will have to reflect each specific financial service and the risks entailed from alternative forms of service provision. This challenge is even greater for digital finance, given the many new forms of provisions and of providers. Put differently, in the new world, policies and regulations will have to vary in a number of dimensions to help ensure efficient service delivery that is also safe to the users and to the overall system. Using that framing, this report advances specific recommendations in three distinct regulatory areas: competition policy, leveling the playing field, and know-your-customer (KYC) rules. Each of these three areas is discussed in a separate section.

The first regulatory area, which will be addressed in section 2, is that of competition policy. Policy regarding the competition of markets must strike a balance between allowing new DSPs to enter financial services markets and ensuring that existing and new financial institutions act prudently; laissez-faire entry has rarely delivered a stable financial system over the long run. The aim is to encourage delivery of a full range of financial services by a system that is safe and sound overall. Financial services markets also should be closely monitored for the emergence of monopoly or oligopoly power, and antitrust authority must be securely in place so that regulators can intervene if necessary. On the other hand, given the enormous potential of digital financial markets to reach the poor but also the large uncertainties about how those markets might evolve and what modalities of operation will deliver the best results, competition policy should not discourage useful cooperation between players, including between financial institutions and DSPs, such as MNOs. To that end, coordination between the regulators of traditional financial services providers and those of DSPs is essential.

The second area of regulation, to be dealt with in section 3, is that aimed at leveling the playing field between alternative suppliers of financial services. The report's recommendations follow the principle that, to the extent possible, similar rules should apply for functionally similar services, regardless of the institutional form of the provider. In other words, any given service should be subject to essentially the same regulations, whether provided by a bank, an MNO, or another DSP. The report also acknowledges that different providers do not necessarily entail the same risks. Another level-playing-field recommendation is, therefore, to consider the risk that the supplier's activities pose on customers and the overall financial sector in such a way that the onerousness of regulation of any provider is commensurate (level) with the risk that the regulation seeks to address. For example, DSPs engaged only in payment services can be subject to lighter regulatory requirements than those engaged in inherently riskier activities, such as providing deposit services and also engaging in credit extension. A level playing field demands that the latter be subject to capital and other requirements similar to those imposed on banks.

The third regulatory area, to be discussed in section 4, is that of know-your-customer (KYC) rules, both domestic and international. Recommendations in this area aim to balance the valid motivations of KYC regulation—in particular the imperative to suppress, to the extent possible, all forms of illicit money laundering and financing of terrorism—with financial inclusion. The key is, again, proportionality: the stringency of any KYC regulation on any services provider should be proportionate to the risk to financial integrity that it seeks to address. The recommendations of the Financial Action Task Force (FATF) already incorporate this principle, but difficulties in implementation often have led to actions by providers inconsistent with the principle—actions that end up discriminating against inclusion. This report therefore calls for greater specificity in FATF guidelines and for policy makers at the country level to establish tiered KYC requirements and progressive penalties for noncompliance. National identification systems and coordination among national regulators must be improved, especially regarding cross-border transactions.

Because improved consumer protection is an overarching goal that runs across the different themes addressed in this report, consumer protection recommendations will be found throughout

the report. In addition, digital payment services receive special attention (box 1.3). Payments—transfers of items of value from one party to another in exchange for a good or service or to fulfill a legal obligation—have been a part of human economic interactions for millennia, evolving from barter to coinage to paper money to today's electronic forms. In modern societies, besides payments in cash and checks, many retail payments involve some digital component, as in a debit or a credit card transaction using a terminal at the point of sale (POS). In such a transaction, information is exchanged between the merchant and the bank or card company, authorizing the transfer of funds between bank accounts, on the basis of information embedded on the card (or in the chip in the card). Similarly, a direct debit transaction or the remote deposit of a scanned check involves the digital exchange of information.

Major progress in financial inclusion has been achieved through the development of digital payment services that do not involve a bank account, as when an MNO uses its network and agents that provide cash-in, cash-out services to allow customers to transfer funds. What is ultimately exchanged remains cash, but "transferring" it digitally is easier and cheaper. Building on this model, other digital services with features similar to those of a traditional bank account are being developed, some that offer stores of value, including some akin to a bank deposit account, with features such as recordkeeping.

More generally, the development of a fully inclusive financial system will likely be largely built on the achievements in payment services. The final section therefore discusses how regulations in all three areas apply in the specific case of retail payment services and adds further recommendations for regulation of that most fundamental service.

Box 1.3 Payment services: Why they are special for financial inclusion

Recent analyses (CPMI and the World Bank Group 2015; Demirgüç-Kunt and Klapper 2013; Radcliffe and Voorhies 2012; World Bank 2008, 2014) show that a well-functioning and inclusive payments system—one that allows all participants to send and receive payments in the most efficient, least costly, and safest ways—not only is essential to meeting the most basic financial needs of the poor but also can serve as their entryway to other, more advanced financial services, such as deposit accounts, credit, and insurance. After all, except for cash transactions, no financial transaction—however sophisticated or complex—does not involve using the payments (and settlement) system. In addition, advances in and expansion of digital provision have, to date, been greatest in the payments field, with many new platforms introduced that greatly facilitate financial inclusion. Indeed, a system that combines fixed and mobile access points (ATMs, phones, POSs), enables payments among various classes of agents (businesses, governments, individuals, and others), maximizes coverage, and is reliable, of high quality, and interoperable seems increasingly feasible for most countries.

Accordingly, the further development of both supply and demand with regard to financial services for underserved populations is likely to build on recent progress in the delivery of payment services. A sound regulatory approach to digital payments will provide important foundations for the productive development of other digital financial services and many directly applicable lessons. For example, addressing successfully the data confidentiality and privacy issues involved in new forms of digital payments provision can provide some lessons for improvements in credit information through "big data," so as to better provide credit to households and to small and medium-sized enterprises. Many other issues are likely also generic to the development of digital services, such as privacy concerns and externalities in the development of essential institutional infrastructure. At the same time, however, payment services regulation may have less to say about important issues specific to the efficient development of other financial services, such as the protection of depositors and other savers whose funds are used to extend credit.

Chapter 2
Competition policy

The regulatory challenge

Financial services markets, like most markets, are most efficient when adequate competition exists among services providers. Competition matters significantly for financial inclusion, especially in developing countries, because a contestable market—that is, a market open to fair competition—can expand to include potential consumers now on the sidelines. Competition also helps ensure that the financial industry engages in efforts to better identify the needs of the underserved, which may differ from those of the currently served. Competition policy thus must allow—and indeed, encourage—new providers to enter the financial services market, and it must make sure that no-longer-viable providers exit.

A challenge in all countries is that market competition cannot be taken for granted through liberal entry and judicious exit only but must be actively promoted and maintained. Policy makers also have to consider that financial services provision involves the use of many intermediate inputs, including networks with their own access and pricing structures that can create barriers to effective competition. Another challenge specific to financial services is how to balance the ease of business entry and exit with the adequate protection of all consumers and continued stability of the financial system as a whole.

The recent emergence of MNOs and other DSPs in financial services markets has brought to the fore new issues regarding the rules that should govern competition, both among these new entrants and between them and the traditional providers of financial services, notably banks. At the same time, however, the arrival of these new providers, some with their own networks built originally for purposes other than financial transactions, has opened new opportunities for cooperation among providers of all kinds, which can itself promote financial inclusion. Thus, another key challenge is how to encourage competition among all these different institutions and networks without deterring or precluding useful cooperation among them.

For now, much uncertainty remains about how these new technologies and business models will evolve and about which ones will deliver digital financial inclusion most effectively. Regulators therefore must leave plenty of room for market experimentation and innovation. Nevertheless, the recommendations on competition policy that follow can be expected to support sustainable financial inclusion only if the additional mandates of financial stability and consumer protection are also achieved.

This section of the report identifies five distinct areas for which regulators have to define the rules of the game with respect to competition policy, given the aim of improving financial inclusion: market entry, market exit, potential abuses of market power, interoperability of systems and services, and contestability of infrastructure. Specific recommendations in each of those areas will be offered.

Market entry

Because traditional and alternative providers of financial services differ in some crucial respects, we divide our recommendations between the two groups, limiting our attention to those services that are largely provided through the use of digital networks. In turn, within the second group, we distinguish between those providers that restrict their services to small payments and transfers or that offer fully safe stores of values, and all other providers. That distinction allows us to highlight some nuances in regulatory practice while letting the recommendations follow the functional and risk-based approaches described in the introduction.

Banks and other traditional providers

RECOMMENDATION 1. Provided that strong regulatory and supervisory institutions and solid consumer protection frameworks are in place, entry of "fit and proper" banks and other traditional providers into the financial services market must be facilitated, with the fewest and least intrusive regulatory barriers possible. Limits on the products and services these providers offer and on the inputs they use to produce and deliver services should be minimal.

As long as regulatory and supervisory requirements are met, no constraints on the entry of traditional providers should be imposed—the market should be fully contestable for domestic and foreign banks and other traditional providers. That contestability will foster competition among all banks and other traditional providers in the country, domestic and foreign, as it has in those many developing countries where foreign institutions freely operate. Rules governing the types of financial products that may be offered should also be limited, and they should be well specified and focused on enhancing consumer protection and safeguarding financial stability.

Regulations regarding bank branching, ATMs, and other (digital) contact points, such as points of sales (POS), should be minimal. Restricting the number, types, and locations of bank branches, ATMs, and POS unnecessarily weakens competition among banks; by making access to financial services less convenient, it also reduces the demand for them and undermines financial inclusion.

Banks and other traditional providers should be allowed, as they choose, either to work solely with third-party agents and networks, to rely entirely on their own branches and agent networks, or to construct whatever mix of branches, proprietary networks, and third-party agents they deem consistent with their internal business strategy (box 2.1). Accountability for the quality of those agents and responsibility for the services they provide, however, must remain with the principal—the bank or the network operator, depending on the arrangement chosen. That way, the entire network can be indirectly regulated and supervised without the regulator having to monitor every agent in the network.

The rules governing the use of offshore technology, data servers, and the like should be minimal and written in ways that do not differentiate by type of provider and that allow for their most globally efficient use. The potential benefits that new and globally active providers can bring to the domestic financial services market may not be achieved otherwise.

Abundant examples can be cited of countries where financial liberalization, including liberal entry, was undertaken without adequate regulatory and supervisory frameworks, only to be followed—often not long after—by a financial crisis. This unfortunate history has focused the attention of policy makers around the world on the appropriate conditions for allowing new entrants into the financial system.[1] Equally important are measures to ensure consumer

Box 2.1 Branchless banking through correspondent networks

Bank branches may be unprofitable in areas with low population density and low average income. Branchless banking or agency banking can help address this barrier to financial inclusion. Branchless banking can be achieved through digital services providers (DSPs), and indeed, much progress is being made in some parts of the world in this way, but banks can also establish their own agent arrangements with third-party entities. These entities may include lottery agents, local post offices, small retail outlets, and other parties with which banks contract (and to which they link digitally) to offer certain financial services, such as opening and using deposit accounts, making and receiving payments, and applying for credit. Branchless banking should therefore be facilitated through appropriate legislation.

For example, due to legislation enacted in 2000, the Brazilian banking system has enjoyed significant success in reaching dispersed populations in low-income areas through its large bank correspondent networks. In other developing countries, including in Sub-Saharan Africa, grocery stores and other small retailers are important bank correspondents. India, by contrast, has enjoyed limited success with its agent banking strategy because excessive regulation has made such operations unprofitable for most agents, especially in low-income areas, where their services are needed most.

1. In India, for example, the government undertook significant expansion of rural regional banks in 1976. However, the regulatory framework was poor, with overlapping rules and perverse incentives, which resulted in most of the new rural banks incurring losses by 1991. Similarly, in Albania in the early 1990s, the government supported the expansion of the informal sector as a means of extending access to financial services to a broader section of the population, but it failed to appropriately regulate those informal providers as their numbers grew. By the mid-1990s, pyramid schemes had become widespread in the sector, precipitating its collapse in 1996, which in turn led to civil unrest and economic turmoil. Also, Mexico deregulated its financial sector in the 1980s and 1990s with the intent of broadening financial access. Poor lending practices in the absence of adequate supervision led to a buildup of financial vulnerabilities, contributing to the tequila crisis of 1994–1995. Similarly, liberal financial entry contributed to the East Asia crisis a few years later.

protection to avoid abuse and misuse and to ensure that consumers obtain the greatest benefits possible from the new financial services being provided. Absent appropriate rules and adequate oversight, the risk is all too real that poorly tailored products get offered and that the failure of one or more of these new providers will lead to losses for depositors and investors and possibly even destabilize the entire financial system, resulting in economic distress and hardship that far outweigh any quick early gains in financial inclusion due to the new entrants.

Nonbank digital services providers

RECOMMENDATION 2. Entry of DSPs that restrict their retail activities to (small) payments and transfers, or that offer stores of value fully backed by safe assets, should be relatively liberal. In contrast, higher entry standards, including "fit and proper" entry rules and tests, should apply to DSPs that, in providing their services, pose risks to consumers and to financial system stability, such as those providing stores of value not fully backed by safe assets, credit, or insurance.

Increased competition can give rise to trade-offs between greater inclusion, consumer protection, and the soundness of the overall financial system. Entry regulations that are too stringent can constrain the growth and depth of financial services, including digitally based services. Regulations that are too lax can create risks for consumers and endanger systemic financial stability. The degree of regulatory strictness should balance these benefits and risks, but the degree of risk can differ by the form of provision. Payment services and store-of-value services fully backed by safe assets typically involve very little risk, whereas deposits that are used to extend credit are subject to the risks of abuse by, illiquidity of, and default of the provider. The strictness of regulation can therefore vary across different forms of provisions for functionally the same type of service.

Some principles of regulation will be the same, however, for all services and all service providers. For example, licenses of any type should be awarded only to providers that demonstrate the technical and financial capabilities necessary to ensure the quality of the services they offer. Similarly, regulation should also be designed to enable DSPs to expand their reach through the use of third-party agents. Just as banks, as described previously, should retain accountability for the quality and soundness of the agents with which they contract to provide services, DSPs and other providers should be held similarly accountable for their agents, whatever the service those agents provide. Rules that specify corrective action against DSPs whose agents' behavior violates minimum standards (which must be defined, at least in broad terms) should be in place and, again, should be the same as for banks and the same across all services. The restrictions placed on links between banks and commercial enterprises because of competition policy or financial stability should similarly also apply to links between banks and DSPs.

For some services, a set of minimum requirements will suffice. For example, for DSPs dealing only with small and limited person-to-person (P2P) transfers or that offer stores of value fully backed by safe assets, license requirements can focus mostly on minimizing risks for consumers— that is, on ensuring the DSP's technical capabilities to reduce operational risks and on documenting a record of honest business conduct and adequate governance capabilities. For those services, in most cases, the desirable model is a clear but relatively minimal set of ex ante rules for entry, with the explicit option of ex post intervention as the market evolves and new risks arise. The appropriate balance between ex ante rules and potential ex post interventions may vary from country to country, however, depending on, among other things, its legal and judicial systems and the state of its financial markets' development.

