CGAP

FOCUS NOTE

Basic Regulatory Enablers for Digital Financial Services

No. 109
May 2018

Stefan Staschen
and
Patrick Meagher

Executive Summary

Digital financial services (DFS) differ from traditional financial services in several ways that have major implications for regulators. The technology enables new operating models that involve a wider range of actors in the chain of financial services, from design to delivery. The advent of DFS ushers in new providers such as nonbank e-money issuers (EMIs), creates a key role for agents in serving clients, and reaches customers who have otherwise been excluded or underserved. This in turn brings new risks and new ways to mitigate them.

For many years now, CGAP has been interested in understanding how these new models are regulated, and how regulation might have to adapt to enable DFS models that have potential to advance financial inclusion. This Focus Note takes a close look at four building blocks in regulation, which we call *basic regulatory enablers*, and how they have been implemented in practice. Each of the enablers addresses a specific aspect of creating an enabling and safe regulatory framework for DFS. Our focus is on DFS models that specifically target excluded and underserved market segments. We analyze the frameworks adopted by 10 countries in Africa and Asia where CGAP has focused its in-country work on supporting a market systems approach to DFS.

The four basic enablers are as follows:

1. **Nonbank E-Money Issuance.** A basic requirement is to create a specialized licensing window for nonbank DFS providers—EMIs—to issue e-money accounts (also called prepaid or stored-value accounts) without being subject to the full range of prudential rules applicable to commercial banks and without being permitted to intermediate funds.
2. **Use of Agents.** DFS providers—both banks and nonbanks—are permitted to use third-party agents such as retail shops to provide customers access to their services.
3. **Risk-Based Customer Due Diligence (CDD).** A proportionate anti-money laundering framework is adopted, allowing simplified CDD for lower-risk accounts and transactions. The latter may include opening and using e-money accounts and conducting over-the-counter (OTC) transactions with DFS providers.
4. **Consumer Protection.** Consumer protection rules are tailored to the full range of DFS providers and products—providing a necessary margin of safety and confidence.

Why the focus on these four elements? They arise consistently in CGAP's experience working on DFS frameworks, and their importance underscored in research and policy discussions. There is wide agreement that the four enablers are necessary (though not sufficient) conditions for DFS to flourish. This is not to deny that DFS has emerged in some markets where one or more of the enablers are weak or missing. It is also not to say that in certain cases other enablers such as healthy competition or interoperability might be equally important. But experience strongly suggests that, in any given market, DFS is far more likely to grow responsibly and sustainably and achieve its full potential when all four elements are in place. (Empirical research confirms some of these correlations.)

Through our research, we aim to understand how a range of countries has addressed the four enablers in their regulatory frameworks and to see what lessons can be learned from their experience. The countries covered are Kenya, Rwanda, Tanzania, and Uganda in East Africa; Côte d'Ivoire and Ghana in West Africa; Bangladesh, India, and Pakistan in East Asia; and Myanmar in Southeast Asia.

Nonbank e-money issuance

E-money accounts and their issuers use different names across the world, but the basic concept is often very similar. The first element in enabling nonbank e-money issuance is to incorporate the concept of e-money in the regulatory framework. E-money combines several functions such as facilitating payments and storing value electronically. A workable definition must squarely address these payment and deposit-like aspects.

The second element is allowing nonbanks to issue e-money. This opens the DFS market to new providers such as mobile network operators (MNOs) and specialized payment services providers (PSPs), which are often more successful in reaching the mass market than are traditional banks. This step also brings such nonbanks (or their subsidiaries) under the authority of the financial services regulator—often the central bank. However, in some of the 10 countries studied, only banks may issue e-money. Typically, commercial banks are not the most efficient providers because of their high costs, which are partly attributable to heavy prudential and operational regulations. Nor is it recommended to permit all PSPs licensed under general payment regulations to issue stored-value accounts. E-money requires specific rules to protect funds collected from clients for future use. There is an essential difference in the risk profiles of pure fund transfers versus stored-value accounts. But banks and PSPs *may* become issuers if the regulations are sufficiently nuanced to afford proportionate safeguards and a level playing field.

The third element is to delimit the range of permitted activities for EMIs. In general, EMIs may carry out core functions such as issuing e-money accounts, cash-in, cash-out, and domestic payments and transfers—but not financial intermediation (except, in a few countries, limited investments in government securities).

The fourth element of the regulatory framework is to address the handling of customer funds converted into e-money (i.e., e-float), in the absence of a license to intermediate depositary funds. Rules in the countries studied require the e-float to be kept in safe, liquid assets. Regulations usually include standards that specify protection of the float funds through some combination of diversification, isolation and/or ring-fencing (from claims on the issuer), and safeguarding (from claims on the institution holding float deposits).

Use of agents

The viability of DFS depends on providers' ability to outsource functions to agents—thereby extending their reach and capturing efficiencies. But this also heightens risks unless some key safeguards are put in place.

One such safeguard has to do with relationships between providers and their agents. Allocation of legal responsibility is considered essential so as not to overburden the regulator with directly supervising a huge number of agents. DFS regulations in the countries studied make the principal (the DFS provider) liable for its agents' actions within the scope of delegated responsibility (expressed or implied). In most cases, however, the regulations do not solely rely on this liability provision and set criteria for the form and content of the agency agreement. They also specify certain due diligence and risk management steps, such as requiring the principal to have appropriate internal controls and agent monitoring systems and to carry out *ex ante* and ongoing (or periodic) assessment of an agent's risks.

Another issue of concern to regulators is the eligibility of agents—that is, who can become an agent (or a certain type of agent). Most countries require all agents to be registered businesses, although this is not always followed in practice because it unduly restricts the number of potential agent locations. A few

countries allow individuals to serve as agents if they are educated, or if they have experience or businesses considered relevant. An issue related to competition, but also one that impacts outreach of agent networks, is whether agents can operate on behalf of multiple providers. Most of the countries studied prohibit exclusivity clauses in agency agreements that would bind an agent to a sole principal.

Agent regulations also deal with the ongoing obligations of both agents and principals, and the security and reporting standards. Security and accuracy of client transactions and the reliability of the technologies involved are commonly addressed in agent regulations. Providing confirmation of transactions to the client is mandatory. Many countries prohibit agent transactions going forward where there is a communication failure.

Regulatory frameworks take different approaches. The treatment of agents depends sometimes on the category of institution represented by the agent (e.g., bank or nonbank), sometimes on the type of account being handled (e.g., e-money or bank deposits), and sometimes on the activities performed by the agent (e.g., account opening or cash handling). Each approach raises distinct challenges in making regulation effective.

Risk-based customer due diligence

DFS operate within regulatory contexts shaped by policies on anti-money laundering and countering the financing of terrorism (AML/CFT). The challenge for financial inclusion is to ensure proportionate treatment using risk-based frameworks that protect the integrity of the system while imposing the least burden on DFS outreach. In discussing customer due diligence (CDD) standards adopted in the countries studied, we consider how effectively they implement Financial Action Task Force (FATF) guidance prescribing the use of simplified procedures in lower-risk scenarios. (Often the regulations refer only to the identification [ID] component of CDD, i.e., know your customer [KYC].)

A common approach is the definition of risk tiers to which CDD procedures of varying intensity are applied. CDD rules typically focus on risks as determined by the features of the accounts or transactions provided, the types of clients, and the modalities of account opening and transacting (e.g., in-person or not). Most of the countries studied define two or three tiers (e.g., high, medium, and low risk).

A major contextual factor in CDD/KYC is the development of national ID documentation and verification systems. Limited availability of official ID documents has constrained financial services outreach, and therefore—in line with FATF guidelines—policies have been adopted to adjust ID requirements on a risk basis. Parallel to this trend of increasing the range of accepted identification methods is an unrelated trend of increasing government investment in universal provision of ID equipped with biometric technology. The benefits of advances in ID systems may obviate the need to accept a broad range of identity documents, but not necessarily the need for tiered account structures. The latter are still required because of other components of CDD.

Consumer protection

Digital channels and the use of agents pose special customer risks because of the potential for communication failure, identity theft, lack of price transparency and access to recourse by the client, and fraud. Ensuring that DFS have the necessary reliability and public trust to become a pillar of inclusive finance means establishing effective consumer protection. Regardless of whether it must be fully in place before DFS can spread, such protection is a necessary part of ensuring a sustainable market with long-term benefits to financial inclusion. In practice, however, the rules in this area are often unclear and incomplete.

The piecemeal extension of consumer protections into specific domains of DFS and DFS providers has tended to create a patchwork of regulation.

Transparency and fair dealing are core components of financial consumer protection (FCP) in DFS as in other areas. DFS providers are required to disclose fees, commissions, and any other costs to clients. Product information is to be posted at all service points and made available electronically. However, few of the 10 countries studied stipulate a standard disclosure format. The regulations usually mandate a written contract (which may be electronic), and sometimes impose a duty on the provider to explain key terms and conditions to the client before contract signing. Also, there are often fairness standards that require or prohibit certain contractual provisions.

It is a cornerstone of accountability to customers and regulators, and thus a tenet of good practice, to require each provider to set up a system for handling customer complaints. The countries studied incorporate this principle into regulation and apply it in some form to DFS providers. Well-developed frameworks address issues such as facilitating access to the system and tracking complaints, response deadlines, and appeals.

Along with issues common to all financial services, DFS consumer protection must also deal with the special risks of electronic transactions. Thus, a majority of the 10 countries impose some standard of service availability and/or digital platform reliability. Beyond this, regulation must balance the need for certainty of execution—nonrepudiation—against the need to allow for correcting mistaken or unauthorized transactions. The regulations may impose a general duty to inform customers of the need to protect ID and password information and the risks of mistaken transactions, or to specify how and under what conditions customers may demand revocation.

Lessons of experience

Some broad insights arise from the study. The experience of the African countries among the 10 countries shows the importance of EMIs—the first enabler. But this needs to be seen in light of a case such as India, where issuers (of what equates to e-money) are limited-purpose banks (called payments banks) that are subject to lower prudential requirements. Such an approach is certainly preferred to an approach where only commercial banks can issue e-money. The second enabler, the use of agents, seems to be the most consistently observed in practice. The liability of the principal for its agents' actions is a key provision that allows the regulator to focus its attention on the principal. In most cases, there is substantial flexibility (as there should be) regarding who can be an agent. The third enabler, risk-based CDD/KYC, is strongly influenced by countries' desire to strictly follow FATF guidance. The shift toward risk-based rules at global and national levels, combined with digital ID system developments, is starting to allow for greater DFS outreach, but at differing rates across countries. Consumer protection, the fourth enabler, comes into the picture rather late, because it has a more obvious role in ensuring sustainability than in jump-starting DFS markets. But its importance as a trust-building element is now widely recognized. Finally, it should be borne in mind that other conditions besides these enablers play a role in shaping DFS development, including policies in areas such as competition, data protection, and interoperability.

A collective learning process is ongoing among policy makers and regulators, both within and across countries, as the frontier of good practice advances. Some of the countries studied (Myanmar) have only recently adopted specific regulations for DFS and have been able to learn from earlier experience of other countries. Others (Ghana) can look back on many years of experience with DFS regulation and learn from past mistakes. Still others (Pakistan) have been able to improve their regulatory framework gradually over time.

Introduction

How can regulation encourage the use of sound, technology-driven methods to speed financial inclusion? What lessons can we learn from experience in countries that have pursued this goal?

It has been more than 10 years since CGAP first studied newly emerging models that use agents as alternative delivery channels and digital technology to connect customers to their financial services providers. We called this ***branchless banking*** and referred to those models that directly benefit the unbanked or underbanked population as ***transformational*** branchless banking.[1] The terminology has changed over the years, especially to recognize the developments in relation to services provided by nonbanks. Nowadays we prefer to use the broader terms ***digital financial services*** (DFS) and ***digital financial inclusion***. But the basic ingredients—agents and technology—remain the same.

We define DFS as the range of financial services accessed through digital devices and delivered through digital channels, including payment, credit, savings, and remittances.[2] DFS can be offered by banks and nonbanks such as mobile network operators (MNOs) or technology companies that specialize in financial services (FinTechs).[3] Digital channels can be mobile phones, cards combined with card readers, ATMs, computers connected to the internet, and others. Customers transact through branches, but also through agents or remotely from their digital devices. They typically use basic transaction accounts targeted at the mass market (including ***e-money*** accounts, also called prepaid or stored-value accounts), but also access services over the counter (OTC).[4]

Four factors distinguish DFS in a financial inclusion—or digital financial inclusion—context from traditional financial services: (*i*) new providers such as e-money issuers (EMIs); (*ii*) heavy reliance on digital technology; (*iii*) agents serving as the principal interface with customers; and (*iv*) use of the services by financially excluded and underserved customers.[5] Each of these factors has implications for digital financial inclusion—and for regulating DFS.

For many years now, CGAP has been monitoring how new DFS models are regulated, and how regulation might have to adapt to support or enable DFS models with the potential to advance financial inclusion. In 2007, CGAP developed a list of "key topics in regulating branchless banking" (Lyman et al. 2008). Four of these topics are now widely considered the core building blocks of DFS regulation. This Focus Note takes a close look at these four basic regulatory enablers and how they have been implemented in practice. We analyze the frameworks adopted by 10 countries in Africa and Asia where CGAP has focused its in-country work on promoting a wider market systems approach to DFS.[6]

The four basic regulatory enablers

The following enablers have guided CGAP's assistance in partner countries in creating appropriate regulatory frameworks for DFS:

Enabler 1: Nonbank E-Money Issuance

A basic requirement is to create a specialized licensing window for nonbank providers—EMIs. These entities accept funds from individuals for repayment in the future (an activity normally reserved for banks) against the issuance of e-money accounts (also variously called prepaid or stored value accounts), a type of basic transaction account. EMIs may issue such accounts without being subject

1 The term "branchless banking" was first used in Lyman, Ivatury, and Staschen (2006). Porteous (2006) introduced the term "transformational".
2 See, e.g., the AFI glossary (AFI 2016). We do not discuss specific issues in offering insurance products digitally.
3 We use the term "bank" to refer to any type of prudentially regulated deposit-taking financial institution unless otherwise indicated.
4 Compare a similar definition of *DFS accounts* in Arabehety et al. (2016). Our definition of transaction account is in line with the definition in the PAFI Report (CPMI and World Bank Group 2016): "Transaction accounts are defined as accounts (including e-money/prepaid accounts) held with banks or authorized and/or regulated PSPs, which can be used to make and receive payments and to store value."
5 This list draws on GPFI (2016), but leaves out the factor of new products and services and their bundling, because the focus here is on many of the same products and services offered before. New products such as digital credit, crowdfunding, and bundled products would require a separate analysis.
6 This approach, described by Burjorjee and Scola (2015), focuses on the core determinants of supply and demand, including regulation and supervision as one of the functions supporting the core.

to the full range of prudential rules applicable to traditional banks—under the condition that they do not intermediate the funds collected from their clients. This opens space to nonbanks that can provide basic financial services, potentially with lower costs and greater efficiency.

Enabler 2: Use of Agents

Next, DFS providers—both banks and nonbanks—are permitted to use third-party agents such as retail shops to provide customers access to their services. This allows the use of existing third-party infrastructure to create much wider access at relatively low cost.

Enabler 3: Risk-based Customer Due Diligence

A proportionate anti-money laundering and countering the financing of terrorism (AML/CFT) framework allows simplified customer due diligence (CDD) for lower-risk accounts and transactions, such as opening and using basic transaction accounts or conducting low-value OTC transactions with DFS providers. This eases providers' costs of customer acquisition, while making more people eligible to access and use formal financial services.

Enabler 4: Consumer Protection

Financial consumer protection (FCP) rules are tailored to the full range of DFS providers and products. It might be argued that such FCP rules are not necessary for the *emergence* of a DFS market. It is nonetheless clear that basic rules in areas such as transparency, fair treatment, effective recourse, and service delivery standards are needed to build consumer trust and create a safe and sound DFS sector in the longer term.

Why the focus on these four elements? They arise consistently in CGAP's experience working on DFS frameworks, and their importance is underscored in research and policy discussions. There is wide agreement that the four enablers are necessary (though not sufficient) conditions for DFS to flourish. This is not to deny that DFS has emerged in some markets where one or more of the enablers are weak or missing, nor that other enablers, such as healthy competition or interoperability, might be equally important in some settings. But experience strongly suggests that, in any given market, DFS is far more likely to grow responsibly and sustainably to its full potential when all four elements are in place.[7] (See Box 1.)

Box 1. The emerging consensus on regulatory enablers

Following a seven-country study in 2007 (Lyman et al. 2008), CGAP identified (*i*) the authorization to use retail agents and (*ii*) risk-based AML/CFT rules as necessary, but not sufficient, preconditions for inclusive DFS, and classified several others as "next generation" issues, including (*iii*) regulatory space for the issuance of e-money particularly by nonbanks; (*iv*) effective consumer protection; and (*v*) policies governing competition.[a]

GSMA characterizes countries' regulatory frameworks on mobile money as "enabling" or "nonenabling" according to criteria including the following: (*i*) nonbanks are permitted to issue e-money; (*ii*) capital requirements are proportional to the risks of the e-money business; and (*iii*) mobile money providers may use agents for cash-in and cash-out operations. Furthermore, GSMA lists CDD requirements as one of the major obstacles to mobile money uptake. It also stresses the importance of customer protection measures such as transparency, customer recourse, and privacy and data protection (Di Castri 2013).[b]

The Regulatory Handbook by researchers from the University of New South Wales (Malady et al. 2015) considers four factors relevant to creating an enabling regulatory environment that are like those presented in this Focus Note.[c]

a The study also mentioned inclusive payment system regulation and effective payment system oversight. The creation of a competitive ecosystem can be regarded as a cross-cutting issue that is not only—and not even primarily—a matter of financial sector regulation. See Mazer and Rowan (2016), who looked at competition in MFS in Kenya and Tanzania. The competition issue most clearly overlaps with our basic enablers 1 and 2. In a recent report, the Center for Global Development makes a distinction between promoting competition and leveling the playing field, with the former addressing market failures and the latter distortions derived from regulations. The report considers these two and KYC rules as the three regulatory topics that matter most for financial inclusion (see CGD 2016).

b But GSMA does not cite consumer protection as a *necessary* regulatory condition for DFS development. See also GSMA (2016).

c They are (*i*) the protection of customers' funds, (*ii*) the use of agents, (*iii*) consumer protection, and (*iv*) proportionate AML/CFT measures.

7 Empirical research confirms some of these correlations. *See, e.g.*, Rashid and Staschen (2017), who looked at evidence from Pakistan; Evans and Pirchio (2015), who researched 22 developing countries and concluded that: "Heavy regulation, and in particular an insistence that banks play a central role in the schemes, together with burdensome KYC and agent restrictions, is generally fatal to igniting mobile money schemes."

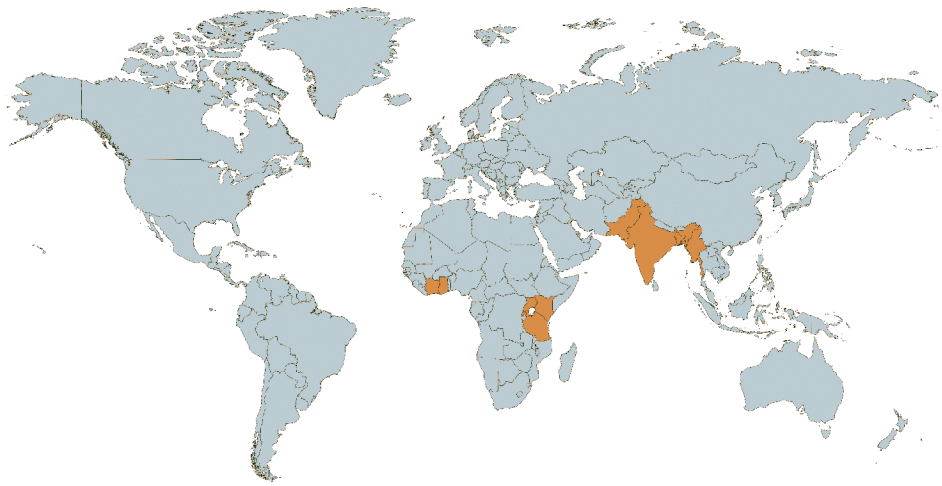
While there is broad agreement that these four enablers comprise the core of an enabling regulatory framework, the detailed content and sequence of specific policy changes are much less clear. Nor are the four enablers equivalent in terms of the type or scope of key regulatory decisions that need to be taken under each to make them effective. Enabler 1 is about creating room for new players that might be better placed to serve the lower end of the market than existing banks. Enabler 2 permits the use of a new channel (by old and new players) that leverages third-party infrastructure. Enabler 3 addresses the specific challenges in serving new customer segments that might previously not have been eligible or were too costly to serve. Enabler 4 stresses the changing nature of consumer protection issues with new players and new delivery channels that have to be taken into account for healthy market development. Even where an enabler is already incorporated into a country's legal framework, there may be need for improving its effectiveness, by continuously fine-tuning regulations,[8] and/or improving compliance and enforcement through supervision.

Approach and objective

The objective of our research was to understand how a range of countries have addressed the four enablers in their regulatory frameworks and to see what lessons can be learned from this experience. For this purpose, a granular analysis is required—of both policy and practice—that makes use of CGAP's understanding not only of regulatory issues across the 10 countries, but also of market structure, provider dynamics, and demand-side issues.