Additional requirements should apply to providers engaged in a greater volume of payments and transfers of larger amounts or in forms of store of value, which involve exposure to loss. The design of licensing rules for those providers should clearly assess the operational and reputational risks that each new player might impose on users and the financial system as a whole and mandate safeguards accordingly.[2] The thresholds between large and small amounts and volumes and between greater and lesser exposure to loss should be set at the authorities' discretion.

For nonbank DSPs that seek to offer digital financial services other than payments, transfers, and fully backed store-of-value services—that

2. For more on this topic, see sections 4 and 5. Additional requirements could also be needed to minimize the risk that "smurfing" (the breaking up of large transfers into smaller transactions to avoid crossing the regulatory threshold that triggers closer scrutiny) poses to the overall payments system.

is, services that can involve risks to the user or the financial system as a whole, such as deposits not fully backed by safe assets, credit, or insurance—even higher entry standards should apply, including "fit and proper" entry rules, as discussed previously for banks.

Market exit

RECOMMENDATION 3. For DSPs active in services beyond payments and fully backed store-of-value services, the rules governing exit from the market must be as well specified, on an ex ante basis, as they are for banks and should typically extend beyond those in the bankruptcy laws governing commercial businesses. Exit rules for DSPs that restrict their activities to small payments and transfers and fully backed stores of value, with no or limited (intraday) exposure to loss and small overall transaction volumes, can largely follow commercial bankruptcy laws and procedures—but with the option for ex post regulation—provided appropriate safeguards to protect customers' funds are in place.

Rules for dealing with weak banks and the prompt resolution of banking insolvencies are well defined, on an ex ante basis, by international standards.[3] In many countries, however, these rules, even when incorporated into local banking regulations, are not always properly enforced. Without appropriate bank exit regulations and enforcement, regulators tasked with maintaining financial stability might withhold or delay the approval of banking licenses for fear that the would-be new entrants might eventually fail and cause systemic disruption; their exclusion could diminish competition.

In contrast to those for banks, exit rules for nonbank DSPs generally are not defined beyond those in nonfinancial corporate insolvency laws. Specific rules can be stipulated, and again they should vary according to the activities of the provider. For DSPs that limit their activities to small transactions in payments and transfers and fully backed stores of value, with no or limited (intraday) exposure, exit rules can follow existing commercial law and procedures covering insolvencies—as long as appropriate safeguards are in place to protect consumers against fraud or loss of their funds due to the provider's solvency problems (see further discussion in section 3 and a specific example in box 3.2). Such safeguards may include specific operational requirements, such as requirements on crucial infrastructure, liquidity, and the like. Moreover, the option of ex post regulation should remain open, as uncertainties about the future evolution of markets can be great.

Exit rules similar to those for banks, and specified on an ex ante basis, are more appropriate for DSPs that have become large players in (retail) payment services, as a means of preserving the sustainability of the overall system. DSPs that offer financial services beyond payments and fully backed stores of value should be subject to ex ante exit rules regardless, along the lines of those imposed on banks.

Abuse of market power

RECOMMENDATION 4. Sound antitrust rules and procedures are needed in the financial sector to avoid the emergence of entities with excessive market power. The antitrust regulators must have adequate tools and resources at their disposal to analyze the current state of competition, and they must have the authority to break up monopolies and oligopolies, penalize collusive behavior, and challenge uncompetitive pricing structures.

Entry and exit regulations alone are not sufficient to ensure thriving competition in financial services. As market structures continue to evolve, first-mover advantages, network externalities, and other underlying features of the market may give rise to monopolistic or oligopolistic situations, especially in small markets with limited foreign competition. Earlier experiences with some financial services, such as credit cards, as well as with other digital services industries, such as software and search engines, suggest that anti-competitive behavior cannot be ruled out even when the conditions for entry and exit are pro-competitive. These situations often are hard to predict, however, and therefore a full menu of ex ante rules is difficult to design.[4]

3. Bank resolution is a relatively recent topic on the regulatory agenda. International standards were first advanced by the World Bank (2001).

4. In principle, ex ante provisions with regard to governance, pricing models, access, and so on can help control for some of the risks associated with anticompetitive situations. They can even encourage cooperative provision of networks and investment in infrastructures while reducing duplicative

To illustrate this concept, consider bundling, a strategy that involves joining products or services to sell them as a single unit. This strategy may turn into a cause for competition concerns if, for example, a manufacturer or MNO controlling a large share of the mobile (handset) market tries to leverage market power over complementary goods such as mobile payments. While the possibility of this occurrence cannot be discarded, it does not appear to be a prevalent behavior as to require regulatory intervention ex ante. Instead, such incidents are better tackled with ex post regulatory interventions, using antitrust law, and on a case-by-case basis.[5] At a minimum, therefore, this approach requires adequate antitrust rules, powers, and enforcement capacity to be in place.

The agencies that set and enforce competition policy must be continually vigilant of changes in the behavior of the companies they oversee if they are to detect anti-competitive practices quickly as markets and institutions evolve. Those agencies must be ready and able to enforce the country's antitrust and other rules and to take appropriate action ex post as new market failures emerge, especially in the rapidly evolving markets for digital financial services. When foreign financial institutions are established in the country, or when some financial services provision involves inputs from beyond the country's borders, international cooperation to restrain undue market power will be needed.

Interoperability

RECOMMENDATION 5. Interoperability among DSPs, and between them and traditional financial services providers—including through open (nonproprietary) technical standards—is essential for effective competition and for financial inclusion. Interoperability ideally emerges as a market solution, and if not, should be encouraged. If regulatory intervention is, however, needed, timing is key: interoperability should not be mandated either too early or too late.

Interoperability of telecommunications services—for example, the ability to make calls to users on other telephone networks—supports competition by preventing the largest provider from dominating the market, increases consumers' choices, and enhances their experience. In the same way, interoperability of digital financial services, such that any user on any network can transact with any other, is key to efficient financial services competition. In its absence, a single provider that has become significantly larger than the rest can exploit the network externalities that its size confers to attract still more customers, possibly becoming a monopoly. Interoperability also enables cheaper delivery of financial services for a given level of quality.[6] If, instead, a number of providers of relatively similar size and capabilities emerge, but their networks are not interoperable, the financial services they offer will be of poorer quality or more expensive, or both. Besides interoperability among mobile payments and other financial services providers, interoperability between such networks and other financial services networks, such as ATM networks—including through open (nonproprietary) standards—is central to allowing digital services to reach sufficient scale and to provide effective competition to traditional payment services.

Interoperability, therefore, can benefit consumers while also encouraging market deepening. The issue is whether (and if so, when) interoperability can be expected to emerge spontaneously, as a market solution, and if it cannot, whether (and when) it should be mandated. Ultimately, regulators should not mandate interoperability. Instead, they should allow the market to spontaneously develop and implement the proper arrangements to reach the desired objective. However, there are situations where regulatory intervention may be warranted. The timing of these actions is key: mandating interoperability among payment services providers too early can inhibit innovation, deter investments, and thus hamper the development of markets. Allowing it to emerge too late can lead to both inefficiencies (such as limited economies of scale, adoption of an inferior technology, or fragmentation of the overall system) and an entrenched monopoly. The result can be restricted access and higher costs for consumers—a recipe for continued exclusion.

Because of the costs associated with both "too early" and "too late" regulatory interventions, interoperability should not be mandated early on in digital payment services development. But the

investment. In practice, and especially in today's rapidly evolving marketplace for digital financial services, however, such rules may not suffice and partly relying on ex post interventions seems unavoidable.

5. See Bourreau and Valletti (2015).

6. This assumes that providers do not apply a surcharge to cross-network transactions.

regulatory authorities might consider taking steps to ensure that these services have the capacity to become interoperable later, for example, by requiring the use of compatible messaging conventions for all payments systems and services. The goal should be to allow sufficient scope for market development and competition within and between networks, while preserving the option to secure interoperability when the regulator assesses that the market has reached a sustainable degree of development.[7] Ex post regulation, when it occurs, need not be invasive, but it should at least prevent barriers to interoperability from increasing—that is, it should avoid moving backward. How this balance is struck in practice will necessarily vary from country to country.

Interoperability is more likely to emerge spontaneously, as a market solution rather than as a government mandate, where there are several players not grossly unequal in size. This implies that the design of entry rules for mobile financial services markets (discussed previously) and an ex post approach to interoperability are generally complementary. Tanzania provides an example of interoperability emerging without a regulatory mandate (box 2.2).

Interoperability can be achieved at different levels of financial services provision—at the customer level, the agent level, or the platform level. Interoperability at the customer level implies that customers can access their accounts using any phone with a SIM card on the same network. Interoperability at the agent level means that agents for one service may serve consumers of another service; no exclusivity applies. Interoperability at the platform level means that money transfers can be executed across networks: the user of one network can send electronic money to a user of another network, which may also be a traditional network, such as an existing ATM network.[8]

Ex post regulation to achieve interoperability need not imply a mandate for full interoperability at all levels at once. Instead, depending on market conditions and country characteristics, a sequential approach by level could be desirable. Kenya's policy, aimed at securing interoperability at the agent level but not at the platform level, is an example (see box 2.2).

Interoperability also means that existing systems should, in principle, be accessible to DSPs offering financial services, subject to standard safeguards. Full interoperability between traditional payments systems and newly developed DSP-operated payments and other financial systems would preferably emerge as a market solution—again, subject to oversight and possible ex post intervention. Regardless, as discussed in section 5, a number of preconditions would have to be met for DSPs to gain access to banks' payments and clearing systems.

Contestability of inputs

RECOMMENDATION 6. Taking into account choices made with respect to interoperability, except where consumer protection and financial stability may be compromised, inputs required for the production and distribution of financial services must be accessible to all providers interested in using them, be fairly priced, and be efficiently provided. Codes and standards can help toward this objective, but direct (ex post) government intervention to eliminate access barriers and address discriminatory pricing might be necessary at times.

Most network industries consider contestability of infrastructure services—the right of providers to equal access, on fair terms,[9] to the underlying networks and other inputs on which the provision of their services depends—a basic requirement. Telephone companies require access to common telecommunications lines, electricity providers to the power grid, water providers to pipelines, and so forth. This statement is no less true for digital financial services, which require, among other elements, access to network services for payment and settlement, credit bureaus, and a functioning telecommunications system. Although advances in technologies are rapidly reducing the vulnerability of some of these inputs to a natural monopoly (much as markets for telecommunications services have become more contestable), cases can still arise in which governments must intervene to avoid the adverse impact of dominant players.

7. For example, to facilitate the eventual achievement of full interoperability, the Bank of Uganda's Mobile Money Guidelines (2013) state that "Mobile money service providers shall utilize systems capable of becoming interoperable with other payment systems in the country and internationally, in order to facilitate full interoperability."

8. See Kumar and Tarazi (2012).

9. Pricing can vary based on volume, duration and scale of use, since those can determine different levels of costs, but should not otherwise be based on the nature of user.

Box 2.2 Full interoperability as a market solution versus as ex post regulation

In Tanzania, interoperability in the mobile payments market evolved through an industrywide process facilitated by the International Finance Corporation, which acted as an agnostic broker between the participants. One of the guiding principles was that all players, irrespective of the size of their business, had the same share of vote in reaching agreement on how interoperability would work. It was then a strategic business decision for each individual operator to join or not. The regulator's stated preference was for the market to reach interoperability on its own; hence, no mandatory regulations were implemented. Three of the country's operators, Airtel, Tigo, and Zantel, initially agreed to interoperate and went live in September 2014. Vodacom (M-Pesa) came on board in early 2016. The agreement allows users of all the networks to send money directly between their mobile wallet and that of any other user on any other network.

In 2014, MNOs in Sri Lanka and Pakistan achieved platform-level interoperability. MNOs in Indonesia had already implemented account-to-account interoperability in 2013 (GSMA 2014). As in Tanzania, in none of these three markets was interoperability mandated.

In Kenya, recent developments illustrate the business incentives created by an ex post regulatory approach to interoperability. M-Pesa, the leading mobile money service, offered by Safaricom, lacks full interoperability with any of the rival services offered by Kenya's three other operators, Airtel, Orange, and yuMobile. In July 2014, Safaricom opened up its M-Pesa agent network to rival Airtel—just before the Competition Authority of Kenya ordered Safaricom to open up its network of 85,000 agents to rivals. The concern of the Kenyan authorities was over the extremely high level of mobile money agents' exclusivity in the country, the highest in East Africa: before July 2014, 96 percent of agents were serving one provider exclusively (Helix Institute of Digital Finance 2013).

Agent-level interoperability still amounts to only partial interoperability because mobile money platforms are not yet interoperable; for example, an Airtel user cannot send cash from his or her mobile wallet to the mobile wallet of an M-Pesa user. Safaricom's initiation of this move of its own accord, however, in view of inevitable ex post regulation, is a promising start (Bourreau and Valletti 2015).

Furthermore, barriers to access in financial services are often more subtle than in other industries, and therefore the policies needed to foster contestability in these services are far from easy to define.

In many countries, policy actions that address contestability of infrastructure services have largely taken the form of putting pressure on traditional financial services providers to open their systems—for example, by articulating codes of conduct—so as to reduce barriers, promote the convergence of standards, limit collusive practices, and encourage scope for consumer mobility by lowering the costs of switching between providers. These efforts should not only continue but be extended to include the new, nontraditional financial services providers that also require access to these crucial inputs. Reciprocally, traditional financial services providers need access to crucial network inputs such as telecommunications services (for example, Unstructured Supplementary Service Data; box 2.3), which may be a challenge because MNOs are entering the financial services market (thus, delivering both telecommunications for multiple users and their own financial services).

In these and other areas, the framers of competition policy in the financial sector may have something to learn from the experience of other network industries, many of which have adopted relatively sophisticated policies. For example, in many infrastructure industries in recent decades, ownership or management of the network, or both, have been separated from the provision of services to ensure fairer competition. Access policies and pricing of network services also are often subject to regulatory review. In these other industries, some rules for those participating in the networks may be standardized through direct government actions or through self-regulatory agencies assigned the task, rather than left solely in the hands of private sector operators or owners.