The analysis is based on a review of relevant laws and regulations from all 10 countries where CGAP has focused its in-country work (see Figure 1).[9] The countries covered are Kenya, Rwanda, Tanzania, and Uganda in East Africa, Côte d'Ivoire and Ghana in West Africa, Bangladesh, India, and Pakistan in East Asia, and Myanmar in Southeast Asia.[10] They figure among the most advanced DFS markets (with the exception of Myanmar),[11] and all but two (Rwanda and Côte d'Ivoire) are former British colonies that share the common law

Figure 1. Countries covered in the research



Bangladesh
Côte d'Ivoire
Ghana
India
Kenya
Myanmar
Pakistan
Rwanda
Tanzania
Uganda

8 E.g., India adopted regulations on agents (referred to as *business correspondents*) in 2006, but has since enacted several amendments to mitigate some of the constraints under the early model.

9 As laws and regulations frequently change, this paper does not include a list of all legal texts consulted. To the best of our knowledge, we considered the state of laws and regulation as of January 2018. For a comprehensive library of DFS-related laws, regulations, and policies, see www.dfsobservatory.com.

10 Unless otherwise indicated, general statements in this paper apply to these 10 countries only.

11 According to the GSMA Mobile Money Tracker, all of them have five or more live mobile money deployments (keeping in mind that DFS is a broader concept than just mobile money).

tradition. While the group is hardly representative of DFS markets in the developing world, it includes diverse countries in terms of size, population, and economic structure. Our intent is to analyze the experience of these 10 markets, and to share the lessons.

Based on legal analysis and our familiarity with the wider ecosystem, we distilled the most pertinent issues relevant to each of the enablers. The objective was not to come up with a complete description of the regulatory framework in each of the 10 countries (this would quickly become outdated), but to explore commonalities and differences, highlighting the most interesting cases for each issue.

1 Enabler 1: Nonbank e-money issuance

Our first basic regulatory enabler is a framework that allows nonbanks to issue a type of basic (digital) transaction account—an "e-money account." Allowing nonbanks to become licensed EMIs is key to unleashing the DFS market and enabling it to achieve scale. Chief among nonbank providers in emerging markets and developing economies (EMDE) are MNOs, who have large networks of agents and own the communication infrastructure that is key to delivering financial services. Absent a framework permitting EMIs, DFS would continue to rely on banks, which usually face heavy prudential and operating requirements, have high costs and complex organizational structures and IT systems, and limited outreach. Banks may also focus on higher-income market segments, to offset high operational costs.

The following are essential components of the first enabler:

- Setting basic parameters for the e-money account and EMIs.
- Establishing licensing criteria and range of permitted activities for EMIs.
- Protecting customer funds converted into e-money (i.e., e-float).

1.1 The legal basis for nonbank e-money issuance

The first step in enabling nonbank e-money issuance is to incorporate the concept in law or regulation.[12] Banking laws are sometimes a bar to nonbank e-money issuance, due to the legal definition of banking business; hence, a specialized definition of e-money as being distinct from deposit-taking is essential.[13] E-money accounts and their issuers have different names and regulatory headings across the world. This can create problems of comparability, but the basic concepts are largely the same everywhere. E-money combines functions such as facilitating payments and storing value electronically. A workable legal definition must squarely address these payment- and deposit-like aspects. For clarity, we use a common definition of e-money based on that used in the European Union for all 10 countries—even if the terminology used in local law differs (see Box 2). In fact, in some countries, the term "e-money" is not used at all.

The second step is to allow nonbanks to issue e-money. The countries analyzed exhibit several approaches to determining who may be authorized to issue e-money (see Table 1). The most common approach is to recognize e-money as a product offered exclusively by payment service providers (PSPs), which generally include banks. Kenya, Rwanda, and Tanzania, for instance, permit only PSPs to apply to become EMIs. Having a

Box 2. E-money definition

According to the European Union (Directive 2009/110/EC, Art. 1.3) e-money is defined as:

(i) electronically stored monetary value as represented by a claim on the issuer, (ii) issued on receipt of funds for the purpose of making payment transactions, and (iii) accepted by a natural or legal person other than the electronic money issuer.

12 In several cases, financial authorities have enabled e-money issuance without defining the concept in legislation (instead, issuing guidelines or no-objection letters).

13 In several countries, the acceptance of repayable funds (even without intermediation) fits the legal definition of banking activity, which prevents the emergence of EMIs. This was the case in Mexico until the adoption of its FinTech law in February 2018.

Table 1. E-money issuance[a]

Country	Institutions that may issue e-money	Banks: requirements for e-money authorization	EMIs (nonbanks): further requirements & limits[b]
Bangladesh	"Mobile accounts" can only be issued by banks or their subsidiaries. (EMIs allowed by law but not in practice.)	Banks to seek prior approval for MFS; must submit full details of services, contracts, agents, etc.	Only bank subsidiaries are permitted (under the same rules as banks). (EMIs allowed by law but not in practice.)
Côte d'Ivoire (WAEMU)	Commercial banks and PSPs may issue but must notify regulator. MNOs must establish dedicated subsidiary and apply for license as EMI.	Commercial banks required only to notify regulator.	EMIs must be dedicated companies and meet capital requirements: minimum 3% of outstanding e-money, and at least equal to their minimum share capital requirements.
Ghana	Banks are authorized as EMIs, nonbanks licensed as dedicated EMIs (DEMIs).	Submit plan for proposed operations, business plan, geographical coverage	If engaged in other activities, nonbank must create separate dedicated legal entity for DEMI. Min. 25% local ownership
India	Issuance (open-loop PPIs) limited to banks and payments banks.	Banks/payments banks to get RBI approval for open-loop PPIs.	No issuance by nonbanks.
Kenya	Banks, PSPs, and other financial institutions authorized to issue e-money. PSP can be telecom company or a nonbank.	None	MNOs must present telecom license. PSPs to keep records and accounts for e-money activities.
Myanmar	Banks and nonbank financial institutions including MNOs can apply to provide MFS	Regulations do not specify, only mention that they require product approval.	Dedicated company required to set up mobile financial services provider. Nonbanks need letter of no-objection from primary (e.g., telecom) regulator.
Pakistan	Branchless banking accounts: Only Banks (Islamic, Microfinance, Commercial Banks).	Application: specify services and strategy, risk management, security, business continuity, etc.	Provision for nonbank e-money issuance under payments law, but no implementing regulations issued
Rwanda	Nonbanks must get license as PSP. Commercial banks and deposit-taking MFIs (supervised financial institutions), must be approved as payment services providers to apply to issue e-money.	Supervised financial institutions approved as PSPs are exempt from licensing, but must obtain further approval to issue e-money.	Application: describe services, governance, risk management, IT infrastructure, consumer policies, trustees, directors.
Tanzania	Only PSPs can issue e-money. Nonbank PSPs must obtain license. PSPs that are financial institutions require regulator's approval.	Financial institutions need PSP license to be eligible. Application: information on services, governance, fund protection.	Nonbank PSPs require separate dedicated entity. Application: like financial institution, also, minimum capital, process/ system architecture, etc.
Uganda	Nonbank can become mobile money services provider (MMSP) as partner of bank. Regulator approves partner bank; mobile money is product of the bank.	Partner bank must apply for approval to issue mobile money on behalf of the MMSP.	Limited company; submit financials, risk management, IT systems. The MMSPs (nonbanks) manage mobile money platform.

a. Some countries separately list banking institutions that are not commercial banks. These distinctions are indicated where relevant.
b. EMI licensing requirements are often in addition to the requirements applied to banks seeking e-money authorization.

PSP certificate is a prior condition for obtaining an e-money license (or authorization). Another approach is for the financial regulator to license EMIs as a separate, stand-alone category of institution. In Myanmar, for example, becoming a mobile financial services (MFS) provider (functionally equivalent to an EMI) requires a registration certificate (e.g., a license) issued under the broad authority of the banking law. Côte d'Ivoire, as a WAEMU member, also offers a stand-alone EMI license.[14] In the approaches cited, policy makers create a regulatory niche, or adapt an existing one, to accommodate the distinct features of e-money.

Some of the 10 countries, however, fall short of this second step by allowing only banks to issue e-money. In all 10 countries, banks *may* become issuers, but as they are already licensed and supervised, they require approval only by the central bank to offer e-money accounts as an additional product. However, three of the countries (India, Pakistan, and Bangladesh)[15] have generally treated e-money issuance as analogous to offering deposit accounts, and thus limited it to banks.

The bank-only approach has a few variants, which is evidence that nonbanks still play a leading role in the DFS space, subject to a few limitations.

- In India, the equivalent of e-money accounts—prepaid payment instruments (PPIs) that are open loop (i.e., can be used outside a restricted network and redeemed for cash)—can be issued only by banks. In addition, the central bank has created the new category of *payments bank* specializing in small savings and payments services. This "differentiated" or special-purpose bank can accept limited deposits, issue e-money, and provide remittance services—but cannot extend credit.[16] Payments banks are subject to less onerous licensing and prudential standards than commercial banks (though more onerous than the typical EMI in other markets).[17] Among the promoters of the 11 entities that received "in principle" approval for a license from the central bank were MNOs, the India Post, and other nonbanks such as agent companies and prepaid payment issuers.
- In Pakistan, a nonbank e-money model has not been permitted either. However, MNOs have either bought majority stakes in banks or set up greenfield banks to offer MFS in a *de jure* bank-based model. Further, these services can be provided through microfinance banks, which benefit from lighter requirements such as lower minimum initial capital.
- Bangladesh follows what is called a "bank-led model." However, the fact that not only banks, but also bank subsidiaries are permitted to offer so-called "mobile accounts" has permitted the largest DFS provider in Bangladesh, bKash, to operate as a nonbank (but bank subsidiary), and thus follow a *de facto* e-money model.[18] This is a case of reality overtaking the original regulatory intent of restricting e-money issuance to the banking system.

In yet another configuration, Uganda requires EMIs to be tightly *linked* to banks—but not to *be* banks. Ugandan EMIs (referred to as *mobile money services providers* [MMSPs]) offer e-money services in partnership with a bank as the licensed entity. The EMI itself is not a licensed institution, but is responsible for managing the mobile money platform and agent network, and for

14 The West African Economic and Monetary Union is a regional jurisdiction that provides for, among other things, common financial services laws and regulations across member countries. Where this paper addresses Côte d'Ivoire, the main regulations discussed are WAEMU-wide and are overseen by the regional central bank, BCEAO. Other WAEMU members are Benin, Burkina Faso, Guinea-Bissau, Mali, Niger, Senegal, and Togo.

15 See the caveat with respect to Bangladesh.

16 Limited-purpose banks are also the current approach in Mexico, where there are "niche banks" limited to payment services.