Even when crucial input and output services are contestable in principle, strong general policy interventions may still be necessary

Box 2.3 Barriers to Unstructured Supplementary Service Data channel access hindering competition

Unstructured Supplementary Service Data (USSD) is currently considered the best available technology to deliver mobile financial services to low-income consumers. USSD is used for the majority of mobile payments deployments in developing countries (with the exception of M-Pesa in Kenya). As MNOs control this key input, there is concern about constrained access to USSD by other providers. Competition could be stifled if MNOs refuse to grant access to USSD, charge unfair prices, delay access, or provide access with poor quality. While MNOs may have valid arguments for withholding effective USSD access, such as potential network congestion, regulatory interventions may be needed to ensure contestability. As regulators decide how best to approach issues related to USSD access, it should be noted that an agreement between MNOs and other players through market forces would be the preferred approach to achieving the objective of enhancing competition. However, in the absence of a market solution, an external dispute resolution mechanism could be set up. As a last option, a coordinated regulatory intervention requiring MNOs to provide USSD access could be used (Hanouch and Chen 2015).

to make contestability work in practice. At times, policy makers may need to require standardization, speed the pace of adjustment, or remove barriers to access. For example, governments may have to insist on open (nonproprietary) technical standards to enhance competition. Furthermore, in recent decades many governments have required that retail payments systems initially developed by individual banks or groups of banks be integrated and opened to all would-be users. This has not only greatly increased the quality of payment services but also often lowered costs. Similarly, in the 2000s the European Union (EU) mandated that charges for financial transfers between eurozone countries be equal (subject to certain conditions) to those for domestic transfers. In addition, some EU countries have mandated easy portability of customers' bank account numbers from one bank to another.

In many countries, credit bureaus are run by banks or groups of banks for their own benefit and are not necessarily open even to traditional nonbank financial institutions, such as factoring companies, let alone new financial services providers, such as DSPs. Financial inclusion may require that access to the information held by credit bureaus be extended more broadly, to facilitate access to credit by low-income individuals and others now excluded, subject to appropriate safeguards and reciprocity standards. As this expansion of access proceeds, however, new policies will be needed to govern the ways in which the new DSPs use and share data about their customers among themselves and with traditional financial services providers. This is, after all, a new area in which issues such as privacy and the misuse of "big data" have to be carefully considered, while at the same time allowing the new data to be used for the delivery of financial services in profitable and sustainable ways.

A contestable infrastructure in the financial sector need not be a source of instability. Policy makers, however, should be aware of the trade-offs that can arise between consumer protection and financial stability on one hand and financial inclusion on the other when nonbank DSPs are granted access to a retail payments system previously limited to closely supervised banks. Such access can create risks for the entire financial system when, for example, a large MNO involved in digital services provision runs into difficulties in another (nonfinancial) part of its business.

Chapter 3

Leveling the playing field

The regulatory challenge

A level playing field in financial services refers to a regulatory environment in which all functionally equivalent financial services are treated equally, whatever the institutional form of the provider; and the onerousness of regulation of any provider is commensurate (level) with the risk that the provider's activities pose to customers and to the overall financial sector.

A level playing field starts with a clear definition of each financial service: What is a payment transaction? What types of stores of value are called a deposit? What is a credit? Often these definitions have been made at some point in time somewhere in a country's banking law or other laws, but the definitions may not have kept up with changes in financial services provision. More generally, inconsistencies in the treatment of services can arise from ambiguities in their formal definitions. This phenomenon is even more visible when looking at different jurisdictions and when financial products and services are offered across borders.

With a definition of each financial service in hand, a level playing field among providers of each service is critical to efficient service provision because it ensures that different providers compete on an equal basis in offering functionally similar services. It also reduces the scope for regulatory arbitrage. Because a level playing field can help expand the frontier of the market for financial services, it is crucial for improving financial inclusion.

Without a level playing field, inefficiencies in provision—static and dynamic—can emerge. Static inefficiencies arise when, even inadvertently, regulations are in place that raise costs for one type of provider but not for others, leading to higher overall costs and reduced access, or when regulations do not efficiently achieve the desired objectives of financial inclusion, consumer protection, and systemic financial stability across all functionally equivalent services. Dynamic inefficiencies arise when, for any new type of financial service, the current rules and market structure inhibit productive delivery and further innovation. As in other industries, an existing dominant set of institutions is likely to try to set the rules of the game in a way that subtly distorts the market to their advantage, thereby reducing dynamic gains—for example, by reducing innovation.[1] Some regulations in Indonesia exemplify distortions preventing a level playing field between e-money providers and constraining the development of their networks (box 3.1). Because of these issues, a common starting point in rules is dynamically very important.

A level playing field is possibly even more important for digital financial services and their role in financial inclusion than for traditionally delivered ones for two reasons. First, as experience has shown, the providers involved in digital financial services often are quite different one from another and often follow very different business models in their activities. This is especially true of the newly emerging providers. Second, the financial services that these different entities provide and the related services of importance to digital financial inclusion, such as the various financial and telecommunications infrastructures, are likely to be covered by multiple regulators.[2] Together these factors suggest that unless steps are taken expressly to prevent it, functionally equivalent digital services will likely not be regulated identically.

At the same time, the level playing field recommendation calls for risks to be regulated appropriately even if the providers

1. If digital finance is largely MNO-led, for instance, and one or a few MNOs dominate the telecommunication market, then obstacles to banks' access to the MNOs networks can easily emerge through access rules and pricing. Conversely, if the prevailing model of digital finance is bank-led, certain regulations might deter the efficient emergence and expansion of digital finance via MNOs. One example is excessive licensing requirements for MNO's agents (such as the requirement that agents of MNOs have full-service bank licenses, even if they are involved only in the cash-in, cash-out part of payment transactions). Another example is the existence of unwarranted limits to use the banks' clearing system.

2. In addition, differences are likely along many other dimensions, such as the tax and accounting treatment of products, depending on which class of provider offers the financial service.

Box 3.1 Indonesia: How regulation can undermine the growth of mobile money networks

Indonesia has an opportunity to become one of the world's largest and most inclusive digital financial services markets, with its high mobile phone penetration, large volumes of government-to-person payments, and diversified financial services industry. Despite these assets and the progress made in recent years, only 36 percent of Indonesian adults have an account at a formal institution (Demirgüç-Kunt and others 2015), and informal cash-based savings and payments still flourish. Recently, the authorities have sought to improve the status of financial inclusion in the country. For example, Bank Indonesia launched e-money regulations governing mobile financial services in 2009 (revised in 2014). However, so far neither banks nor MNOs have implemented inclusion programs at scale. The financial inclusion agenda remains constrained due to regulatory restrictions.

The e-money regulation permits only big banks with a core capital of approximately US$2.6 billion (known as book IV banks) to hire informal, unregistered entities (that is, mom and pop shops) as e-money agents. By contrast, smaller banks and MNOs can partner only with registered legal entities. Given that most airtime outlets and mom and pop shops in poor and rural communities are not legally registered, this restriction effectively blocks MNOs and nonbanks from building dense agent networks in these communities. As a result, MNOs are struggling to scale up their operations and expand their rural footprint.

offer the same or functionally equivalent services. Absent regulatory action to the contrary, the continual introduction of new financial products creates the possibility that the risks of various types of providers—banks, MNOs, and other nonbank DSPs—to the user and to the financial system overall will vary. Leveling the playing field means that different providers may be subject to different risk-based requirements, even when they offer functionally equivalent services that do not differ with respect to other regulations (such as those aimed at enhancing competition, consumer protection, or financial integrity). The need to assess risks appropriately applies especially for providers engaged in store-of-value services.

The recommendations in this section on contestability of market infrastructure are intended to complement those on competition policy in section 2. Here the report advocates, for example, against rules and actions that unnecessarily prevent MNOs and other DSPs from competing with banks in the area of digital finance. It also calls for proper and equal access to crucial institutional infrastructure—for example, for the ability of new players to tap into a payments system built and possibly dominated by existing providers. This section of the report begins by discussing and offering recommendations for two key areas for action: clearly defining each financial service and adopting a level playing field within each. Specific recommendations for payments, deposits, and credit services follow. The section concludes with recommendations regarding consumer protection and the structure of supervisory agencies.

Defining and differentiating between services

RECOMMENDATION 7. Leveling the playing field for financial services starts with regulatory agencies clearly distinguishing the various services from one another.

Defining the various financial services and clearly drawing the lines between them is difficult but essential. An important distinction is the one between payments-only services on one hand and store-of-value services on the other. This distinction can be based on the length of time the transaction takes (very limited in the case of payments) and the value of the transaction (small for retail payments). A store of value can then be defined as any balance, no matter where it is held, whose nominal value can be withdrawn at par immediately or used to pay for any type of good or service, real or financial.[3] It thus includes, among others, e-wallets and deposits.

Within the store-of-value category, further distinctions can be made using other criteria. These criteria may include, for example, the amount of recordkeeping needed (limited for e-wallets, greater in the case of bank deposits) and overall functionality (more limited for e-wallets, less

3. Even this definition, however, can leave some ambiguity as to what a deposit is and what a payment is. For example, whether a payments balance is considered "intraday deposits" depends on how a day is defined and on whether the payments service operates around the clock or not.

so for bank deposits).[4] The exact definition of a deposit with the general category store of value can be complex. A deposit can be defined as a store of value that has greater functionality; for example, its owner can use the deposit to make transfers and has access to records and statements (online or paper). Importantly, deposits typically come with additional recordkeeping and safeguard requirements for the provider. Other services, such as credit and insurance, must be defined, as well.

Regulating functionally equivalent services equally

RECOMMENDATION 8. To the extent possible and applicable, identical rules should apply to functionally identical services, regardless of the institutional form of the provider.

Today, and likely more so in the future, multiple forms of financial services provision coexist. What matters, however, is that the functionally identical services are treated equally. In turn, this means that the definition of each service must not be based on the type of issuer. For example, defining a deposit as a specific type of claim on a bank—and only a bank—violates the recommendation of equal treatment across providers.

Although the concept of a level playing field is a simple and familiar one, applying it in the form of specific recommendations is a complex task. Equality of treatment and regulation by function can require fundamental changes in laws to allow functionally equivalent services to be treated as such. Existing definitions of payment services in a country's banking or payments law may have to be revised, for example, to allow for new forms of delivery.

Even when providers deliver functionally the same service, a level playing field does not mean that regulatory approaches cannot vary across services providers when risks vary across providers. Importantly, MNOs and other DSPs whose business models restrict their provision of financial services to payments services, with limited intraday exposure, and fully backed stores of values need not be subject to the same regulations imposed on those DSPs whose financial services involve greater risks to users and the financial system. Such risks may include using the funds for lending or providing insurance or other forms of intermediation. One way of visualizing this is to think of providers of financial services as arrayed on a ladder, whose rungs represent increasing degrees of risk: the greater the risk to customers and the overall financial system associated with a given provider, the stricter should be the regulation and supervision of that provider. But, again, it should be done on the basis of the risks the provider represents, not on the basis of the type of service offered.

Payment services

RECOMMENDATION 9. A consistent regime for regulating all forms of payment services provision is preferable, and the rules should ensure a level playing field in the delivery of various payment services.

Payment services should be regulated under a payments law, which can be either a separate law or part of the banking law; in either case, the law should cover all forms of payment services delivery, including delivery by MNOs and other DSPs.[5] Although different models may exist, establishing a consistent regime for regulating all forms of payments services provision is desirable. A recent trend is toward countries adopting a general law that governs the national payment system, covering all aspects of the payment industry from operators to systems, instruments, and services.

RECOMMENDATION 10. Risks to users and general financial stability concerns arising from payment services, such as intraday settlement risks and other (systemic) risks, should be addressed within the payment system framework and should not differentiate by type of provider. MNOs and other DSPs that limit their provision of retail financial services to payments should be subject to payment regulations only.

4. In the new EU Payments Services Directive, for example, a "payment account" differs from a "bank (or deposit) account" in that the former may be used only for executing payments, whereas the latter can be used both for payments and as a store of value. This appears to be a workable definition and one that is being adopted by a number of other countries. Cash is also a store of value. It differs from many other stores of value in that it is held anonymously.

5. Section 5 of this report addresses the issues involved in achieving a level playing field and competition across providers of payment services; this section discusses how to establish a level playing field between providers of payment services and those of other financial services.

Rules that ensure a level playing field imply, among other things, equitable access to common institutional infrastructure and associated pricing rules that apply irrespective of the type of financial services provider. Rules must consider risks, though. They can therefore include requirements that providers use robust technologies and limit operational risks, thereby addressing, in part, the risks to consumer protection and financial stability. The rules can still differentiate by size of transaction, volume, and other technical or cost factors (for more on this topic see section 5) and, of course, when systemic financial stability concerns call for differential treatment (for example, when a single provider accounts for a very large share of aggregate transaction values or assets).

For most digital payment transactions, the risks that arise during completion of the transaction are small:[6] the funds will be available to the recipient almost as soon as they are sent. Because settlement of the transaction does not necessarily take place at the same time, however, risk can arise for the service provider and thus for the final user in case of the provider's failure. For the time an open position exists, it has to be managed within the payment system according to the usual payment regulations.

Because the payment transactions important for financial inclusion will be low in average value but can be large in aggregate volume, and because some of the providers (typically the new ones) are not necessarily otherwise regulated, some adaptation will be necessary to make the model safe for financial inclusion. One way to cover some of the individual and systemic risks inherent in the intraday flow of payment services provided by an MNO or other nonbank DSP, while preserving a level playing field, is to require each DSP to open a dedicated trust account at a bank while its customers maintain individual records with the DSP, but not with a bank. The MNO or other DSP would hold a single aggregate account at a bank for the total amount of individual net exposures (that is, netting out gross exposures). The size of the aggregate account would be subject to some limitations, in part related to the size of the bank and its capital, and the regulator may require the funds to be distributed across multiple banks as a way of ensuring diversification. Limits would have to be imposed on the size of payments eligible to be conducted in this model (for example, less than the equivalent of US$100 per day). This is essentially the M-Pesa model in Kenya (box 3.2).

This model, however, is less likely to suffice if either the aggregate account or the flow of transactions through it becomes large relative to the country's financial and payment system. In this case, regulators could require that, once a certain size threshold is crossed, the excess balances be invested at the central bank or in government or other highly liquid, safe securities to limit the risk of financial instability and contagion. Regulators might also require, as in the case of commercial banks, direct participation by the MNO or other DSP in the clearing system, which would also give the regulators direct visibility at the transaction level; or, if the DSP remains an indirect participant, it might be required to share some aggregate data with the regulator.[7] Other measures, including rules regarding the use of robust technologies, might be adopted alongside or instead of these requirements—again, to reduce overall risk.

Providers of store-of-value services

RECOMMENDATION 11. For MNOs and other DSPs whose services go beyond simple payment transactions, additional regulation and supervision should apply. Those regulations may include restrictions on the use of the funds. For those store-of-value instruments that are not fully backed with safe assets, regulations should typically be similar to those that apply to deposit-taking institutions ("banks"). They can include, if applicable, insurance and related requirements.

To level the playing field regarding risk of the provider, DSPs and other providers of payment services that do not offer a store of value should not be subject to the same regulatory requirements imposed on those that do. For the small transactions with limited (intraday) exposure that these providers handle, payment system regulation and oversight should provide adequate protection to the individual for risks in the transaction and to the financial system for the risk in the flow of transactions and otherwise. These providers will,

6. If the services provided by DSPs extend beyond payments to providing a store of value, they must be regulated differently (see the subsection on deposit services later in this section).

7. Payment services providers should not necessarily be required to be direct participants in a clearing system, given the costs involved, and providers may find that indirect participation is more cost effective.