17 Payments banks are also subject to ownership rules, including a minimum share (40 percent) for the promoter in the initial years, followed by diversification requirements and restrictions on equity and voting rights concentration.

18 BRAC Bank owns 51 percent of bKash, with the remaining shares owned by Money in Motion, IFC, and the Bill & Melinda Gates Foundation. Bangladesh (as well as Pakistan) in practice does not permit a nonbank-based model, despite having regulatory provisions allowing nonbanks to issue e-money. Bangladesh's Payments and Settlement Systems Regulations (2014) define e-money issuance as a payment service (only PSPs qualify)—but no license has been issued to nonbank EMIs to date. Also, Pakistan's Payment Systems and Electronic Fund Transfer Act (2007) provides sufficient room for the direct licensing of nonbank providers as EMIs, but the State Bank of Pakistan never issued implementing regulations to this effect.

issuing "mobile wallets," (i.e., e-money accounts), under some basic rules established in regulatory guidance.[19]

In the countries studied, but also in many other EMDE, full-fledged traditional banks have not been efficient DFS providers because of their high costs and their heavy prudential and operational regulations. In Bangladesh, for example, while more than 20 banks have been licensed to provide MFS, none of them comes close to bKash, the only nonbank provider. Bank regulations include a wide range of prudential norms that are not required for EMIs that do not intermediate public funds. These rules are too burdensome for banks focused on e-money issuance to flourish—except in those cases where limited purpose banks are exempt from many of the requirements. While commercial bank regulations are too heavy, generic PSP regulations are typically too light for purposes of e-money issuance, given the different risk profiles of fund transfers versus stored-value accounts.

E-money is a distinct product with similarities to both deposits and payments, and should be regulated accordingly. This is why e-money is increasingly treated as a kind of *payments-plus* activity.[20] Thus, Kenya and Tanzania require providers to have a PSP authorization but also (with the exception of banks) to submit to more rigorous further scrutiny to gain an e-money license.[21] Ghana and WAEMU allow banks to become authorized EMIs through a relatively simple process, while nonbanks must obtain an EMI license.[22] A variety of regulated institutions in these two jurisdictions may seek authorization to issue e-money, including PSPs and microfinance institutions (MFIs), and nonbanks such as MNOs may apply for an EMI license.

1.2 Licensing requirements, permitted activities, and reporting

Once a policy of nonbank e-money issuance is in place, further steps are required to define licensing criteria and to delimit the range of permitted activities for EMIs. Limiting the range of permitted activities is important for lowering the risk profile of EMIs, which in turn allows them to take advantage of relaxed entry and ongoing requirements (i.e., less stringent than for commercial banks). The most important limitation for EMIs is the prohibition on intermediating funds collected from their clients.

Where e-money is conceived as being not a deposit-like but rather a payment-like or *payment-plus* product, there is a straightforward policy basis for licensing nonbanks as EMIs and regulating them accordingly. For institutions already engaged in other types of business, licensing (or lighter-touch *authorization*) often requires the applicant to establish either a unit (Kenya) or a subsidiary dedicated to e-money issuance (in Côte d'Ivoire and Ghana for all types of nonbanks, and in Myanmar for MNOs). The separation of e-money operations (and finances) from those of a parent nonbank company is considered essential for effective supervision (BCBS 2016, p. 11). The other option is to set up a new, free-standing EMI. The legal term for licensed EMIs differs across countries.[23]

Allowing nonbanks to issue e-money entails bringing them under the direct authority of the financial services regulator—in the 10 countries, the central bank. In some countries, where an MNO seeks to become an EMI, it must provide supporting evidence from the telecom regulator—for example, a certified copy of its telecommunication license

19 This arrangement came into being not by design but because of Bank of Uganda's lack of legal authority to authorize or regulate nonbank PSPs (in the absence of a dedicated payments law).

20 For this reason, in certain jurisdictions e-money is subject to both payments regulation and a specialized e-money regulation. In the European Union, e-money is subject to the general rules of the Payments Directive, which are applicable to all types of payments, and to the rules of the E-Money Directive, which focus on the deposit-like functions of e-money.

21 See relevant sections of National Payment System Act and Regulations (Kenya); and Tanzanian National Payment System Act, 2015 and Electronic-Money Regulations 2015, Third Schedule (Tanzania).

22 Myanmar falls into the same category, although the regulations lack clarity on how exactly they apply to banks when they want to launch MFS.

23 E.g., dedicated EMI (DEMI) in Ghana, *etablissement de monnaie electronique* in Côte d'Ivoire (for issuers that are not banks, PSPs, or MFIs), and MFSP in Myanmar.

Table 2. Capital requirements and authorization fees (US$)

Country	Licensed EMI (nonbank)	Minimum initial capital: EMI	EMI authorization / application fees	Minimum initial capital: Bank
Côte d'Ivoire	EMI	490,000	Information not available.	16.36 million
Ghana	DEMI	1.2 million	2,200	14.25 million
India	Payments bank	15.4 million	Information not available.	77.2 million
Kenya	EMI	193,000	Authorization fee: 9,700 Application fee: 50	9.7 million
Myanmar	MFSP	2.2 million	Information not available.	14.8 million
Rwanda	EMI	121,000	Financial institutions: 1,200 Nonfinancial institutions: 6,000	3.6 million
Tanzania	EMI	224,000	900	6.7 million
Uganda	MMSP	n.a. [must partner with a bank]	Information not available.	6.9 million

(Kenya) or a no-objection letter (Myanmar). Minimum initial capital for EMIs is lower than for banks, ranging from just under US$200,000 for an EMI in Kenya to US$2.2 million for a mobile financial services provider (MFSP) in Myanmar. In comparison, payments banks in India need more than US$15 million in capital (see Table 2).[24] Other requirements deal with matters such as the business plan, risk management, settlement of customer claims, and IT systems. EMIs are generally required to be limited liability corporations, and some countries impose ownership requirements (see Table 1). In Ghana, for example, a dedicated EMI must have at least 25 percent indigenous ownership.

The range of EMIs' activities is often restricted to core functions such as issuing e-money accounts, cash-in/cash-out, and domestic payments and transfers. Payments could include utility bills, merchant payments, salary disbursements, elderly allowances, and tax payments (as in Bangladesh). Other related services are treated differently across countries. For example, OTC transfers are expressly permitted in Ghana and prohibited in Uganda, while other countries (Tanzania) do not address the issue directly. Inbound international remittances are also subject to varied, sometimes unclear, treatment. For example, in Ghana and Myanmar, such remittances are expressly permitted, while in other countries (Uganda) there is no explicit rule. In such cases (Kenya), general rules on money remittance services might apply.

Most importantly, financial intermediation by EMIs is not allowed.[25] These EMIs cannot provide services such as credit, investments, insurance, or savings on their own account, but in some cases, may provide access to them in partnership with a licensed financial institution. Further, e-money accounts are generally subject to quantitative ceilings (e.g., maximum e-money outstanding per issuer or maximum balance per customer).

In addition to the licensing requirements, EMIs are subject to ongoing reporting requirements that are relatively light (see Box 3).

Box 3. Reporting and access to data

EMIs must submit regular reports to the central bank. The rules generally demand monthly reporting on, for example, the number of accounts, volume and value transacted, agents, incidents of fraud, complaints, scope of services, and loss of data. There is also annual reporting in the form of audited financial statements and reports on risk management and IT practices (in some cases, including an external system audit, as in Bangladesh). The regulator is generally allowed to access all databases and registries of transactions from EMIs and agents. Records of electronic transactions are to be kept for a period of years (e.g., five years in Myanmar, seven in Kenya).

24 Kenya also offers a *small e-money issuer* license with lower minimum capital, but restricts issuance to closed and semi-closed loop instruments. Several other countries including India and Pakistan also provide a sliding scale of requirements for issuers of closed-, semi-closed, and open-loop instruments, but only the latter are considered here as having the functionality of e-money.

25 Strictly speaking, it is the intermediation of deposits in the form of loans that is prohibited. Some jurisdictions, including WAEMU and Rwanda, permit placement of funds in approved investment and debt instruments.

1.3 Treatment of e-float

The last key component of the framework for nonbank e-money issuance is the protection of funds collected from customers and converted into e-money (i.e., the e-float).[26] Upon receipt of funds from the customer, the rules generally require the prompt deposit of those funds in bank accounts or placement in other safe, liquid assets. The rules may specify a time limit for the funds to be deposited or reconciled with the e-float, or simply state that the funds in the e-float account may never be less than the aggregate e-money issued.[27]

The first concern arising here is whether and how customer funds are protected from any claims and risks to which the EMI is subject. A third-party claim on the EMI (e.g., due to default or bankruptcy) could attach to funds in the e-float account. The e-money rules do not always address this issue directly,[28] but some countries require the isolation and ring-fencing of e-float funds from claims on the EMI. In Ghana, the regulations require e-float deposits to be separately identified, and prohibit any commingling with funds that have a different source or purpose.[29] In contrast, the rules in Uganda stipulate that e-float funds are the property of the customer and not of the EMI. It is important that these countries have set up such protections, but whether they are effective against other legal claims will need to be confirmed in practice.

Some countries protect the e-float (once deposited in a bank) by specifying that it should be placed in a special type of account. One approach is to require such deposits to be placed in a *trust* account administered by a trustee on behalf of the e-money customer (as in Kenya, Myanmar, Tanzania) (Greenacre and Buckley 2014).[30] A similar arrangement is an *escrow* account. This is an account managed by a third party, where funds are released upon the occurrence of conditions stated in the escrow agreement (e.g., authorized payment, settlement).[31] An escrow account is required for EMIs in Uganda.

The second question is what prudential safeguards apply to the e-float. In most of the 10 countries, regulations mandate that all customer funds (100 percent of all e-money outstanding) be deposited with commercial banks.[32] Partial exceptions to this rule are WAEMU and Rwanda, where a portion of the funds—up to 25 percent and 20 percent, respectively—may be placed in other types of safe investments. Further, concern about concentration risks on the part of the investor (the EMI) or the investee (the bank holding the e-float) has resulted in diversification rules. Some countries place ceilings on the proportion of an issuer's e-float funds deposited in any single bank (e.g., in Tanzania the maximum is 25 percent), while others set a limit on the value of e-float deposits as a percentage of the recipient bank's net worth (e.g., 15 percent in Ghana, and 25 percent in Rwanda). (See Table 3.)

There are a variety of approaches to interest accrued on e-float accounts. Some jurisdictions such as WAEMU and the EU do not permit any interest to be paid to e-money customers for the funds deposited.[33] Alternatively, several countries (such as Ghana, Kenya, Tanzania, and Myanmar) prescribe the allocation of any such interest accrued (Tsang et al. 2017). Tanzania, for example, requires

26 This discussion draws on Tarazi and Breloff (2010).
27 This is the case, e.g., in Myanmar, Tanzania, Rwanda, and Ghana (See Table 3).
28 E.g., in Côte d'Ivoire, the rules restrict the use of the funds to e-money reimbursement. This provides a measure of protection, but it is not clear whether this would be effective, e.g., in the case of the EMI's bankruptcy.
29 The European Union has a similar provision. See Oliveros and Pacheco (2016). This in effect means that the e-float funds should not appear on the issuer's balance sheet and not be available to meet any other obligations of the issuer.
30 Trusts are better known in common law than in civil law countries; however, the law in this area has been evolving.
31 Although the relevant law differs in detail across countries, escrow is designed to place assets beyond the legal control of the issuer, which protects them from many third-party claims. In comparison, a trust is a more formalized structure and is usually deemed to be a stronger protection to the assets in it.
32 The central bank may specify or approve certain banks for this purpose (e.g., in Kenya, those meeting strength criteria).
33 For Côte d'Ivoire, see *Instruction N°008-05-2015 Régissant les Conditions et Modalités d'Exercice des Activités des Émetteurs de Monnaie Électronique dans les Etats Membres de l'Union Monétaire Ouest Africaine (UMOA)* (2015), arts. 32-35. For the EU, see Directive 2009/110/EC, art. 12.

Table 3. Regulations on e-float

Country	Fund safeguarding rules	Diversification requirement	Interest payment	Reconciliation
Côte d'Ivoire	Placed in a bank. At least 75% in sight/demand deposits, the balance in time deposits, T-bills, or corporate securities.	Not specified.	No interest paid to e-money customers.	Daily
Ghana	Hold as liquid assets in banks.	Not to exceed 15% of net worth of bank.	80% of income from pooled account to be paid to EMI clients.	Daily
Kenya	Trust Fund	Once float exceeds US$950,000, max 25% of float may be kept in a single bank and 2 of the banks must be strong-rated.	Income from trust account to be used according to trust legislation or donated to public charity, but not paid out to customers.	Daily
Myanmar	Trust Account	Central bank may set a limit on number of accounts in pooled account.	Interest from trust should go to clients.	Daily
Rwanda	Trust Account or special account. Up to 20% in short-term government securities; up to 10% in term deposits (max 3 months).	Not specified.	Pass through at least 80% of interest earned on float account.	Daily
Tanzania	Trust Account	If float exceeds US$45,000, max 25% of float may be kept in a single bank. Each single bank cannot hold trust float funds exceeding 50% of its core capital.	Interest from trust shall be used for direct benefit of e-money customers.	—
Uganda	Escrow Account	Bank of Uganda may require.	Not specified.	Daily

interest accrued in the trust account to be used for the direct benefit of customers and held in a separate account until it is paid out. Bangladesh and Myanmar have a similar rule. Ghana requires 80 percent of the interest accrued on e-float accounts to be paid to e-money customers.[34] In Kenya, by contrast, income generated from e-money trust funds must be donated to a public charitable organization in accordance with trust legislation and in consultation with the central bank.

How are e-money accounts and e-float accounts treated under existing deposit insurance systems? Often, this issue is not explicitly addressed in the law or regulation. In that case, e-float accounts would, in principle, fall within the deposit guarantee system—that is, if accounts from legal persons are covered. But the simple application of this guarantee would pose problems, since e-float accounts exceed the per-account ceiling. In India, payments banks issue e-money against deposits, which are covered by the deposit insurance and credit guarantee corporation. Ghana's e-money regulations require e-money accounts to be granted the same protection as deposit accounts. In Kenya, a pass-through deposit insurance policy covering individual customer account balances held in the trust accounts has been adopted but not yet put into operation (Izaguirre et al. 2016; Oliveros and Pacheco 2016).[35]

34 Some customers in Ghana have reportedly asked that no interest be paid to them for e-float, which raises the question of what alternative arrangements (e.g., *Shari'a*-compliant vehicles) might be made to enable such customers to share equitably in the earnings.

35 Very few countries, including the United States, have pass-through deposit insurance provisions in place.

1.4 Summary of experience

The following general patterns emerge from the 10 countries' experience in this area:

- In all 10 countries, nonbanks are playing a leading role in offering basic transaction accounts to the mass market.[36] This was accomplished by the countries generally abstaining from imposing the full range of requirements applicable to commercial banks in exchange for limiting their range of activities and prohibiting intermediation of funds. Seven of the 10 countries have opened space for nonbank e-money issuance by creating a separate regulatory niche for EMIs.
- The three largest countries among the 10 countries—all from South Asia—did not create a separate licensing window for EMIs, choosing to restrict e-money issuance to banks (and bank subsidiaries in the case of Bangladesh). In India, limited-purpose banks with lighter requirements than full-fledged banks were introduced by regulation, allowing nonbanks to establish separate entities to obtain a license and issue e-money. The approach is different in Pakistan, where nonbanks need to acquire stakes in existing or newly founded banks (though the latter can be microfinance banks). In Bangladesh, the dominant EMI is a nonbank that is not directly licensed by the regulator and operates under the auspices of its parent bank.
- In the case of EMIs, there is convergence on prudential safeguarding of e-float funds in bank accounts, and isolation of the funds from third-party claims through trusts or similar structures.
- Other questions remain open to divergent approaches, including whether and how e-float funds are to be protected by deposit insurance systems or whether customers should benefit from interest earned on the e-float account.

2 Enabler 2. Use of Agents

Inclusive DFS depends on providers' ability to outsource customer-facing functions to agents—thereby extending their reach and capturing efficiencies. Traditional service channels, especially "brick-and-mortar" branches, cannot solve the distribution problem in a cost-effective manner. Ideally the full range of providers—banks and nonbanks such as EMIs—should be permitted to distribute their products and services cheaply through a wide range of agent types. But this heightens agent risks that may affect customers or providers. A balance must be struck between inclusion and safety.

In this part, we discuss the following critical dimensions of the second enabler:

- Establishing a basic framework for the use of agents in DFS, in which the responsibilities of agents and principals are clearly delineated.
- Fixing criteria for the form and content of the agency agreement, including the type and scope of the agency.
- Setting standards of eligibility and procedures for authorization of agents.
- Providing for ongoing obligations of both parties, including security and reporting standards.

Our analysis of these areas identifies a few distinct approaches that the different countries follow in regulating agents used by DFS providers. These reflect policy decisions such as categorizing agents by the types of providers they represent or by the kinds of activities in which the agents are engaged.

2.1 Basic framework for DFS agency

Agency arrangements are familiar across many sectors of the economy and can be adapted to the needs of financial services, including DFS. Agency contracts are usually governed by a well-developed set of legal standards. Depending on the context, these may include common law principles, provisions of the civil or commercial code, legislation on certain types of agents (e.g., broker, distributor, trustee), or general outsourcing rules for financial institutions.

In the DFS context, heightened risks arise not only from the differing interests of principals and agents, but also due to intervening factors

36 Most, but not all, of these are e-money accounts.

linked to technology platforms, remote access, and the complexity inherent to financial services. Regulators have identified operational, consumer, and money laundering/terrorist financing risks as the major agent-related risks (Dias et al. 2015). In response, the countries studied have developed specific regulations to govern agency relations and their inherent risks.

Where agents are permitted, allocation of legal responsibility is essential. Every agent acts on behalf of a responsible *principal*. Agency regulations generally stipulate the principal's liability for its agent's actions within the scope of delegated responsibility (whether expressly or clearly implied). Regulations in the countries studied make this principal liability explicit, sometimes requiring it to be stated in the agency agreement. In several countries, the laws expand the liability of banks to include *any* improper actions of the agent (this applies only where a bank is the principal).[37]

However, the regulations do not solely rely on this liability provision. They also specify due diligence and risk management steps to be taken by principals with respect to their agents. Regulations generally require the principal to carry out *ex ante* and ongoing (or periodic) assessment of an agent's risks and to have appropriate internal controls and risk management systems. In half of the 10 countries,[38] the rules require principals to provide agents with training on their role in financial services delivery. Some countries such as Bangladesh, India, and Rwanda have detailed risk management frameworks (e.g., IT requirements) for the use of agents by licensed institutions as well as rules for agents' liquidity.

A few experts have questioned the need for financial institutions to assume liability for and oversight of the activities of all agents (e.g., Mas 2015). They argue that most agents are simple "cash merchants" transacting against their own money. In the real-time, prefunded environment of DFS as it is seen in most of the 10 countries, cash-in and cash-out transactions, unlike bank deposits, do not increase bank liabilities but only transfer values between account-holders.[39] This limits agent risk essentially to consumer protection and AML/CFT issues. When outsourcing goes beyond this level, for example, when agents are involved in account opening or credit assessments, the risks increase.[40]

Several countries distinguish between nonbank and banking agents across the board, imposing stricter requirements on the latter. Few countries have implemented a truly risk-based approach and have instead imposed differential treatment on agents that basically offer the same standard services. An activity-based approach applying uniform rules to all types of providers and all types of accounts for a given type of activity (e.g., cash-in/cash-out versus loan disbursement) seems optimal for creating a level playing field. This is particularly the case with increased agent sharing and models where bank accounts are served through EMI agents, as is the case in many digital credit models.[41] (See Box 4.)

2.2 Terms of the agency agreement

Beyond establishing the basic framework for DFS agency, policy makers are concerned about the form and content of the agency agreement (i.e., what an agent may be hired to do and how the agent is bound to the principal). We first take up the how question.

In all 10 countries, a written contract is required for retaining an agent, and model agreements may be inspected by the regulator. In some countries, the regulations prescribe contractual language, such as

37 Bangladesh, Kenya, Myanmar, and Tanzania apply this rule (in Tanzania it includes acts of omission), reasoning that the principal bank is the party best able to monitor agents' behavior and to deter misconduct.

38 Bangladesh, Kenya, Pakistan, Rwanda, and Tanzania.

39 An exception is India, where the central bank has instructed the principal bank to consider the cash handled by the agent as its own cash and lower the agent's prefunding levels as it gains experience over time with the agent. RBI Circular on Issues in Cash Management—RPCD.FID.BC.No. 96/12.01.011/ 2013-14.

40 Kenya distinguishes between cash merchants and full agents in its National Payment System Regulations (Arts. 14–18), but imposes identical standards on them.

41 This is the case in, e.g., Kenya and Tanzania, where banks have partnered with EMIs to offer bank accounts to e-money customers. Customers can access their bank accounts only by moving money in and out of the mobile wallet offered by the EMI partner. Examples for this are M-Shwari in Kenya and M-Pawa in Tanzania.