Box 3.2 M-Pesa and other models for ensuring liquidity and safety for digital payments

To ensure that a customer's money held by a nonbank mobile provider is safe while the payment is being completed, regulators typically require that the provider maintain a specified amount of liquid assets and satisfy some other limitations. One common approach is to require the funds that are collected but not yet transferred to and cashed out by the final recipient to be "ring-fenced" (that is, legally segregated from other assets of the provider) and held in a bank account. This is essentially the M-Pesa model in Kenya. M-Pesa is a payment platform. Funds from the cash-in payments received but not yet paid out are deposited in trust accounts held by Vodafone, M-Pesa's owner through its local operator Safaricom, at several commercial banks. Those banks, like all commercial banks in the country, are prudentially regulated by the Central Bank of Kenya, and the funds are segregated from those of Safaricom, so that in case of its bankruptcy, the funds will not be comingled. Liquidity and solvency concerns are thus reduced because funds in any amount that at a given point in time remain in the mobile money system are fully backed by the pooled account or accounts.

An alternative approach, used in the Philippines and the West African Economic and Monetary Union (WAEMU), requires that the funds be held solely in certain liquid assets designated by the central bank as appropriate for the purpose. In the WAEMU, the total assets held this way may not exceed 10 times the provider's capital. The approach in the European Union is to require that funds be either deposited in banks (to which standard concentration and exposure rules then apply) or invested in segregated, low-risk liquid assets. Providers may also take out insurance to cover any deficiency (di Castri 2013a).

however, still be subject to some requirements, such as disclosure rules and KYC rules (with various exemptions based on transaction and value thresholds, see section 5).

In contrast, MNOs and other providers whose services go beyond simple payment transactions to include store-of-value instruments should be subject to additional regulations. Among those regulations may be additional recordkeeping, disclosure, and higher KYC requirements. Importantly, providers will be treated differently depending on the risks that they impose, which will vary depending on whether the stored value is invested in safe assets or used for making loans or other risky investments.

For many forms of store-of-value instruments, safety will come in the form of the assets allowed to be held and other limitations imposed on the activities of the provider. A limitation that is increasingly viewed as appropriate is for the DSP to be prohibited from on-lending the funds, but rather be required to either hold all the funds collected in a segregated deposit at a bank or invest them in safe assets, such as government and other highly liquid securities.[8] In such cases, even if not insured, the funds will be safe. One specific such form is a narrow bank.[9] This is essentially India's proposal on payment banks (Reserve Bank of India 2014): these DSPs must obtain a banking license, but the license they acquire is not a "full" one in that the DSP agrees not to exercise its lending rights under the license but must invest in certain explicitly permitted securities. Other legal models, such as trust funds, can be used, too. These DSPs would still be subject to other rules (similar to brokers' investment and segregation rules), as well as other requirements, such as concentration limits, but would not be subject to further bank-type regulation and supervision.

For DSPs that offer store-of-value services but that are not willing to forsake lending or other intermediation activities, the question arises whether other forms of safety can and should be provided—including insurance—through public mandates. Many, but not all, countries today have deposit insurance for banks, and this report does not proclaim that countries should have it, as it comes with not just benefits but risks. Deposit insurance for banks is well understood; it provides protection for depositors from the consequences of bank failure and is known to reduce the risk of a run on a bank or on the financial system at large. At the same

8. The criteria for these securities could be aligned with that of "Level 1 assets" (high-quality liquid assets), as recommended by the Basel Committee on Banking Supervision in its Basel III standards; see BCBS (2013).

9. Narrow banks (also called payment banks) are already safe because of the restrictions on their investments. Nevertheless, accounts could be covered by deposit insurance to avoid any misperceptions and possible adverse competitive implications. For example, payment banks in India are covered by deposit insurance.

time, deposit insurance introduces moral hazard and can lead to increased risk taking on the part of banks, which can, in turn, create systemic risks. Extending insurance to all store-of-value forms could be risky for any insurance agency and for the government more generally.

To reduce moral hazard and other risks, when deposit insurance is present, related bank regulations typically involve rules for the types and amounts of assets that may be held, the types of activities in which the bank may engage, its structure of liabilities, and how to resolve problems of illiquidity and insolvency when they arise (for example, many banking laws around the world, but not all, specify depositor preferences in bankruptcy). All such rules aim to reduce risks and protect the depositors and other creditors of the bank, the deposit insurance agency, and the overall financial system in the case of bank failure.

Although the general consensus is that nonbanks involved in the provision of store-of-value services need some regulation and supervision, as yet no established best practice exists regarding the need for and usefulness of insurance or about the best specific regulations and modalities accompanying it for various classes of store-of-value products. The answers will, to a large degree, be country specific. From the perspective of ensuring a level playing field, however, distinguishing among three groups of services is useful:

- Services that are required to have insurance.
- Services that are not allowed to have insurance.
- Services whose providers are allowed to choose whether or not to have insurance.

The criteria used to define those three groups can be expressed in either positive or negative terms, that is, according to whether the characteristics of a service or the activities of the provider indicate that it should be included or excluded, respectively, from a group; whatever the criteria chosen, overlaps and gray areas may occur. Providers granted access to insurance or required to have it will of course also have to meet other criteria, as will be discussed further. For those providers not granted access to insurance or that choose not to have it, other rules may apply (for example, their product documentation may have to carry a disclaimer stating that "these funds are not covered by insurance"). Issues pertaining to each of the three groups, consistent with leveling the playing field, are discussed next.

- Criteria for services that are required to have insurance include the following: the service is an extension of an already-covered regular bank deposit (for example, small amounts stored on a chip-card that is linked to an insured bank account); or the service is functionally fully identical to equivalent bank products (for example, a mobile checking account with functionality equivalent to a traditional account).[10]
- Criteria for services that are not allowed to have insurance may include the following: the stored value is usable only in a closed system (that is, only for certain transactions or certain stores, as with gift cards); or the stored value is not linked to an individual person or account but rather is stored anonymously, and the balance, in case of loss, cannot be restored (in other words, the stored value is equivalent to cash in terms of loss recovery); or the value is denominated in foreign exchange or some other unit with fluctuating value. Other criteria might also be used. The Philippines is a case in which insurance is not allowed for any type of digitally stored value.[11]
- Criteria for services that are allowed to be offered without insurance include the following: a low limit is imposed on the balance held (for example, less than the equivalent of a few U.S. dollars); or the stored value has not been acquired through a means that is already part of the regular banking or payments system (for example, gift cards bought in convenience stores); or the use of the stored value is not subject to certain security means, including ID verification and passwords, and is held

10. Besides the need to ensure a level playing field, an argument for requiring that some types of products be covered universally is one related to adverse selection: better capitalized or too-big-to-fail providers may prefer to opt out of deposit insurance—the former because they believe that they have sufficient capital to survive a run, the latter because they expect to be bailed out. This leaves only the weaker players—that is, those most likely to actually need insurance benefits—thus undermining the sustainability of the deposit insurance scheme.

11. In the Philippines, bank deposits that are digitally transacted, MNO-issued e-money, and certain other store-of-value accounts are excluded from deposit insurance coverage. In practice this means, for example, that if a bank holds funds for e-money purposes but the MNO manages the funds, the account holders do not have any insurance (GPFI 2014). Aside from the practical and political difficulties in adapting such fundamental pieces of legislation as a country's banking laws, the reasoning is not clear why all digital products should be excluded. Furthermore, to avoid repercussions, providers must raise public awareness that those products are not covered.

anonymously. All store-of-value products that do not satisfy these criteria may have insurance, at the provider's discretion —provided, of course, that they meet the other criteria (discussion follows).

All store-of-value services providers—whether banks, other financial institutions, MNOs, and other DSPs, thus including store-of-value cards and products such as balances in PayPal—must disclose to customers to what extent, if at all, their stored values are covered by insurance.

For providers that either are required to have or choose to have insurance, different models can be used for its provision. Insurance for digital store-of-value products can be provided in any of various forms—for example, directly or indirectly (box 3.3). Additional requirements for eligibility in an insurance scheme include those pertaining to recordkeeping, proper customer identification, and ability to promptly issue refunds in case of failure, including when working through third parties, such as MNOs. Importantly, deposit insurance comes with limitations on the type and quantity of risky assets held by the institution to reduce moral hazard and other concerns. Related to that criterion, the entity will be subject to supervisory oversight.

When a provider has the choice of whether or not to have insurance or chooses to provide safety in another way, trade-offs may arise that make the insurance option unattractive from the provider's or the consumer's point of view. One factor is the related costs, which, besides the recordkeeping and customer identification costs, include the insurance premium. Because those expenses will likely be passed on to the customer, they can deter financial inclusion. Providers may therefore choose to provide safety using the narrow bank or similar models or to forsake providing any form of insurance or safety, in which case other rules, notably on disclosing the lack of insurance, still apply.[12]

12. Some concerns parallel to the debate, mainly in developed countries, are regarding which financial products may or may not be allowed to have or are required to have government-provided insurance. Some financial instruments, such as money market fund accounts—notably those with so-called par value guarantees, as in the United States—have elements functionally equivalent to those of deposit accounts, but are not explicitly covered by deposit insurance because they are otherwise not regulated and supervised in the same way as banks. They do face limits, though, on asset compositions, and they have to disclose their status.

Providers of credit services

RECOMMENDATION 12. To the extent that the DSPs uses stored values to fund the credit it extends, additional requirements will have to come into play, typically similar to those applied to banks to protect the individual saver, the insurance provider (if the stored values are insured), and the stability of the overall financial system.

Like other nonbank financial institutions and nonfinancial corporations, DSPs can, in principle (subject to prevailing laws), be allowed and choose to extend credit to their customers or otherwise engage in forms of financial intermediation. DSPs can, for example, act as leasing companies or as person-to-person (P2P) and person-to-business (P2B) lending platforms. As with other credit providers, eligibility to provide those services comes with certain requirements for both lender and borrower, notably related to consumer protection (for example, because investment risks may arise and liabilities may exist beyond those reasonably covered under the principle of "buyer beware"). In general, depending on the exact legal structure chosen, the applicable rules will come from general commercial law or from specific laws governing nonbanks (for example, leasing or factoring firms) but not from microprudential or banking laws. Additional requirements may nevertheless arise. Some may come from securities laws; for example, although practice is still evolving, P2P and P2B platforms in some countries currently may not offer investment products beyond a certain size to the general public, and certain disclosure rules apply.

Rules will have to differ, however, if the financial services provider uses any stored values for credit provision because the safety of those values is no longer assured. To protect individual savers, the insurance provider (if the stored values are insured), and the stability of the overall financial system, additional regulatory requirements —similar to those applied to banks—will be needed. The case of Kenya's M-Shwari (box 3.4) shows how standard bank rules apply when a mobile deposit is used for lending, with the only difference being the channel or platform used to access the deposit and extend the loan.

More generally, DSPs that offer store-of-value instruments to the general public but are not fully backed by safe assets would be subject to general bank regulations and supervisory oversight. Specifically,

Box 3.3 Direct versus indirect provision of (deposit) insurance for digital accounts

Although so far no clear standard model has emerged, (deposit) insurance can be applied to digital transactional platforms through one of two main approaches.

The first is direct coverage, whereby regulation is adjusted as needed to bring digital transactional platforms within standard bank deposit insurance coverage. This model would apply to store-of-value products that are a direct extension of a bank deposit, and those products would not be subject to additional rules beyond those that apply to the primary deposit. The same argument applies if a specialized bank provides mobile deposit services through a subsidiary that is a deposit insurance member. This is the model used for M-Shwari in Kenya (see box 3.4). Direct coverage is more demanding for some modalities of providing deposit services. For one thing, the liabilities of any third-party agent involved, such as an MNO, would have to be clarified relative to those of the bank (for example, in the case of technical failure of the MNO to conduct a transaction). This model is practiced in Mexico, where banks hold and manage customers' funds while paying the premium for the digital transactional platform.

For store-of-value products not offered as extensions of a bank deposit, insurance can be offered but, consistent with a level playing field, the provider would be subject to the same regulations and supervision as banks with regard to deposit insurance, including coverage limitations and required contributions to the insurance fund. In the case of payment banks offering deposits, limits on their lending or investment would negate the need for many such requirements. These and other rules, such as requirements to fully back up amounts with investments in high-quality liquid assets, can also be applied to other store-of-value products. Limits would apply to the total amount that may be covered, whether held at the bank or in the store-of-value product.

The second approach is indirect coverage, whereby the aggregate customer funds held in pooled custodial accounts are insured, and some insurance is indirectly provided to the individual account balances managed by a third party (such as an MNO that issues e-money, or an e-money issue of reloadable prepaid cards). Because the funds in the bank really are no different from a normal deposit, they are subject to deposit insurance and associated regulation and supervision. The bank or banks in which the funds are held must of course themselves qualify for insurance, but the provider of the payment accounts (the MNO) need not. The main issue with this model is that the pooled account must also qualify as an insured deposit and importantly, its insurance will typically be capped to cover only a certain amount. For example, if the maximum coverage is limited to, say, Na100,000 per account, only a small fraction of the overall deposits aggregated in the trust account, which can run into billions of nairas, is insured. This means that for each individual account holder the fund protection is almost inexistent.

The United States provides interesting experiences with coverage of digital funds, using the so-called pass-through model. As long as the e-money is placed in a U.S.-insured depository institution, it is considered an insured deposit. For pooled custodial accounts, pass-through protection applies to each customer up to the insurance limit. To qualify for pass-through protection, however, the bank's records must disclose the custodial nature of the pooled account; the bank's records or the issuer must disclose the names of the individual owners and the amount owed to each; and the agreement between the issuer and the customers must indicate that ownership of the funds remains with the customer. Because these rules are not difficult to meet, most e-money schemes in the United States already comply, given their standard practices (FDIC 2008).

Kenya used to have indirect coverage for M-Pesa, as banks hold the customer's funds in bank deposits that are insured, but it has since moved to make individual accounts in principle eligible for pass-through treatment, along the lines of the U.S. example. An administrative issue for many developing countries for indirect coverage is whether the accounts data are kept up to date and can be reconciled quickly so that payout can be quick if needed. Additional requirements can therefore be imposed under indirect coverage, notably those related to recordkeeping in real time, with the ability to reconcile accounts, and assurances on the use of robust technologies and the like. Questions arise as to whether these additional requirements make this model practical for MNOs and whether they make indirect coverage equivalent in practice to direct coverage.

nonbank entities that use the fund they raised for lending or risky investment would have to become—and be licensed as—some form of bank. They would thus be subject to the same capital, reserve, and other prudential requirements as banks, as well as to any other limitations on banks regarding the types of assets they may hold and the activities in which they may engage, and they would be supervised accordingly. For all practical purposes, this implies that the vehicle used by the DSP becomes an independently capitalized bank that is regulated and licensed under the same law as banks. (This approach would also obviate the need for continued efforts to synchronize two different pieces of legislation intended to regulate effectively identical entities.) The regulations and forms of supervision to which they are subject could still, however, differ according to the rules applicable to various classes of banks or other deposit-taking financial institutions. For example, they could differ depending on size or by type of entity (such as microfinance institutions). The presumption is that those differentiations are justified on their own merits and do not tilt the playing field; if they do, further adjustments—which are beyond the scope of this report—will be needed.