Box 4. Contrasting approaches to agent regulation

The countries studied illustrate divergent approaches to agent regulation, of which we have identified three. The institution-based approach defines agent rules within the regulatory framework for different types of financial institutions that are permitted to use agents. The focus here is on who may use agents, and what conditions apply to each category of provider—with the requirements depending on the type of principal doing the outsourcing. An alternative approach is the *account-based* approach, where the rules depend on whether agents serve bank accounts (savings or credit) or e-money accounts. An *activity-based* approach defines different rules for agents depending on the types of services being outsourced regardless of the type of principal or the type of account served.

Most agent regulation is institution-based (see Table 4). This approach is straightforward in a country like Pakistan, where only banks—including microfinance banks and Islamic banks—can offer DFS. Similarly, in India, the regulations for different types of banks, including the recently launched payments banks as well as banks issuing PPIs, all refer to the same set of rules for agents (business correspondents).[a] The different categories of banks are subject to the same agent rules. However, the institution-based approach leads to fragmentation in a country like Kenya, where banking agents, deposit-taking MFI agents, and PSP agents have their separate regulations.[b] While this approach might reflect a risk-based regulatory design, more often the differences stem from the fact that different types of agents are regulated under different laws (e.g., banking law vs. payments law vs. microfinance law). Account-based and especially activity-based approaches are usually closer to a true risk-based model.

The account-based approach comes into the picture when, for example, banks offer not only deposit and credit accounts, but also e-money accounts, through agents. In Bangladesh, only banks (and bank subsidiaries as in the case of bKash) can use agents. Bangladesh has banking regulations dealing with banking agents as well as distinct, overlapping MFS rules applicable to banks (and bank subsidiaries) authorized to offer MFS. In Tanzania, banks can be EMIs, in which case their e-money agents follow the rules for EMI agents rather than for agency banking. In these two examples, different departments supervise agent activities, depending on the type of account offered by the principal regardless of the type of activity undertaken by the agent (which could be the same standard cash-in and cash-out operations). Payment, MFS and e-money accounts come within the authority of the payments department, while bank accounts are under banking supervision.

There are two examples of activity-based approaches in the countries studied. Ghana and Rwanda apply a common set of agent outsourcing rules to different types of institutions. In Ghana, banking and e-money agent activities come under a single, common framework (though handled by different departments of the Bank of Ghana), just as Rwanda applies the same set of agency rules to banks, MFIs, PSPs, remittance services providers, and EMIs. Differentiated treatment can then be applied to the various *activities* carried out by the agents. This treatment is defined in part by the rules generally applicable in areas of activity such as e-money issuance, remittances, and deposits. Also, Ghana and Rwanda permit a wider range of activities to agents that are companies (in Ghana, companies meeting a size threshold) than to individual agents.[c]

a PPI issuers that are not banks are permitted to use other agents, but not for open-loop payment instruments.
b The same holds true for banking agents, PSP agents, and EMI agents in Tanzania. But Tanzania's Electronic Money Regulations (2015) take an account-based approach that does not differentiate among the types of institutions approved to issue e-money—thus making it a hybrid.
c Also, in Bolivia, Brazil, Colombia, Paraguay, and Peru, a single regulation applies to all regulated providers allowed to hire agents. This includes EMIs that were introduced by laws issued after the agent regulation was already in place (Dias et al. 2015).

a statement of the principal's liability (e.g., for rapid transfer agents in Côte d'Ivoire, banking agents in Tanzania, PSP agents in Rwanda). Other mandatory clauses may address the principal's authority to monitor and inspect the agent (banking agents in India) or the agent's duty to retain pertinent records and make them available for inspection by the regulator (India, Rwanda).

Another common feature in this area is the prohibition of exclusivity clauses in agency agreements. The majority of the 10 countries prohibit agency agreements that bind an agent to a sole principal. Pakistan, Rwanda, and Bangladesh take a slightly different approach, stipulating that an agent *may* serve several institutions, thus leaving open the possibility (at least in principle) that an agent and provider could choose to enter an exclusive agreement. Such regulations are aimed at protecting competition by limiting vertical tie-ups and at promoting access to the services of more than one issuer at the agent point of service.

Most of the sample countries also require providers to facilitate interoperability, including at the level of their agents, which has a similar effect on competition and access. In a few cases (India), by contrast, exclusivity is allowed or even mandated at the subagent or retail outlet level.[42] In Pakistan, the central bank retains the authority to impose limits on agent sharing with the aim of encouraging providers to open new agent locations.[43]

Agency scope

There remains the question of *what* agents may be authorized to do on the principal's behalf. DFS regulatory frameworks identify activities for which the use of agents is *permitted and prohibited.* The range of permitted activities may vary with the type of principal represented (bank or nonbank agent such as a PSP or EMI agent). In Ghana, for example, banks are permitted to deploy agents for a wider range of services—marketing and sale of credit, savings, insurance, and investment products—than are EMIs.

The basic functions that can be outsourced to agents include cash-in and cash-out, payments services, and information collection and document completion for account opening. On this last point, the actual opening of accounts is generally handled by the principal. In Ghana and Pakistan, however, lower-level accounts can be opened at an agent or (in Pakistan) even remotely by phone (with a biometrically verified SIM). The countries studied include some where OTC is prohibited (Bangladesh, Uganda), where it is explicitly permitted (Ghana, Pakistan), and where the regulations are silent.[44] In addition, banking agents can handle regular banking functions, such as disbursing (usually small) loans, accepting deposits, and collecting loan payments, on behalf of the principal bank. In a few cases (Ghana and Bangladesh), they may receive and/or send international remittances. The prohibitions, especially for agents of nonbank issuers, are many and usually include dealing in foreign currency, opening accounts, cashing checks, providing cash advances, and others.

Types of agents

The question of the possible scope of a DFS agency is often answered by setting up rules that differentiate among categories of agents. In the DFS context there are a variety of types of agents serving a wide range of principals. The varieties of agents can be categorized in different ways, including by the type of principal institution they represent (see Box 4).

Agents may, alternatively, be distinguished based on the type of contractual relationship they have with the principal. They can be directly contracted by the principal or subcontracted by another agent who in turn holds a contract with the principal. In the latter case, they are typically referred to as *subagents* and their principals are called *master agents*. In some cases, several levels of outsourcing (creating long principal-agent chains) are permitted, which makes it more difficult for the principal to ensure regulatory compliance and manage risks.

Further, agents can be described as *wholesale or super-agents* if they provide cash management services to other agents who may themselves have a direct agency contract with the principal (and thus are not subagents). Similarly, *agent network managers* can be hired by the principal to provide support services to agents. Agent network managers (e.g., under Ghana's regulations) are concerned with recruitment, training, compliance monitoring, liquidity management, and general support. They are typically not agents themselves (although they could be). The agents they manage are directly contracted by the principal. In some cases (e.g., Selcom in Tanzania), these agent network managers are aggregators, offering facilities such as payment integration services.

42 Mobile money agents have in some instances been allowed to be exclusive. This was formerly the case in Kenya and Uganda. Where exclusivity is not prohibited—as has been the case in several countries such as Tanzania for e-money agents and in Brazil (Dias et al. 2015, p. 25)—one could argue that such an approach is justified on several grounds. Exclusivity, among other things, could help maintain clearer accountability and liability by the principal as compared to nonexclusivity. It also incentivizes providers to expand outreach by recruiting new agents and to be the first to build an agent network.

43 Framework for Branchless Banking Agent Acquisition and Management, sec. 9.9 (b).

44 WAEMU provides for separate authorization of agents for *rapid funds transfer*, i.e., OTC services.

Table 4. Agent regulation overview

	Regulatory approach	Types of agents	Role in account opening (examples)	Types of specialized agents
Bangladesh	Account-based	Banking, MFS	Receive account opening documents.	Not specified.
Côte d'Ivoire	Institution-based	Banking, e-money, rapid transfers	Sign agreements with clients.	Primary (master) agent: contract subagents.
Ghana	Activity-based	Banking, e-money	E-money: Open minimum or medium KYC accounts on behalf of issuer.	Agent network manager for banking and e-money agents: recruitment, training, compliance monitoring, liquidity management.
India	Institution-based	Business correspondent (bank, incl. payments bank)	Identify customers. Process & submit applications.	Not specified.
Kenya	Institution-based	Banking, MFI, PSP	MFI: Collect documents for account opening.	Wholesale agent/wholesale cash merchant: Distribute money to retail agents.
Myanmar	Institution-based	Mobile banking, MFSP	Mobile banking: Cash deposits.	Not specified.
Pakistan	Institution-based	Branchless banking	Open and maintain branchless banking accounts.	Super-agent (established retail outlet or distribution setup); Agent Network Manager/Aggregator: Training and monitoring agents, reporting to financial institutions, liquidity management.
Rwanda	Activity-based	Banking, e-money, PSP	Customer identification (2-factor). Collect account opening info from clients (only if agent registered as company).	Agent network managers/ super-agents: Management and coordination of basic agents' activities.
Tanzania	Account-based for e-money accounts, otherwise institution-based	Banking, e-money, PSP	Banking: Collect documents for loan applications.	Wholesale agent (company): e-money distribution, retail management.
Uganda	Institution-based	Banking, mobile money	Banking: Collect documents and info for account opening.	Not specified.

These diverse types of agents respond to providers' need for a wide range of service points along with mechanisms to support and monitor them. Thus, the use of master agents or agent network managers becomes critical. Using agents properly means identifying, training, monitoring, and managing agents while ensuring their liquidity, risk management, and compliance with regulatory and customer service standards. Providers may outsource some or all these functions to master agents or agent network managers.

In practice, the terms used for the different types of specialized agents—master agents, super agents, agent network managers—are not consistent across countries.[45] (See Table 4 for examples.)

2.3 Agent eligibility and authorization

The next concern that regulation must address is to determine *who is eligible* to become an agent (or a certain type of agent) and what kind of approval

45 Rwanda, e.g., provides for super-agents and basic agents; Ghana authorizes agents and master agents; and Kenya provides for wholesale and retail agents.

(if any) is required by the regulator. The rules seem to vary greatly in the effectiveness of their implementation and the burdens they impose.

Most of the 10 countries require agents to be registered businesses, whether companies or individuals.[46] In several countries, the eligibility standards state that an agent must be an enterprise with its own independent (and viable) line of business. This is clearest in Kenya, where one is prohibited from continuing to provide services as an agent if the separate line of business is not commercially viable.[47]

These kinds of requirements appear designed to mitigate risk—but their cost-effectiveness is not always clear. First, such rules may not be well-targeted. It is worth asking whether someone who has specialized in agency services should be ineligible purely due to failure to meet a registration or "line of business" standard. Second, the burden of these requirements may undercut the objective. Providers sometimes have difficulty recruiting new agents because of such standards. Third, the extent of compliance with these rules is open to question, especially in countries with rapid e-money uptake and thus urgent demand for agents.[48]

A few countries (India, Bangladesh, Ghana) allow individuals to serve as agents if they are educated, or if they have experience or businesses considered relevant (e.g., insurance agents, retired bankers, heads of self-help groups, mobile agents). Qualifications of a potential agent may include having a good credit history, character references, IT capacities, and a minimum level of experience in operating a business—as well as an account in a licensed financial institution.

Policy makers and regulators face a choice between *ex ante* enforcement of eligibility rules (prior approval) or *ex post* (inspection). In some cases, as a first step, general approval for the use of agents or for a network of agents may be required. This may need to be followed by the provider obtaining authorization for individual agents or groups of agents—as is the case for banking agents in Kenya and Uganda (bulk authorization).[49] Different standards may apply to agents of different scale (e.g., master agents and subagents that operate on their behalf) or function (bank versus nonbank agents). Banking agents are most rigorously controlled in WAEMU, where individual agent approval is required along with financial guarantees and other conditions not applied to EMI agents. In Kenya, when PSPs recruit agents, PSPs simply need to notify the central bank 14 days before the commencement of the agent's operation and report basic information periodically.[50] Master agents and agent network managers may be subject to stricter standards, as in Ghana, where providers must apply much more comprehensive due diligence.[51]

Regulations may apply eligibility requirements not only to agents but also to providers themselves when they seek to outsource. Pakistan, for example, requires financial institutions to meet minimum prudential thresholds to contract branchless banking agents.[52]

2.4 Ongoing duties of agents and principals

A DFS provider's use of agents imposes ongoing regulatory obligations on both parties. Among these are the kinds of risk management requirements discussed previously as well as duties

46 Most admit businesses, generally, in addition to specific groups such as MFIs, the Post, or cooperatives. Others (including India, Bangladesh, and Ghana), have a longer list of eligible entities, e.g., retailers, petrol stations, local government offices, nongovernment organizations, and courier services.

47 Guideline on Agent Banking (CBK/PG/15 [Kenya], art. 4.4).

48 The Helix Institute's Agent Network Accelerator Survey, Kenya Country Report 2014 notes that 36 percent of Kenyan agents at that time were dedicated, i.e., did not offer a separate line of business.

49 Guideline on Agent Banking (CBK/PG/15 [Kenya], part II).

50 National Payment System Regulations (Kenya) 2014; CGAP (2015, 15).

51 Bank of Ghana Agent Guidelines (2015), arts. 10, 11, 15.

52 The threshold is moderate, including compliance with minimum capital standards and "fair" CAMEL rating (State Bank of Pakistan, Branchless Banking Regulations, art. 9.2 [2016]).

of disclosure, which is addressed in Section 4.2, as it relates to consumer protection. Other obligations include record-keeping, reporting, and ensuring the certainty and security of transactions.

Security and technology

Regulators are concerned with ensuring the security and accuracy of agent-assisted transactions and the reliability of the technological platform. Requirements in this area overlap with consumer protection (see Section 4.2). In the countries studied, it is mandatory to provide confirmation of transactions to the client (in some cases, including fees). The implication, made explicit in the case of Tanzania (for banking agents), is that a provider or agent must not complete a transaction if a receipt or acknowledgment cannot be generated.

A related rule prohibits agent transactions going forward where there is a communication failure. In Kenya and Rwanda, for example, all transactions must be processed in real time. The regulations in several countries (Côte d'Ivoire and Tanzania) hold the principal issuer responsible for ensuring the reliability and security of their systems, as well as the confidentiality and traceability of transactions.

The countries studied require providers to have approved plans in place for contingency and disaster recovery, including for technology-related interruption of services. In some countries, these plans are to be stipulated in the agency agreement and assessed as part of the licensing and supervision processes.

Reporting and records

Agents are not required to report directly to the regulator. But principals do need to identify their agents to the regulator either by periodic reporting (e.g., monthly in Bangladesh) or by the maintenance of updated rosters (e.g., on the provider's website) with names, addresses, and in some cases (Ghana and Tanzania), geographic information system coordinates.[53] Regulators may also demand aggregate data on clients, transaction value/volume, fraud incidents, consumer complaints, and remedial measures. Pakistan has introduced a web-based agent registry system through which it collects and maintains disaggregated data on individual agents (Dias et al. 2015).[54] Rwanda is in the process of rolling out a data collection system that will pull data directly from the EMI's operational system (Dias and Staschen 2017).[55]

Regulations also impose record-keeping requirements and establish the authority's right to conduct inspections at both the principal and the agent. The provider/principal ensures that the agent keeps necessary records and keeps data from the agents in the principal's own system. Providers must keep records for several years (requirements vary from five to 12 years), and consistent with the regulator's standards for organizing records.[56] Further, in most countries, the regulator has the authority to inspect the premises, books of account, and records—not only of the principal but also of its agents and, in some cases (Myanmar and Ghana), other partners and services providers used in the provision of DFS.

2.5 Summary of experience

The following general patterns emerge from the 10 countries' experience in this area:

- There has been some convergence on the regulation of agents. The principal's liability is a core tenet in all 10 countries. Most regulators have taken a flexible approach as to the kinds of organizations and individuals that can be agents. Further, norms of nonexclusivity and interoperability are prevalent, though there are differences in application.
- Certain divergences remain on the general approach toward agent regulation. While the institution-based

53 For a more detailed description of reporting requirements, see Dias and Staschen (2017).
54 Ghana is in the process of setting up a similar agent registry.
55 Rwanda's new system should help address the common problem of over-counting agents and access points, which can give a misleading picture and hence the proximity that consumers enjoy. E.g., 98 percent of agents are counted twice in Colombia, as each bank reports shared agents as its own (Arabahety 2016). In addition, large numbers of inactive agents are often included in such counts.
56 E.g., in India, agents (business correspondents) that work for multiple institutions must maintain separate data for each of their principals, and avoid commingling data.

approach is still most prevalent (e.g., different treatment of bank and nonbank agents), a few countries follow an account-based approach (rules are defined for certain types of accounts that can be accessed through agents regardless of the issuer) and two countries (Ghana and Rwanda) have implemented an activity-based approach (same rules for same activity). Whereas institution- and account-based approaches might not have posed a problem in the past, trends such as increased sharing of agents and partnerships between banks and nonbanks make these approaches less tenable.

- In general, the countries' regulatory approaches are not fully risk-based or proportionate. This is partly because of the continuing use of institution-based approaches and partly because of differences across countries in support for multiple types of agents, such as simple cash merchants, who present lower risks if operating against a prefunded account and in a real-time environment.

3 Enabler 3. Risk-Based Customer Due Diligence

DFS operate within regulatory contexts shaped by policies on AML/CFT. The challenge for financial inclusion is to ensure proportionate treatment using risk-based frameworks that protect system integrity while imposing the least burden on DFS outreach.

The essential components of the third enabler include the following:

- Adopting the principle of simplified CDD in lower-risk scenarios.
- Translating this principle into risk-based tiers for different kinds of accounts, transactions, clients, and methods of account opening and transacting (remote or in-person).
- Addressing constraints on customer identity documentation by recognizing a wider range of ID types and making use of new methods of identification for lower-risk transactions, which are made possible by advances in ID systems (wider coverage, better accessibility).

3.1 Simplified customer due diligence

AML/CFT rules are held to international standards set by FATF. The FATF Recommendations (2012) and related guidance set forth CDD methods and risk criteria that take financial inclusion into account, allowing for simplified procedures for lower-risk scenarios (FATF 2017) (see Box 5).[57]

The FATF language simply may be incorporated into financial sector regulation, offering providers a basis for adapting their procedures. However, most of the 10 countries translate that guidance into more specific rules that define lower-risk scenarios and the corresponding simplified methods. Providers appear generally reluctant to implement

Box 5. Customer due diligence and the scope for simplification

Standard CDD has four elements, according to the FATF Recommendations (no. 10), and each of the elements can be simplified where risks are assessed as lower (2012, INR 10, para 21):

- Identifying the customer and using independent sources to verify the identity. Simplification can be done by, for example, reducing the extent of ID information required or postponing the verification.
- Identifying the beneficial owner and taking reasonable steps to verify that identity and understand the customer's ownership and control structure (in the case of a legal person). These checks are required to ensure that the account holder and anyone represented by that holder are identified (including any "politically exposed persons"). A simplified process could, for example, use information provided by the customer without verifying it.
- Obtaining information on the purpose and nature of the business relationship between the customer and the financial services provider. Simplified CDD can infer this from the type of transaction or the relationships.
- Conducting ongoing monitoring and due diligence as needed to ensure that all transactions are consistent with the institution's knowledge of the customer, its business and risk profile, and its source of funds. This means keeping the client profile sufficiently up to date to identify anomalous transactions. The degree of monitoring could be reduced based on a reasonable threshold.

57 FATF has published extensively on the risk-based approach and its application, e.g., to the banking sector (FATF 2014), to prepaid cards, to mobile payments and internet-based payment services (FATF 2013), and to money and value-transfer services (FATF 2016).

a risk-based approach without this kind of specific regulation (de Koker and Symington 2011). Thus, while FATF's concept of risk-based CDD does not *require* explicit definitions of risk scenarios and procedural adjustments, such definitions appear to be more effective in ensuring the use of risk-based CDD in practice.

Regulatory provisions on risk-based CDD emphasize the first element of customer identification and verification, which is often called Know Your Customer (KYC). But there are also examples of simplification of the other elements. Pakistan, for example, permits reduced frequency of customer ID updates and less intensive on-going monitoring for accounts with a limited monthly turnover.[58] Bangladesh provides such an allowance for low-risk customers,[59] as does Myanmar (for banks).[60]

3.2 Tiered approaches

A common regulatory approach to risk-based CDD is the definition of risk tiers to which due diligence procedures of varying intensity are applied. This is in line with FATF guidelines that suggest countries should consider such a tiered approach to implement simplified CDD measures in lower-risk scenarios (FATF 2017, para. 74). Such risk tiers are determined by the features of the accounts or transactions permitted, the types of clients, and the modalities of account opening and transacting (e.g., in-person or not). Most of the 10 countries define two or three tiers (e.g., high, medium, and low risk). In some cases, however, the rules are different for DFS (e.g., tiered structures applying only to transactions via agents and/or only to EMIs) as compared to general rules applying to bank accounts and/or branch-based transactions. One reason for this is that DFS rules were introduced more recently and with a clear focus on reaching previously unserved customers, while legacy CDD rules for banks continue to coexist (see Table 5).

Account, transaction, and client restrictions

Several countries define at least one differentiated type of account with lower CDD requirements.[61] These accounts are subject to lower balance and transaction limits than regular or enhanced CDD (i.e., higher risk) accounts. Other restrictions may apply (Ghana), such as prohibiting a client from having more than one such account or considering the account dormant after 12 months of inactivity. In like manner, one-off transactions (e.g., OTC transfers) may have lower ceilings to qualify for simplified CDD (Ghana and Pakistan). A further complication arises in some countries (Ghana, Myanmar, Tanzania) where tiered KYC is available only to EMIs or to mobile money providers. In Pakistan, only branchless banking accounts are subject to the tiered structure.