For DSPs that do not go beyond offering small payments or transfers and small store-of-value services, the best way to avoid an excessive regulatory burden, while keeping the playing field level and avoiding systemic risks, is restrictions on the use of the funds, including through using the narrow bank model.

Consumer protection

RECOMMENDATION 13. All providers of financial services—banks, MNOs and other DSPs, and others—must be made subject to regulations aimed at protecting consumers from fraud, abuse, and discrimination. For any given service, these regulations should be equivalent across all types of providers of that service.

Box 3.4 Kenya's M-Shwari: A standard bank-based deposit and credit service offered via mobile means

M-Shwari is essentially a bank deposit account service offered by the Commercial Bank of Africa (CBA) as an e-wallet, with access offered through Safaricom's M-Pesa (see box 3.2). Each M-Shwari customer has a separate bank account with the CBA, which pays between 2 and 5 percent annual interest depending on the characteristics of the deposit. Deposits in and withdrawals from M-Shwari deposit accounts can be made only through M-Pesa (which sets its own maximums on balances, daily transaction values, and values per transaction, as well as a minimum withdrawal amount) and its agents, which handle the accounting. Short-term loans similar to other bank loans also are available through M-Shwari to customers with good credit scores, derived from the customer's past usage of Safaricom products.

Because M-Shwari deposits are standard bank deposits, they are subject to the reserve requirements, deposit insurance requirements, and other regulations and supervision that apply to any bank deposit. M-Shwari deposits also are counted in the standard measure of financial inclusion in Kenya. Know-your-customer (KYC) requirements are similar to those in other countries: tiered levels of deposits may be opened based on stored data for M-Pesa (for tier 1), verification of M-Pesa KYC data on the government's individual database registry (for tier 2), and original data and a copy of a PIN certificate (for tier 3). This KYC procedure is compliant with FATF standards and recommendations aimed at balancing the goals of financial inclusion and reduction of risk.

Since its launch in November 2012, M-Shwari has met with considerable success. As of mid-2015, the service had attracted some 5 million customers, and CBA disburses 50,000 loans every day (Cook and McKay 2015a, b). This rapid growth, compared with other countries where bank deposits have been offered along with mobile money, probably reflects the ease of signing up online for the lowest tier and the ease of depositing and withdrawing funds through M-Pesa and its agents. The success of M-Shwari has also encouraged other countries to use digital personal information data to form the base of KYC and to overcome the information asymmetry problems inherent in extending credit safely.

Full transparency and disclosure to consumers about the characteristics of products being offered to them, as well as about fees (direct and indirect) and interest charges (when relevant), are the first line of consumer protection. Accordingly, the relevant authorities must set standards for disclosure that are adequate and equal across providers of a given service.

Protection against fraud usually follows the country's commercial law, which applies equally to banks and nonbanks. Where this is the case, a level playing field should already be in place, at least in principle, if the legal and judicial system is operating adequately. Where this is not the case, additional rules, harmonization of existing rules, or both are essential, as is effective coordination among the various regulators involved.

Regulators also must ensure that, when fraud or other infractions occur, proper recourse mechanisms for consumers are in place and, for a given service, do not differ by type of service provider. This recommendation may require some adaptations to current rules and modalities. For example, for very small transactions, "no-fault" or equivalent rules for nonbank providers may be needed (under such a rule, the consumer does not have to prove his or her case to prevail, but the provider can still prevail if it can show neglect on the consumer's part). Recourse for nondelivery of a small payment sent through a service provided by a DSP will require a different approach than for "typical" payments through banks for commercial (nonfinancial) business transactions.

The rules also have to ensure that in no part of the process of providing payment (and other financial) services does any discrimination against certain classes of customers (for example, women) exist. This stipulation can call for, among other things, efforts to train staff in understanding and appropriately addressing cultural or religious diversity among customers.

These recommendations do not suffice to fully ensure consumer protection in general, and increased financial inclusion can create new consumer protection concerns. For example, well-intended policies sought to increase U.S. homeownership by making mortgages available to households previously excluded, using, among other tools, innovative financial technologies. The combination of those policies and innovations with poorly structured incentives, faulty rules, and lax oversight—in short, a failure of regulation—allowed for the widespread sale of products ill-suited to the consumers to whom they were marketed. In fact, the recent U.S. financial crisis is sometimes blamed on those practices, as they led to systemic risks.

Beyond the recent crisis, there are many cases of exploitation of vulnerable customers, whether through sale of inappropriate or overpriced products or through outright fraud and theft—Ponzi schemes being a classic example. Microfinance institutions' problems in South Asia are one of the many examples in which financial inclusion goals were compromised. The lesson to be learned is that for all their potential benefits for inclusion, financial innovations can at times be hijacked and turned into threats to consumers, which regulation must be constantly ready to address through means that go beyond ensuring sufficient disclosure and recourse mechanisms. A useful initiative that supports policymakers' efforts to improve financial consumer protection is the World Bank's Consumer Protection and Financial Literacy diagnosis' tool, which assesses a country's legal, regulatory, and institutional frameworks for financial consumer protection using the World Bank's Good Practices for Consumer Protection (World Bank 2012b), as a benchmark. More than two dozen developing countries had been assessed and received recommendations by the end of 2015.

Establishing clear supervisory assignments

RECOMMENDATION 14. Coordination among supervisory agencies is as essential for digital financial services as for traditional ones. Coordination problems can be minimized by specifying clear mandates for all agencies involved and by ensuring their adequate accountability and independence. Memorandums of understanding can further help improve coordination.

Coordination among different supervisors remains often difficult to achieve for a variety of reasons: information may not be easily or fully shared because of legal barriers; mandates may overlap or may not be clearly defined; and, especially, the presence of multiple supervisory agencies may ignite turf battles. These problems can give rise to overlaps and gaps in supervision. Even when regulations and guidelines have been well designed ex ante, unforeseen risks can remain, calling for ad hoc, ex post regulatory interventions. Such circumstances will test regulators' ability to avoid coordination failures across multiple agencies.

These challenges also arise for nondigital financial services, so some general advice thus applies. The key to avoiding coordination problems is twofold: clear mandates for all supervisory agencies, and proper accountability and independence of each. Beyond that, however, specific recommendations for institutional design are hard to come by. Regular meetings between staff of the various agencies and the central bank—to discuss issues, reach decisions, resolve conflicts, apprise each other of what they are doing, monitor implementation, and plan initiatives for the future—can help.

More may be needed for the new, digital services, however.[13] As a practical matter, some sort of explicit, formal mechanism of coordination between the MNO regulator and the authority in charge of payment oversight rules may also have to be in place. The development of memorandums of understanding between relevant authorities (such as the Central Bank and the National Communications Commission) can provide a useful framework to foster and institutionalize dialogue and collaboration between various government departments on matters of mutual interest and where the authorities' competence is not exclusive. This communication can help define who should be in charge of enacting and enforcing rules in the digital finance space. The coordination task can be eased to some degree by creating separately capitalized subsidiaries for specific services so that even if other resources (networks, agents, branches) are comingled, the legal ownership of claims is clearly defined and therefore capable of being regulated and governed independently.

13. The problem is not different in principle from the usual one of multiple supervisory agencies. The lessons here are limited, because many models exist: some countries have a single supervisory authority, others "twin peaks" (separating prudential supervision from supervision of business and market conduct); the deposit insurance agency, or the central bank, may or may not be involved in supervision; and so on. Each arrangement has its pros and cons; hence, no simple ranking of models by efficacy is possible.

Chapter 4
Know-your-customer rules

The regulatory challenge

Financial integrity is an essential regulatory objective. To pursue this objective, an international policy advisory body, the Financial Action Task Force (FATF), created a number of standards to promote effective implementation of legal, regulatory, and operational measures for combating money laundering (ML) and the financing of terrorism (TF). Essential to operationalizing financial integrity is the need for financial institutions to know who they are dealing with. A financial system in which customers are allowed total anonymity is one that can easily be abused and corrupted, including by persons or entities engaged in ML/TF. Such a system also is more subject to the risk of financial cronyism and related financial instability. Last, but hardly least important for purposes of this report, financial institutions that do not know their clients will be less willing to extend their full range of services to them, thus hindering financial inclusion. Hence, strong KYC rules governing all financial institutions are indispensable to the efforts of the global community toward financial integrity and financial inclusion.

The challenge in designing such rules, at the national and the international levels, is to ensure that they are always consistent with the objective of financial inclusion—that is, that the rules are adequate to the task of maintaining financial integrity yet do not create unnecessary barriers to inclusion, but rather, work to enhance it where possible.[1] A consensus on this goal is already shared among policy makers worldwide who are working to develop sound KYC rules. It is reflected, in particular, in the current recommendations of the FATF in its fight against ML/TF. Those recommendations now explicitly acknowledge the need for a risk-based approach—as advocated here for other goals, as well—to be developed through the principle of proportionality. As expressed by the G20, "To strike the right balance, existing regulations should be carefully analyzed to establish whether their demands on service-providers are proportionate to the risk" (GPFI 2011).

What is much less clear is how, precisely, to implement the risk-based approach.[2] The cost to a financial services provider of applying due diligence to meet a given set of KYC rules varies less than proportionally with the size of the customer's account. If, by ignoring this reality, KYC rules are not defined differently for different types of customers, particularly the poor, financial inclusion will be undermined because financial services providers may then find that applying the rules to the smallest accountholders is uneconomic, and they may therefore choose not to seek their business or to accept them as customers, or the providers may charge them more than most low-income customers can afford. More generally, KYC rules have to reflect the realities and the risks of those parties seeking access to finance.

Internationally, and to a significant extent within many countries as well, KYC regulations do not yet meet the essentials of a rigorous, risk-based approach (box 4.1). The task, then, is to implement the approach in such a way as to improve financial inclusion and financial integrity. Recommendations for KYC also must be consistent with the more general recommendation in section 3 to level the playing field between various types of financial services providers. The rules should not seek to tilt the playing field in favor of or against banks, providers of mobile money, or other institutions involved in service provision, such as MNOs and other DSPs.

A number of features of current KYC regulations worldwide are not consistent with a risk-based approach. First, the stated aim at present is to completely eliminate ML/TF. Certainly, no level of

1. For further discussion of the international dimension, see CGD (2015).

2. Importantly, there is a need to generate and use data to support the risk-based approach. However, further analysis is needed to determine efficient ways to proceed with these tasks.

Alan Gelb is the main contributor to this chapter.

Box 4.1 Biometric screening: How a risk-based approach can inform technology choices

Although the details may differ from one industry or regulatory area to the next, effective risk-based approaches to setting regulatory policy share four characteristics: First, the cost–benefit trade-offs between the alternative risks that policies seek to minimize are clearly understood. Second, incentives and penalties are properly calibrated to achieve an optimal balance among the identified risks. Third, should risks materialize, responsibility for that outcome is clearly specified. Fourth, enough is known about the effects of alternative options for mitigating risks to inform policy makers' choice of the optimal trade-off.

Biometric screening shows how a risk-based approach to KYC can lead to different policies when the objectives and the conditions differ. Any technology for biometric screening will be associated with a specific trade-off between Type I and Type II errors: the more the system is tuned to prevent Type I errors (false rejection—that is, denial of a legitimate identity claim), the more it will be prone to Type II errors (false approval—that is, acceptance of a false, and possibly fraudulent, identity claim).

Investment in a higher quality technology, however—for example, replacing fingerprinting with iris scans, or combining the two—can reduce either or both types of errors, resulting in greater overall accuracy of identification. This presents a trade-off of a different nature, namely, between accuracy of identification, on one hand, and cost and user convenience on the other. For example, requiring fingerprints and iris scans might reduce both types of errors, but it might require a more costly system and be more time-consuming for users.

A risk-based approach to screening recognizes that the optimal choice along any trade-off curve will be different for, say, access to a nuclear facility than for access to a health program. In the first case, Type II errors are to be rigorously avoided, even if it means that more Type I errors must be tolerated and that users may be rather seriously inconvenienced; the consequences of failing to block a fraudulent identity claim are simply too great. In the second case, too many Type I errors could lead to many eligible recipients being denied service, and too inconvenient an identification procedure could lead frustrated users to abandon the program. Thus, in this case it is better to err in the direction of tolerating Type II errors and to trade off some higher level of misuse for greater ease of use.

A second point also emerges from the adoption of a risk-based approach, namely, that any penalties levied on the security provider should depend on the severity of the consequences of a breach. To continue the preceding example, penalties should be far higher for a breach of nuclear security than for a case of unauthorized health system access. The stronger sanction for error for more serious breaches establishes an incentive for the security provider to be more vigilant—and to adopt a more accurate technology, if the provider has the choice and if the technology is not so expensive that it is cheaper to pay the penalty for error.

either activity is to be condoned. In practice, however, no amount of regulation can hope to reduce these activities to zero simply because criminals determined to engage in those activities can resort to less transparent options outside the formal financial system.

Second, current approaches do not provide clear guidance on how to calibrate due diligence to the scale of social risk. Requirements that fail to differentiate between large and small customers work to the detriment of financial inclusion because the cost of due diligence becomes extremely high for the provider and the user, relative to transaction size, when the transaction is small. Low-income customers are thus, almost by definition, those whom standard due diligence procedures will tend to price out, leaving them financially excluded.[3]

Third, current KYC regulations do not clearly articulate which violations of ML/TF laws are considered more serious and which

3. Estimates of the costs of complying with ML/TF regulation suggest that the direct, out-of-pocket costs are high and increasing over time, both for traditional financial institutions and for other providers of financial services, and that KYC-related costs represent the second-largest component of those costs. However, the breakdown of those high reported costs across small and large clients remains unclear (KPMG International 2014).

less so, and the correlation between the severity of the offense and the penalty to be imposed is missing. Although the largest fines to date have involved scandalous cases of willful violations, penalties for less egregious offenses have been largely uncertain. A sound regulatory approach is needed to create more clarity ex ante; penalties cannot simply be decided ex post as violations are discovered. Without greater clarity, financial institutions will naturally assume the worst and respond as if all infringements carry a very high penalty. This is bound to lead to outcomes that are inefficient from the perspective of financial inclusion. Extreme uncertainty among providers about the penalties they face will reduce their incentive to provide services to all, but especially to small clients from whom the provider already earns relatively little profit.

Finally, the current regulatory regime relies on strong customer identification credentials. In many countries, however, the basic legal ID system is weak or even nonexistent, which can undermine the value of KYC efforts. Because existing forms of legal IDs cannot be relied on, providers are forced to develop their own identification credentials (like the bank verification number in Nigeria), which is costly and possibly uneconomic for smaller accounts, again discouraging inclusion. The "K" in KYC can thus not be separated from the need for robust identification to be widely and easily available, including to low-income individuals.

This section of the report identifies six areas for action: better coordination of KYC efforts; requirements to take a practical, risk-based approach; stronger national identification systems; clarified and more graduated penalties for violation of KYC rules; increased direct international transactions; and differential approaches, by country.

Improving cross-border coordination

RECOMMENDATION 15. An urgent need exists for greater coordination of efforts toward a sound global KYC regime, both among the national authorities of different countries and—within some countries—across individual agencies. Clearer guidance from the FATF could be useful in both cases.

Cross-border transactions pose special challenges to a risk-based approach to KYC. One challenge is the present lack of coordination between countries' regulatory authorities regarding ML/TF risks. Another is the heterogeneity of financial corridors between sending and receiving countries. A third is the additional regulatory uncertainty stemming from the multiple layers of existing guidance and regulation—from the FATF, from national regulators, and in some countries, such as the United States, from regulators at subnational levels. Although countries on their own can make progress on the domestic front, improving the trade-off between KYC requirements and the ease of cross-border transactions will require better coordination between regulators across countries, particularly because some national rules have implications for other countries.

Scaling KYC requirements to client size

RECOMMENDATION 16. In line with the risk-based approach, KYC rules should recognize the minimal risks posed by customers undertaking small transactions by allowing for restricted and graduated accounts. Less onerous KYC measures should be required for certain types of basic 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 DSPs: the rules must be similar for all providers of the same service.

One important way to maintain financial system integrity without undermining financial inclusion is by establishing tiered KYC requirements. Typically this is done by creating restricted accounts, with limits on balances and transactions and subject to simplified KYC requirements. Cumbersome forms of documentation that many poor people will be unable to provide, such as proof of address and a declared source of income, should be waived for these accounts. Instead, a basic form of legal identification should suffice. India, Peru, and South Africa are countries where banks already offer restricted accounts involving lower levels of due diligence (box 4.2).

In the mobile domain, SIM card registration can provide a minimal and equivalent KYC requirement for opening a restricted account. Many countries already require the registration of SIM cards (the removable chip within a smartphone or other device that contains information about the user's identity): as of July 2013, at least 80 countries had mandated or were actively considering mandating the registration of prepaid SIM users (GSMA 2013). Box 4.3

Box 4.2 Restricted bank accounts in three developing countries

India, Peru, and South Africa have implemented the risk-based approach for the formal banking sector by establishing reduced KYC requirements for "basic" bank accounts with limits on balances and activity (inflows and outflows). 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 4.4). The maximum balance in a restricted account is Rs50,000 rupees (US$733.49),[1] the aggregate of all credits in a financial year must not exceed Rs100,000 (US$1,466.99), and total withdrawals and transfers in one month may not exceed Rs10,000 (US$146.70). In Peru, restricted accounts require only a national ID and are limited to a balance of not more than 2,000 soles (US$571.96), with daily transactions capped at 1,000 soles (US$285.98). In South Africa, restricted accounts have a maximum balance limit of R25,000 rand (US$1,580.63), a daily transactions limit of R5,000 (US$316.13), 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 no 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, Namibia, and Swaziland).

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, Peru requires information about the accountholder's occupation and employer and the purpose of opening the account, and South Africa requires at least an address and tax number. All three countries also have reasonably good mechanisms to authenticate that the customer is in fact the person shown on the ID—a capability that is lacking in some other countries.

Note

1. Conversions to US$ are estimated using the average daily exchange rates during February 2016.

describes how SIM card registration works to establish restricted accounts in Kenya.

Authorities in a number of countries have thus already made significant advances in complying with the objective of KYC recommendations by allowing the introduction of restricted bank and mobile accounts subject to less onerous KYC measures. This policy formally (if implicitly) recognizes the lesser riskiness of small accounts and sends a valuable signal to financial institutions that the authorities value their efforts to encourage financial inclusion. In many other countries, however, progress so far has been scant.

Unfortunately, no comparable progress has been made at the international level toward formally graduating KYC requirements for cross-border transactions. Limits for small transactions need not be uniform across countries, but differentiated limits could be set according to the conditions of the sending and receiving countries. The list of "high-risk and non-cooperative jurisdictions" maintained by the FATF could serve as a basis for these limits, with lower indicative limits for countries considered riskier.

Strengthening national identification systems

RECOMMENDATION 17. National identification systems must be strengthened, both to facilitate compliance with KYC rules for banks and DSPs and to support the effectiveness of the preceding recommendations as they apply to cross-border transactions.

To meet the standards needed for adequate KYC enforcement, government-issued ID systems must be robust enough to prevent individuals from setting up multiple accounts under different identities. Moreover, in principle, and for countries judged to have the

Box 4.3 Safaricom's tiered accounts for mobile money

In Kenya, Safaricom's M-Pesa (the money transfer service) and M-Shwari (a system of savings and credit accounts that operates exclusively through M-Pesa; see box 3.4) illustrate the application of the graduated account approach to mobile accounts. Each individual who opens an M-Pesa account must show a government-issued identity card and complete an application form that requires personal details such as name, ID number, and home address. Individuals wishing to receive more than 100,000 Kenyan shillings (Ksh) in a single year are required to provide a copy of their identity document in addition to the application form.

M-Pesa users are allowed to open M-Shwari accounts without any additional documentation or verification. Using an M-Shwari account, however, requires authentication of identity. For deposits up to Ksh250,000, identity is authenticated against the official government registry. This procedure can also help ensure against an individual opening more M-Pesa accounts than are permitted (two). For further deposits up to Ksh500,000, the depositor must go in person to a Safaricom shop and present the original and a copy of the identification document used. For amounts exceeding Ksh500,000, depositors must also present the original and a copy of the depositor's PIN (tax) certificate. Any movement of funds into or out of an M-Shwari account must pass through M-Pesa, where individuals would have previously undergone basic customer due diligence, as described above. In addition, M-Shwari transactions are subject to the M-Pesa maximum daily transaction limit of Ksh150,000 (di Castri 2013b).

Box 4.4 Technology-driven identification in India: Carrots versus sticks

Biometric identification technology is rapidly helping developing countries close the "identification gap" that separates them from richer countries. India recently launched an ambitious unique identification (UID) program, which aims to provide every resident with a unique, secure identification number, also known as an Aadhaar. The program, overseen by the Unique Identification Authority of India (UIDAI), has established a low-cost, ubiquitous authentication infrastructure to easily verify identities online and in real time. An Aadhaar is a 12-digit number that is stored in a centralized database and linked to the individual's basic biographic and biometric information: a photograph, a full set of fingerprints, iris scans, and, more recently, a digital faceprint.

Although participation in the Aadhaar scheme is voluntary, the massive effort has enrolled more than 900 million people. Enrollment is free. Although people have experienced some institutional pressure to enroll, Aadhaar seems to have been welcomed by many people in India who previously felt "unrecognized." The elimination of duplicate, ghost, and fake identities across India's multitudinous existing identification schemes will substantially improve the efficiency of delivery systems and help ensure that government benefits reach the intended beneficiaries. Financial inclusion also will be stimulated as subsidies start to be delivered through Aadhaar-linked bank accounts.

By enabling people to open restricted accounts subject to later showing proof of identity (see box 4.2), India is using financial access as a carrot that encourages registration rather than registration as a stick that constrains financial access. Until the Aadhaar numbers are seeded into criminal and security-related databases, however, Aadhaar cannot be used to check individuals against government lists in those areas.

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. Although still in its early stages, the Aadhaar ID system in India is a good example of a system capable of supporting the dual goal of promoting financial inclusion and satisfying a risk-based KYC approach (box 4.4).

Multilateral organizations can play two important roles in the effort toward strengthening systems of identification worldwide: first, by supporting national governments of developing countries in their efforts to improve their ID systems, and second, by working toward establishing global quality standards for identity 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 such as the World Bank and other multilateral development banks have begun to take a more systematic approach toward ID systems. Financial regulators should engage with that process.

Clarifying and graduating penalties

RECOMMENDATION 18. In keeping with the principle of proportionality, regulators must articulate what they regard as more and less serious failures of KYC processes and set rules and penalties accordingly. For small accounts and limited transactions, penalties should be set according to failures to comply with KYC requirements rather than on whether or how many infractions have taken place. Penalties should also be set on a graduated basis, increasing as the failure of compliance becomes more severe and regular.

In an undertaking as complex as KYC regulation of financial services, fully and explicitly laying out all the penalties for every imaginable violation of the rules is impossible. In addition, excessively onerous and costly KYC regulations on financial flows and ex post sanctions on their violation will tend to divert financial flows into less transparent channels, including cash, even though this increases costs and reduces convenience for legitimate users. Thus, if financial institutions are required to pursue KYC diligence up to the point at which the expected risk is zero, the objective of overall financial integrity may fail to be achieved. The need for regulatory predictability demands, however, 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, not on the basis of whether or how many violations have 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 the basis for penalties and the severity of the infraction. As just outlined for domestic transactions, penalties relating to small transactions should be graduated according to the seriousness of the failure to comply with mandated due diligence processes. Also, authorities could benefit from guidance from the FATF regarding the size of transactions considered small enough to pose minimal risk.

To assist in setting appropriately graduated KYC requirements and penalties, more quantitative research should explore the nature and extent of illicit transactions, both domestic and international, and whether conducted through the financial system or through other channels. Researchers should also investigate the trade-offs between different types and levels of regulations and penalties.

Encouraging international account-to-account transactions

RECOMMENDATION 19. Regulation should encourage a shift from cash-to-cash wire transfers toward direct international transactions between identified holders of bank accounts or e-money.

With the rapid spread of e-money and an increasing prevalence of digital money transmission, technology is already facilitating a shift from less transparent, cash-to-cash wire transfers and other mechanisms (such as *hawala* in the Middle East and elsewhere) toward direct, account-to-account transfers, whether to and from a bank account or an e-money account. Advances in that direction could reduce the cost of remittances and increase their transparency, thereby reducing KYC concerns. Especially because international remittances often are repeat transactions, this approach could include establishing notional "transmission accounts" with money transfer operators for otherwise unbanked customers. Those accounts would be subject to the same minimal KYC requirements as for restricted bank accounts or e-money accounts but would serve solely as vehicles for money transmission.

Some countries, such as Kenya, already have the necessary infrastructure in place to support account-to-account transactions and indeed have seen them become the dominant mode of international transfers. This recommendation would have to be implemented in parallel with initiatives to promote domestic financial inclusion, however, to avoid disruption to cross-border remittances. In the interim, the

suggested approach is to open up restricted accounts, such as those portrayed in box 4.2, to similarly restricted international transactions.

Recognizing the need for different approaches for difficult cases

RECOMMENDATION 20. In cases in which 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, or positive, list.

A positive list (in the present context, one that lists only those individuals and entities permitted to conduct transactions and that 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 that allows all others). Hence, a "safer corridor" system available only to those entities 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 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 creating a safer corridor is under exploration for Somalia (box 4.5).

Box 4.5 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, auditing sender and receiver identities, monitoring remittance amounts for abnormal activity, and scrutinizing 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 parties involved (Beechwood International 2013).

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 October 2014, the U.K. government began developing the U.K.–Somalia "Safer Corridor" Pilot (see Government of the United Kingdom 2015; and Makin, Clark, and Lonie 2015). Following extensive analyses and consultations, steps to help formalize the remittance sector in Somalia, giving banks in the UK greater confidence about the final destination of any money being sent through their channels, are being drawn up.

Chapter 5

Achieving financial inclusion in retail payments

The expansion of digital financial inclusion—and the realization of its benefits—depend on progress in further extending payment services. This section of the report can thus be seen as an application of the recommendations in the previous sections to a financial service that is crucial to financial inclusion. Progress in financial inclusion as it relates to payment services involves achieving ubiquity, convenience, and trust in those services. Ubiquity means that everyone in a country enjoys proximity, digital or physical, to the payment network. Convenience requires, besides ubiquity, ease of use and affordability for the consumer, yet in a manner that is sustainable for the provider. Trust requires adequate consumer protection and the mitigation of various risks—technological, financial, and legal—both to the individual user and to the financial system as a whole, achieved at reasonable cost to providers and users.[1]

As with other financial services, progress in fostering inclusion in payment services will depend on ensuring, through various policies, effective competition among payment service providers, a level playing field among the types of payment services, and adequate protection for consumers of the services, including through balanced know-your-customer (KYC) rules. (See sections 2, 3, and 4, respectively, for a broader discussion of each component.) More than for other services, however, the institutional framework of the payment system—its organization, infrastructure, and the laws and rules governing its use—matters greatly. This is so in large part because payment services and related (retail) clearing and settlement infrastructures involve crucial network externalities on both the demand and the supply sides: the value of these services to any given user or provider depends on the number of other users and providers participating in the network with whom they can transact. Given the scope for market failures, the public sector has an important role as a regulator and overseer to ensure that the market develops—but does not tend toward a natural monopoly—yet that safe and equitable access requirements are adopted and implemented. It is this institutional framework to which the recommendations here apply.

Countries differ greatly in many respects, the modalities for the provision of payment services are evolving rapidly, and regulatory interventions have to balance various public and private concerns. Each country's choice of framework will depend on, among other things, its policy goals and their prioritization; the existing supply-side structures and their capacity to play a beneficial role in financial inclusion and in the upgrading of payment service provision; concerns regarding the risks of undue market concentration, consumer abuse, and financial instability and the country's ability to handle risks; and institutional and legal constraints and the extent to which they allow or hinder experimentation.

Annex 2 discusses how some of these considerations affected the approaches that authorities in Australia, the European Union, and Kenya took in developing institutional frameworks for digital payment services and how those approaches changed over time. (A pattern somewhat similar to Kenya's was followed in the Philippines, which in 2004 saw the first successful mobile payment service in a developing country, with regulation adopted later; see Khan 2012.) These examples show that the optimal approach to building an institutional framework for a country's payment system that serves the objective of financial inclusion remains unclear, and the systems remain in flux in many countries around the world. Two points, however, are clear.

The first point is that payment services, like other financial services, will be provided in all countries by a variety of institutions, some of which (banks, for example) will engage exclusively in financial services whereas others (such as MNOs and other DSPs) maintain a significant presence in other sectors. The second point is that effective regulation of the market for payment services will involve all three of the key regulatory areas identified previously: adequate competition, a level playing field (identical regulation for identical services), and adequate KYC rules and consumer protection (the

1. These features of payment systems are closely related to the three key elements of financial inclusion (availability, affordability, and quality) discussed in section 1.

latter achieved in a way that balances these concerns and inclusion). Specific recommendations under each of those three headings follow.

Promoting effective competition

Effective competition in payment services requires more than the ability of new service providers, including DSPs, to enter the market and weak providers to exit. It also involves making sure that all providers have access to business critical inputs and networks, that pricing policies do not raise barriers against efficient provision, and that the markets for payment services display the right degree of interoperability, balancing the interests of those entities that want to enter (and who must recover their investment) with the need for a large enough market to gain economies of scale, given the inherent network externalities in payment services.

Access

RECOMMENDATION 21. In principle, regulation should not impose on payment services providers, users, or other network participants any of the following: rules that discriminate between authorized payment services providers as to the rights, obligations, and entitlements of participants; restrictions on the basis of institutional status; or restrictive rules for effective participation in other systems.

Rules for access to the payment system should generally be left to the system's managers because access rules are business matters, not matters of policy. The rules must be consistent, however, with a level playing field; they should be objective, nondiscriminatory, and proportionate to their aim; and they should not inhibit access to the system more than is necessary to safeguard against specific risks and to protect the system's financial and operational stability. Because of the network externalities and the overall importance of the payment system, regulators can have a legitimate role in determining which types of providers have access to it and under what conditions. In addition, circumstances may call for continued regulation and oversight with respect to specific concerns (for example, the use of robust technologies). Any such requirements are recommended primarily for the sake of efficiency and market competitiveness because inclusion, as such, is not directly linked to access criteria.

Pricing

RECOMMENDATION 22. As a general principle, and consistent with this report's general recommendations on competition, pricing of payment services can be left to the market. In some circumstances, however, interventions may be needed to ensure that pricing policies are in line with the provider's actual costs. Such interventions may include, for example, limits on interchange fees. Ensuring near-universal access may also require other types of interventions.

Charges for payment services arise for two distinct groups of participants: on one hand are the fees and other charges imposed on consumers for use of the service, and on the other hand are the interchange fees charged to merchants and other intermediaries for the use of payment systems (card switches, for example) and networks (ATM, POS, and mobile networks, for example). Interchange fees are only indirectly related to financial inclusion. For both groups, the pricing of these charges can almost always be left to the market to decide: in a competitive environment, payment service providers will have an incentive to keep prices low to expand their business and so maximize revenue. The main issue is to avoid collusion in the market and abuse of a dominant position because either can affect business choices adversely and foreclose new entry, thus reducing competition. In addition, prices to all participants must be kept transparent and as low as possible, to make products and services affordable in order to encourage the use of digital payment instruments.

Competition issues can arise, however, in terms of pricing and access, which raises questions about whether and how best to intervene. As noted in section 2, network externalities can lead to monopolistic or oligopolistic pricing of financial services and to other deviations from full competition, possibly requiring intervention. Among the possible responses are the setting or capping of various fees, such as fees for transactions that go off the network (box 5.1). In general, a graduated approach to such problems, stepping up the level of intervention incrementally if problems persist, is best.

Box 5.1 Application of pricing recommendations for treatment of mobile off-net fees

Off-network (off-net) transfers occur when the recipient of a money transfer is not registered with the mobile money network used by the sender. The recipient may be registered with another mobile money network or may not be registered with any network. Typically, fees charged for such off-network transfers are much higher than for equivalent on-network transfers (often, these are free).

An important issue is whether off-net fees should be capped through regulatory intervention. Important trade-offs are associated with this policy decision. On one hand, the lack of government interference in the conduct of business in this area (including the setting of all types of fees) supports increased supply of services and products by existing players. On the other hand, high off-net fees increase the costs to customers, deterring inclusion and encouraging inefficiency (for example, users may acquire multiple SIM cards and engage in inefficient cash-in, cash-out behavior to avoid paying the fees). The policy challenge, therefore, is to balance these and other costs and benefits in deciding when and to what extent to intervene in this and other pricing procedures.

An escalating approach is generally best, with some more specific recommendations, as follows:

- At the very least, reporting and monitoring of off-net fees is essential. Transparency and disclosure of all prices and fees charged to users must be mandated ex ante.
- Limits on off-net fees might have to be introduced ex post if they are identified as a major incentive to cash-in, cash-out behavior, which imposes costs on (the development of) the industry. Experience from mobile voice communications and data transfers shows that alternative ways to intervene exist, ranging from straight caps to milder interventions, without specifying the level. Rules may also be necessary to ensure equal treatment irrespective of the form of payment (for example, to ensure that cash is treated the same as digital money).
- Before resorting to regulatory intervention, however, authorities must determine whether market solutions can, by themselves, lower or eliminate off-net fees. In Tanzania, achieving interoperability between two MNOs brought about the removal of off-net fees. Direct regulatory setting or capping of prices, including interchange fees, should therefore be a last resort.

Pricing policies should also be in line with the actual cost of providing the service, however, to avoid unsustainable provision. Unbanked populations often are too poor to afford high fees, and typically their transactions are of low monetary value. Also, many of the unbanked reside in remote areas, making delivery of services to them more costly. As a result, payment services for those populations may well be unprofitable unless either they are subsidized in some way or the providers can cover their costs by other means (for example, through higher fees for other customers or through sales of other services to the same customers). To achieve near-universal service in remote areas, where service may be uneconomic, the regulator might have to set more articulated competition and pricing policies (such as allowing for tiered pricing, in which large-value transactions or richer customers pay more, thus subsidizing service provision for the poor), permit mechanisms for recovery of costs (such as a general fee imposed on all customers that pays for specific services), or offer incentives to provide service, such as up-front, time-bound startup subsidies. Such mechanisms can draw on experience with policies adopted in other network industries with universal or near-universal service obligations, such as electricity, mail, and water.

Interoperability

RECOMMENDATION 23. Consistent with recommendations in section 2, regulatory intervention to ensure interoperability of payment systems should be undertaken mostly ex post—and then only when necessary. If intervention is required, regulators should be mindful not to mandate interoperability of payment systems either too early or too late; the former can dampen innovation and market development, whereas the latter can allow one or more dominant players to accumulate too much market power.

Interoperability of payment systems and networks is a cornerstone of financial inclusion because it ensures that the ability to transfer funds does not depend on a single communications network or service provider, which would impair competition and affect consumers' experience. Also, interoperability enables providers to more easily use different access devices at the same entry point and process different payment instruments within the same platform. Furthermore, network interoperability serves to limit duplicative investments and thus can lead to greater financial sustainability for the most competitive networks—that is, those that provide the best services.

Interoperability of the payment system is not an all-or-nothing proposition. Rather, it can be achieved at different levels of the payment chain at different times. As a consequence, the real issue is not whether interoperability in general is desirable but rather to what extent and at what level it is appropriate and possible at a given time. In deciding those matters, the need for financial inclusion and efficiency must be balanced against proprietary rights on technology and intellectual property and against the need for protection of new entrants from undue risk, both of which will encourage new development and competition for the market.

Leveling the playing field

A level playing field is as important a principle for payment services as for other financial services. It requires action at various levels: at the level of the merchant offering various types of POS services and at the levels of the institutional infrastructures needed to deliver the payment services and settle the payments.

Payment options

RECOMMENDATION 24. Merchants should be free to choose which payment channel or channels they will use, but they should be discouraged from signing exclusivity arrangements. Customers should not be forced to use, or to pay more for, one means of payment when more than one are available. Regulation should be technology neutral, and standards should be based on functionality.

Competition among payment services is most likely to prevail when merchants can choose the channel or channels they will accept for payment—cash, checks, debit cards, store-of-value cards, or Internet or other platform-based products. Merchants should be discouraged, however—and possibly in some circumstances even prevented—from signing agreements that limit their use of payment services (or acceptance devices) to a single provider. Besides locking merchants in at a time when technology and new forms of financial service provision are rapidly changing, such exclusivity agreements limit competition in the payment services market.

For merchants that accept multiple payment channels, including cash, the general policy should be that the customer should be free to choose among them, without regard to whether one costs the merchant more than another. Whether a merchant should be permitted to offer a discount (or impose a surcharge) for the use of a specific instrument—as a way of encouraging or discouraging its use over others—is controversial. In the European Union, for example, surcharges have not been prohibited as a general rule, but caps have been set on interchange fees for card-based transactions as a way of limiting such practices. Elsewhere (for example, in some U.S. states) such prohibitions against differentiation exist, but the benefits, if any, to users are not clear.

Finally, regulators should use a technology-neutral approach to the treatment of different payment instruments. They should base their regulatory standards on the functions executed and the risks connected with them, not on which specific technology is used. They should avoid allowing regulation to be driven by or biased toward the needs of any specific technology or technologies. For instance, electronic payment instruments should all be regulated as a whole, rather than mobile payment services only, given their many common features. And to limit regulatory arbitrage and enforce a level playing field, regulators should avoid a piecemeal approach.

Clearing and settlement infrastructures

RECOMMENDATION 25. The operation of infrastructures for the processing, clearing, and settlement of payments is best left to the market, with retail payment instruments fully integrated. As a general principle, the public sector should be involved only as a regulator of infrastructure but, in exceptional cases, could serve as an operator of the infrastructure.

Choices about how to process, clear, and settle payments are best left primarily to the market. Such choices will contribute to shaping the national infrastructure for clearing and settlement, however, and thus should be subject to general policies in this respect (see Committee on Payments and Market Infrastructures and the World Bank Group 2015). Retail payments should be fully integrated into the national payment system so that users can use any instrument they wish (provided it is potentially interoperable), knowing that it is fully secure from clearing and settlement perspectives. With current technology, most digital transactions are executed in real time, and this is indeed highly recommended. It does not necessarily mean, however, that the transactions are also settled in real time within the payments system, between the entities (banks or DSPs) that hold the payer's and the payee's transaction accounts. Whether to settle transactions on a net (batched) basis or on a real-time basis is at the discretion of the individual service provider, whose choice may depend on the volume and average size of the transactions.

A clear public interest exists in having a country's real-time gross settlement system run by the central bank because that system also is important for monetary policy and therefore for the stability of the entire financial system. Such motivations are less likely to exist for retail payments, however, and thus those systems are more likely to be run by the private sector.[2] If, nevertheless, the central bank or a government agency is involved in operating a retail payment system, it should do its utmost to cooperate with the private sector. When the market is unwilling or unready to build the relevant infrastructure, the public sector (usually the central bank) may be able build it, preferably in cooperation with the private sector.[3] When that occurs, what also often happens (and is indeed preferable) is that at a further stage, the central bank privatizes the system. Regardless, the payments system must be reviewed on an ongoing basis—as to its safety and reliability—and enhanced as necessary.

Ensuring consumer protection and KYC

RECOMMENDATION 26. A solid institutional framework requires disclosure of fees charged—in ways that make them easily comparable across providers and products—and the provision of adequate customer recourse and dispute resolution mechanisms. The objective of financial system integrity should be balanced with that of not unnecessarily hindering access to payment services.

Competition, self-regulation, and reputational mechanisms can provide strong incentives for private sector institutions involved in payment services to ensure an adequate degree of consumer protection, but government regulation also has a role. The capacities of local supervisory and competition agencies should be taken into consideration, as well. Analysis of those capacities may reveal a need for further support and training of staff (abroad, if necessary) and for greater reliance on private forms of monitoring and enforcement of consumer protection rules, including through consumer charters.

KYC requirements should be proportional to the risk, as recommended by the Global Partnership for Financial Inclusion. Regulators can adopt less burdensome standards for low-value payment services, for example, such as adjusted KYC procedures and lower capital requirements for small store-of-value products, along with less strict oversight.

2. Some countries consider their system of clearing for card transactions important for systemic financial stability. In such cases, more oversight would be warranted.

3. Another argument for the government to play a role is that the government sector is likely to be a large-volume, recurrent payer. Payments in which it is involved include government collections (taxes) and payments to contractors, utility and transit fares, payrolls, remittances, social services, welfare, and other kinds of payments processed in bulk. Using the formal payment system for those purposes can not only save costs but also increase the usefulness to consumers of having transaction accounts, thus promoting more widespread adoption of such accounts.

Annex 1

Three main principles for pro-inclusive regulation

Three fundamental principles underlie the approach to regulation for financial inclusion advocated in this report: regulating by function, regulating by degree of risk, and balancing ex ante and ex post regulation. This annex expands on these principles.

Regulating by function

With the influx of new providers and the development of new business models, the conventional mappings between financial products and services and different types of institutions are becoming increasingly blurred. The way for regulators to deal with this protean environment is to regulate by function rather than by type of institution. Such an approach seems appropriate not only to the broader task of regulating financial services effectively but also to promoting the goal of financial inclusion.

Regulating by function can serve a dual purpose: that of leveling the playing field across alternative providers and that of reducing uncertainties regarding the nature of the regulatory framework that might apply to new players. Consider, for example, the hotly debated issue of regulation and supervision for e-money issued by MNOs and other DSPs. The view taken in this report follows straightforwardly from the principle of regulation by function: as long as DSPs limit their provision of financial services to small transactions in payments, remittances, and transfers, with limited intraday exposure—that is, as long as they do not offer a substantial and long-lasting store of value—they should not be subject to bank-type regulation and supervision. (They may—indeed, should—be subject to typical oversight of payment services and to typical consumer protection regulations, however.) If instead these DSPs offer what may properly be called store-of-value instruments, then they should be required to either accept limits on their activities, including their investments, or be subject to regulation and supervision and possibly have insurance (with associated other conditions and allowing for choice among various insurance modalities).

Regulating by degree of risk

Regulation according to risk of the financial services provider is already a fundamental principle of the modern approach to financial regulation. The various capital and liquidity requirements, capital surcharges, and other regulations recommended for banks by the Basel Committee on Banking Supervision are based on this principle (see BCBS 2010). The committee's recommendations were advanced to enhance the stability of commercial banks and the financial system, but the objective of improved financial inclusion requires a similar risk-based approach. Current national legislation on financial regulation in many countries, however, omits (and sometimes even contradicts) any notion of risk-based regulation as a means toward greater financial inclusion. One important reason is that the concept of promoting financial inclusion is itself relatively new in many countries and still nonexistent in a few. Another reason is that, unlike in the case of regulation aimed at financial stability, regulators have not yet accumulated sufficient experience in dealing with the potential trade-offs and unintended consequences that can result from enacting regulations aimed at improving financial inclusion, especially through new types of financial service providers.

This report maintains that a risk-based approach should guide all aspects of the regulatory framework for financial inclusion: the riskier the financial service provider is to the user or the whole financial system, or the more the user is potentially at risk of loss of funds or of fraud, abuse, misuse, or being sold an inappropriate product, the higher should be the regulatory bar. Rules to implement this approach can include the licensing of providers who are allowed to offer certain financial products; capital or liquidity requirements (or both) and other limitations on some providers; and consumer protection rules and KYC regulations, among others, for specific financial products. Regulation today in many countries, especially regarding KYC rules, fails to incorporate a sufficiently risk-based approach, whether in terms of international standards or in terms

of local regulation. The good news is that a number of countries are achieving progress.

Balancing ex ante and ex post regulation

Regulation of the financial system differs significantly from that imposed on most other economic sectors in one important respect: Banks and other traditional providers of financial services are subject to regulations that are well defined on an ex ante basis. Regulations governing the activities of most other industries (except health care) more typically follow an ex post approach.

Ex ante regulation refers to rules that set prerequisites on providers as a condition for their being allowed to participate in a market. This type of regulation starts from the assumption that, left on its own, the market will not generate safe and efficient outcomes and that participation therefore must be regulated. Ex ante regulation is predominant in the financial sector because of the many market failures to which it is subject, in part because of the extensive interconnections between players. For example, capital requirements are placed on banks as a means of avoiding moral hazard—that is, of preventing them from taking excessive risks, with the expectation that the government will bail them out should they fail.

Ex post regulation, in contrast, refers to regulatory intervention that occurs only after a problem or market failure has been identified (usually following a formal investigation). This regulatory approach typically is adopted in industries other than financial services, to ensure appropriate market conduct and, especially, to avoid anticompetitive behavior by dominant market players.

Because the provision of digital financial services involves the participation of both the financial services industry and an important nonfinancial industry—the telecommunications industry—designing an appropriate mix of ex ante and ex post regulation for digital services is a difficult challenge. The view taken in this report is that the mix will depend on the service provided. For example, as emphasized previously, payments and transfer services provided by MNOs and other nonbank DSPs generally pose limited risks to the financial system and therefore can be subject to lighter ex ante regulation. This approach will best serve the efficient development of the market, as excessive ex ante regulation would inhibit innovation and the development of new products and markets. However, because the possibility remains that the market will develop in undesirable ways (for example, with the emergence of a dominant player), the option of imposing tough ex post regulatory intervention must be preserved. As the market evolves to provide services beyond payments, and as the activities of DSPs converge toward those of banks, more ex ante regulation that is consistent with the principles of regulating by function and on the basis of risk will be necessary.

The right balance of ex ante and ex post regulations will also depend on each country's circumstances. For example, countries whose financial systems are well developed, with good institutional environments, and countries with very poorly developed financial systems may both operate best under a more laissez-faire model for digital financial services, but for different reasons. In the former, financial stability concerns may be less paramount, allowing for greater experimentation, whereas in the latter, the potential gains from financial inclusion are greater, making the emergence of new models attractive. In the Philippines and in Kenya, for example, the delay in issuing regulations was arguably important in allowing market innovation to develop and regulators to base regulations on the actual risks revealed through market dynamics rather than on ex ante suppositions.

Annex 2

Examples of approaches to defining payments services: European Union, Australia, and Kenya

Ex ante and ex post regulation of e-money in the European Union

The first version of the E-Money Directive, adopted by the European Union in 2000, exemplifies the ex ante approach to prudential regulation of payment services. In hindsight, this measure turned out to be a barrier to innovation by setting overly strict regulatory hurdles. Consequently, the directive was revised in 2007 (and to be transposed into national legislation by all EU and EEA member states by 1 November 2009 at the latest) to set less stringent requirements.[1]

One of the declared aims of the 2000 directive was to regulate the newly emerging e-money services so as to prevent a lack of legal certainty from hampering innovation. That directive, however, not only regulated e-money products as such but also specified which kinds of entities could offer them. It also established prudential requirements for so-called electronic money institutions (EMIs), which are entities offering payment products that store value not in a bank account but somewhere in a software program or electronic device.

When the European Commission assessed the application of the 2000 directive in 2005, it found that certain of the directive's restrictions and requirements—and, in some cases, their national implementation and interpretation—had slowed the development of the e-money market and kept it from reaching its full potential (The Evaluation Partnership 2006). In addition, legal uncertainty as to the applicability of the directive to certain business models had restrained the development of certain products. Accordingly, the rules were subsequently revised.

Two important developments had occurred in the meantime. First, certain newly launched products clearly did not create stores of value, but they still involved financial services that required regulation. A new payment services directive was therefore adopted in 2007, covering a wider spectrum of services and imposing lower prudential requirements on what were called "payment institutions" (PIs). The directive also allowed the creation of "payment accounts" by a PI, which differ from standard bank accounts in that they may be used only for executing payments and may keep money on deposit for only a limited time. Second, the 2000 E-Money Directive had never really worked for EMIs, in large part because its prudential requirements were disproportionate to the actual scope of their activities. These requirements had been derived from those of credit institutions, which provide a much wider range of services, including services of higher risk.

Those considerations led in 2009 to a new E-Money Directive[2] that imposed regulatory requirements closer to those for PIs under the 2007 directive. Both directives will soon again be revised, and their combined application should reveal whether the revised approach has indeed produced better results.

Australia's approach to regulation of payment services and fees

In 1998, Australia passed the Payment Systems (Regulation) Act for the regulation of payment systems and purchased payment facilities, and for related purposes. The act defines the payments system broadly as any fund transfer system that facilitates the circulation of money (thus including retail systems), and it covers "any instruments

1. Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC". Official Journal of the European Union. 5 December 2007.

2. Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC.

and procedures that relate to the system" (Australian Government, 1998, Part 2, page 3)

Under that broad definition, the Reserve Bank of Australia (RBA) is empowered to regulate all card-based and other schemes for the processing of transfers. In addition, because "purchased payment facilities" (a term that includes store-of-value products) are regulated under the same official powers as payment systems, the RBA has the authority to authorize each facility individually and impose specific conditions. The act permits deposit-taking institutions and any other entities authorized by the RBA for that purpose to offer these products, and for the "any other entities" group, the RBA may decide on a case-by-case basis whether to grant such authorization.

Access to the provision of innovative retail instruments is thus regulated by the RBA under its general policy on retail payments. That policy is subject to a general criterion of public interest, whereby the RBA judges whether a product or service is financially safe for use by participants, efficient, and competitive and does not materially cause or contribute to increased risk to the financial system. Efficiency and stability are, however, not the only possible concerns, because the act permits the RBA to "have regard to other matters that it considers are relevant." Although financial inclusion concerns are not mentioned explicitly, the RBA could impose specific requirements deriving from those concerns, at least as far as they can be connected to efficiency concerns.

Developments in payment system regulation in Kenya

At its inception in 2007, Safaricom's M-Pesa was launched using a trust account at the Commercial Bank of Africa (CBA), into which the net balance of many small accounts that were operated via phone were consolidated (today, M-Pesa's funds are held as trust accounts in several commercial banks—see box 3.2). Although the trust account met the requirements of the country's trust law; although the account was, as a bank product, subject to regulation and supervision by the central bank; and although Safaricom and its agents were licensed, regulated, and supervised by the Communications Commission of Kenya (CCK), the mobile payment scheme nevertheless started without any specific license or authorization for the service. It also was not designated as a specific new service later under a different mechanism, such as those sometimes found in countries where payment instruments are regulated separately from banking services. Other such services later followed. The existing trust law, the banking act, and other laws sufficed to allow for regulation and supervision, and the central bank and the CCK agreed to share information as regulators.

Within just a few years, M-Pesa had achieved high market penetration, with no sign of risk to users or to the financial system as a whole. Whether the lack of specific ex ante regulations contributed to that success, or whether a more stringent regulatory regime would have greatly hampered M-Pesa's performance remains unsettled, however. Its success also did not dispel concerns about the potential distortions and risks from its operation. Already at M-Pesa's inception, the banking sector had claimed regulatory discrimination because M-Pesa was not subject to the same regulatory burden imposed on bank-provided payment services and, unlike banks, was permitted to use agents for cash-in, cash-out transactions. At about the same time, Zain, a competing MNO that was launching a new mobile product, complained about Safaricom's dominant position (Alliance for Financial Inclusion 2010).

In that context, in 2011, a National Payment System Act was adopted, which was then implemented through regulation in 2013. Accordingly, in June 2014, the central bank issued guidelines for authorization of payment service providers. Nonbanks that provide payment instruments are, as a consequence, no longer only indirectly regulated. The Kenya Bankers Association has also proposed that deposit insurance coverage be passed through to mobile money account holders, subject to rules on the fiduciary being an insured depository institution, on sufficient records being kept to identify the beneficial owners of the funds and their entitlements, and on the deposit and related information being kept available for inspection either at the bank or with the trustee or some other party (such as the MNO providing the service).

References

Alliance for Financial Inclusion. 2010. *Case Study: Enabling Mobile Money Transfer: The Central Bank of Kenya's Treatment of M-Pesa*. Bangkok.

Australian Government. 1998. Payment Systems (Regulation) Act 1998, as amended as of 2011. https://www.comlaw.gov.au/Details/C2011C00182.

Bank of Uganda. 2013. "Mobile Money Guidelines, 2013." Bank of Uganda, Kampala. ucc.co.ug/files/downloads/Mobile-Money-Guidelines-2013.pdf.

BCBS (Basel Committee on Banking Supervision). 2010. *Basel III: A Global Regulatory Framework for More Resilient Banks and Banking Systems*. Bank for International Settlements, Basel.

———. 2013. *Basel III: The Liquidity Coverage Ratio and Liquidity Risk Monitoring Tools*. Bank for International Settlements, Basel.

Beechwood International. 2013. *Safer Corridors Rapid Assessment: Case Study: Somalia and UK Banking*. HM Government and Beechwood International, London.

Bourreau, Marc, and Tommaso Valletti. 2015. "Enabling Digital Financial Inclusion through Improvements in Competition and Interoperability: What Works and What Doesn't?" CGD Policy Paper No. 065. Center for Global Development, Washington, DC.

Brookings Institution. 2015. *The 2015 Brookings Financial and Digital Inclusion Project (FDIP) Report*. Washington, DC.

CGD (Center for Global Development). 2015. "Unintended Consequences of Anti–Money Laundering Policies for Poor Countries." CGD Working Group Report. Washington, DC.

Claessens, Stijn, Patrick Honohan, and Liliana Rojas-Suarez. 2009. *Policy Principles for Expanding Financial Access: Report of the CGD Task Force on Access to Financial Services*. Center for Global Development, Washington, DC.

Cook, Tamara, and Claudia McKay. 2015a. "How M-Shwari Works: The Story So Far." Consultative Group to Assist the Poor (CGAP) and Financial Sector Deepening (FSD), Washington, DC.

———. 2015b. "Top 10 Things to Know About M-Shwari." Consultative Group to Assist the Poor, Washington, DC.

CPMI (Committee on Payments and Market Infrastructures) and the World Bank Group. 2015. *Consultative Report: Payment Aspects of Financial Inclusion*. Bank for International Settlements, Basel, and World Bank Group, Washington, DC.

Demirgüç-Kunt, Asli, and Leora Klapper. 2013. "Measuring Financial Inclusion: Explaining Variation in Use of Financial Services across and within Countries." *Brookings Papers on Economic Activity* 46 (Spring): 279–321.

Demirgüç-Kunt, Asli, Leora Klapper, Dorothe Singer, and Peter Van Oudheusden. 2015. "The Global Findex Database 2014: Measuring Financial Inclusion around the World." Policy Research Working Paper 7255, World Bank, Washington, DC.

di Castri, Simone. 2013a. "Mobile Money: Enabling Regulatory Solutions." GSMA (Groupe Speciale Mobile Association), London.

———. 2013b. "Tiered Risk-Based KYC: M-Shwari Successful Customer Due Diligence." GSMA (Groupe Speciale Mobile Association), London.

The Evaluation Partnership. 2006. "Evaluation of the E-Money Directive (2000/46/EC): Final Report." Report for the DG Internal Market and the European Commission, Middlesex, UK.

FDIC (Federal Deposit Insurance Corporation). 2008. "Stored Value Cards and Other Nontraditional Access Mechanisms, New General Counsel's Opinion No. 8." Financial Institution Letter FIL-129–2008. Washington, DC.

GPFI (Global Partnership for Financial Inclusion). 2011. "G20 Principles for Innovative Financial Inclusion." Alliance for Financial Inclusion, Bangkok.

———. 2014. 2nd GPFI Conference on Standard-Setting Bodies and Financial Inclusion, Session 4: Deposit Insurance and

Digital Transactional Platforms—A Frontier Issue. http://www.gpfi.org/sites/default/files/documents/Session%204_Deposit%20Insurance%20and%20digital%20transactional%20platforms.pdf.

Government of the United Kingdom. 2015. "UK–Somalia Safer Corridor Initiative—October 2015." London. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/471064/UK-Somalia_Safer_Corridor_Initiative.pdf.

GSMA (Groupe Speciale Mobile Association). 2013. "The Mandatory Registration of Prepaid SIM Card Users." White paper. London.

———. 2014. *2014 State of the Industry: Mobile Financial Services for the Unbanked*. London.

Hanouch, Michel, and Gregory Chen. 2015. "Promoting Competition in Mobile Payments: The Role of USSD." Consultative Group to Assist the Poor, Washington, DC.

Helix Institute of Digital Finance. 2013. "Agent Network Accelerator Survey: Kenya Country Report 2013." Nairobi.

Khan, H. R. 2012. "Financial Inclusion and Payment Systems—Recent Trends, Current Challenges and Emerging Issues." Bank for International Settlements, Basel.

KPMG International. 2014. "Global Anti–Money Laundering Survey 2014." Amsterdam.

Kumar, Kabir, and Michael Tarazi. 2012. "Interoperability in Branchless Banking and Mobile Money." Consultative Group to Assist the Poor, Washington, DC.

Makin, Paul, Dick Clark, and Susie Lonie. 2015. "Executive Summary: Detailed Recommendations to Reduce and Manage Risk at the 'Last Mile' of the UK-Somalia Safer Corridor Pilot." Consult Hyperion, Guildford, U.K.; and FSD Africa, Nairobi.

Queen Maxima of the Netherlands. 2015. "Speech by Her Majesty Queen Máxima of the Netherlands, United Nations Secretary General's Special Advocate for Inclusive Finance for Development (UNSGSA), at the All Governors' Meeting." Bank for International Settlements, 9 November, Basel, Switzerland.

Radcliffe, Daniel, and Rodger Voorhies. 2012. "A Digital Pathway to Financial Inclusion." Bill & Melinda Gates Foundation, Seattle. http://ssrn.com/abstract=2186926.

Reserve Bank of India. 2014. *Guidelines for Licensing of Payment Banks*. Reserve Bank of India, Mumbai. https://rbi.org.in/scripts/bs_viewcontent.aspx?Id=2900.

Tellez, Camilo, and Peter Zetterli. 2014. *The Emerging Global Landscape of Mobile Microfinance*, Washington, DC: Consultative Group to Assist the Poor.

Winiecki, Jacob, and Kabir Kumar. 2014. "Access to Energy via Digital Finance: Overview of Models and Prospects for Innovation." Consultative Group to Assist the Poor, Washington, DC.

World Bank. 2001. "Principles and Guidelines for Effective Insolvency and Creditor Rights Systems." Washington, DC.

———. 2008. *Finance for All? Policies and Pitfalls in Expanding Access*. World Bank Policy Research Report. Washington, DC.

———. 2012a. "Developing a Comprehensive National Retail Payments Strategy: Consultative Report." Washington, DC.

———. 2012b. "Good Practices for Financial Consumer Protection." Washington, DC.

———. 2014. *Global Financial Development Report 2014: Financial Inclusion*. Washington, DC.

———. 2015. *The Little Data Book on Financial Inclusion*. Washington, DC.

For an electronic version of this book, visit
www.cgdev.org

ISBN 978-1-933286-96-9