In several cases, e-money accounts have three versions or tiers:

- A basic account with minimal opening requirements and correspondingly low ceilings for transactions.
- A mid-range account allowing for bigger transactions and more stringent requirements, but less than a full KYC procedure.
- A higher-limit, full-KYC account. This tier may include special accounts designed specifically for businesses. The business accounts have much higher limits than individual accounts.[62]

Differentiated KYC requirements for businesses provide higher quantitative transaction ceilings in exchange for more rigorous procedures for account opening. Such business accounts are mostly used by agents and merchants, who regularly handle larger amounts of cash and higher transaction volumes than the regular clientele. Account opening in such

58 State Bank of Pakistan, AML/CFT Guidelines on Risk Based Approach for Banks & DFIs (updated 31 March 2015), arts. 7–8. This applied to accounts with a monthly turnover up to PKR 25,000 (US$226) such as basic bank accounts and Level 0 branchless banking accounts until monthly limits were raised to PKR 40,000 (US$328) in 2016.

59 Bangladesh Bank (BFIU), Money Laundering and Terrorist Financing Risk Assessment Guidelines for Banking Sector, sec. 6.3, 6.11.

60 Central Bank of Myanmar Directive No. 21 /2015, arts.14, 16, 22.

61 E.g., Ghana, India, Tanzania, Myanmar, and Pakistan.

62 E.g., Myanmar sets a daily MFS transaction limit for businesses of 1 million kyats (US$723) compared to 50,000 kyats (US$36) for the lowest individual tier, a monthly transaction limit of 50 million kyats (US$36,000) compared to 1 million for the lowest tier, and a balance limit of 10 million (US$7,223) compared to 200,000 kyats (US$145) for the lowest tier (Central Bank of Myanmar, Regulation on Mobile Financial Services [FIL/R/01/03-2016], sec.17). This tiering scheme applies to EMIs, but not to banks that provide MFS.

Table 5. Selected KYC requirements for e-money accounts

CDD/KYC coverage and tiers	Quantitative limits for low KYC	Illustrative KYC requirements
Ghana		
Tiered KYC schemes apply only to EMIs. E-money KYC tiers: minimum, medium, enhanced.	Limits for minimum KYC: • Maximum balance: GHC 1000 (US$226) • Daily transactions: GHC 300 (US$68) • Aggregate monthly transactions: GHC 3000 (US$677)	• Minimum KYC: Any type of photo identification • Medium KYC: Official ID documentation listed as acceptable[a] • Enhanced KYC: Same requirements as that of opening bank account.
Myanmar		
MFSP covered. Three levels of MFS accounts: Level 1 (lowest level) and Level 2 for individuals; Level 3 for legal entities.	Limits for level 1 accounts: • Transactions: MMK 50,000 (US$37) per day; MMK 1 million (US$736) per month. • Maximum balance: MMK 200,000 (US$147)	• Level 1: National ID document. • Level 2: National ID document and SIM registration. • Other KYC requirements: Permanent and mailing address, date of birth, nationality.
Pakistan		
Applicable to branchless banking accounts (being full banking accounts). Three levels of accounts: Level 0 (lowest), Level 1, and Level 2.	Limits for Level 0: • Transactions: PKR 25,000 (US$226) per day, PKR 40,000 (US$362) per month, and PKR 200,000 (US$1,811) per year. • Maximum balance: PKR 200,000 (US$1,811)	Level 0 requires: • Capturing the image of the customer national ID document • A digital photo of the customer • Verification of customer data against NADRA system. Account opening can be through physical or digital means.
Rwanda		
All EMIs covered. Tiers: Individuals, individual customers with higher levels, legal entities, basic agents, etc.	Limits for Tier 1 (Individuals): • Single transaction: RWF 500,000 (US$592)	Customers can be electronically registered or follow e-KYC procedures.
Tanzania		
Tiered KYC applies to mobile money issuers. Tiers: Electronically registered (lowest level); electronically and physically registered; SME accounts. No tiering for card-based e-money.	Limits for electronically registered mobile money accounts: • Single transaction limit = TZS 1 million (US$446) • Maximum balance = TZS 2 million (US$892) (stated as "daily" balance, i.e., average not to exceed threshold)	Alternative IDs: Employment ID, social security ID, or a letter from the ward/village executive.

a. National ID, voter identification, driver's license, passport, and other government documents, such as the National Health Insurance Scheme identification.

cases may require the client to visit a bank branch, to provide additional documents such as a business registration, and to comply with the full KYC procedure (as required for regular bank accounts).[63] For example, Tanzania provides four risk-based KYC tiers for EMIs, including one for retail agents and one for wholesale agents.[64] Similarly, the KYC rules applied to e-money in Ghana provide higher ceilings for agents and separate treatment for merchant accounts.

In India, CDD requirements for payments banks are the same as for banks. Thus, uniform standards on account opening apply across institutions, including simplified CDD for opening small-value accounts. Also, India classifies certain customers as low risk

63 In Myanmar, this highest MFS tier requires a registration certificate, which can be a problem for agents that are informal businesses.

64 Retail agents require only the basic documents (e.g., business registration and tax ID number) required to conduct commercial activities, while wholesale agents must be registered corporates and are permitted to distribute e-money and manage retail agents (Electronic Money Regulations, 2015 [Tanzania], Third Schedule). This tiering scheme applies only to mobile money. For card-based e-money, the general rules contained in the AML/CFT legislation (2013) and regulations (2015) apply.

(thus eligible for simplified CDD), including members of self-help groups and foreign students.[65] Where simplified CDD applies, customers may be issued closed and semi-closed loop PPIs. However, when issuing e-money (open-loop PPIs),[66] banks must apply standard CDD, and the simplified CDD rules provided in the banking regulations do not apply.[67]

Face-to-face versus remote transactions

In most DFS models it is essential that customers have the option to be identified either at an agent or remotely (electronically). Accordingly, another basis on which to define tiered KYC treatment is whether the business is done *in person* between the provider and the client. Where accounts are opened or transactions are carried out through an agent, CDD performed by such agents is treated as if conducted by the principal, and the ultimate responsibility rests with the principal (FATF 2017, para 118f). The provider must properly analyze the capacity of its agent and supervise the agent's application of the CDD rules and procedures—but those rules and procedures do not change. The standards to be used in overseeing third-party CDD are somewhat demanding, since money laundering is a high-priority area of risk. Thus, for example, banks in India and MMSPs in Uganda must ensure that their agents are licensed or registered, and that they have AML/CFT policies and systems in place that are effectively implemented and monitored and are regularly updated.[68] In any case, the principal remains liable for the proper completion of KYC and the agent performs only a clerical or conduit rule.

FATF considers *nonface-to-face scenarios*—accounts opened electronically *without* visiting an agent—as potentially posing higher risks.[69] Some countries have special KYC rules for accounts opened remotely. Tanzania, for example, provides for differentiated accounts based on whether the accounts are registered physically or electronically by mobile phone. These accounts have tiered transaction limits along with differentiated CDD/KYC requirements, and they impose special risk management (governance and MIS) responsibilities on the provider.[70] Also, Pakistan recently permitted lower-tier mobile wallets to be opened remotely from the customer's mobile handset, taking advantage of the fact that all SIM cards in Pakistan are now biometrically verified against the central ID database.[71] As a result, account openings have sharply increased (Rashid and Staschen 2017).

3.3 Loosening the ID constraint: Risk-based rules and evolving ID systems

A major contextual factor in CDD is the development of national ID documentation and verification systems. ID systems need to integrate all relevant information so that each ID document is matched with a single client and with the relevant account. Until recently in most of the 10 countries, limited availability of official ID documents seriously constrained financial services outreach, and therefore—in line with FATF guidelines—policies were adopted to adjust ID requirements on a risk basis. The reasoning was that widening the range of acceptable ID documents should facilitate access to financial services.

The countries studied include several that recognize alternative forms of ID in lower-risk settings, and several others that do not. India is an example of the former. Where India's regulations allow simplified measures for verification of customer identity, alternative documentation may be accepted in lieu of a national ID card, including photo ID cards issued by banks (public and private) and by central regulatory authorities. Another alternative is a letter

65 RBI Master Direction—Know Your Customer (KYC) Direction, 2016, DBR.AML.BC.No.81/14.01.001/2015-16, sec. 3, 16, 22–24; RBI Master Circular—Policy Guidelines on Issuance and Operation of Pre-paid Payment Instruments in India, DPSS.CO.PD.PPI. No.01/02.14.006/2016-17, sec. 6–7.

66 Only open-loop instruments have the full functionality of e-money and, thus, they fall under our definition of DFS.

67 Policy Guidelines on Issuance and Operation of Pre-Paid Payment Instruments in India, 2016, DPSS.CO.PD.PPI.No.01/02.14.006/2016-17, sec. 7.3.

68 An agent completing documents and conducting CDD on behalf of a principal is not the same as opening an account for the client at the principal institution—an authority that often cannot be delegated.

69 FATF 2012, INR 10, para 15; and FATF 2013, ch. IV, para 40, 69.

70 Bank of Tanzania, Electronic Money Regulations, 2015, Third Schedule, Form F.

71 A Level 1 account, which may be opened remotely with a biometric SIM card, has transaction and balance ceilings that are two to four times higher than the Level 0 limits (SBP, Branchless Banking Regulations 2016, art. 4.1)—reflecting increased confidence in the biometric system.

issued by a gazetted officer, with a duly attested photograph of the customer. These officially valid documents are sufficient for small-value accounts and some semi-closed loop PPIs. But open-loop instruments equivalent to e-money require full KYC measures.[72] In Ghana, in addition to risk-tiered ID requirements for e-money accounts, OTC clients are subject to reduced quantitative ceilings if they do not have existing e-money accounts or cannot present "acceptable" ID documentation (as required for medium KYC measures).[73]

Other countries (Myanmar, Tanzania, Côte d'Ivoire) recognize only a few forms of official identification for KYC purposes, such as the national ID document, passport, and driver's license. In Rwanda, EMIs must identify their clients by means of a national ID document or passport, which is verified through the national ID database—the only stated exception is the identification of a minor by her/his duly identified parent.[74] But limitations on acceptable ID documentation need not eliminate risk-tiering. In Myanmar, ID requirements are graduated, but acceptable ID documentation is limited for all tiers to the national ID document, driver's license, passport, or SIM registration. In CDD as in other domains discussed in this paper, the extent to which requirements are followed in practice is open to question.[75] Enforcement capacity should be an important element to consider when determining CDD rules.

The quality and ubiquity of the ID system is also important. Governments are increasingly investing in universal ID documents, databases, and biometrics as the practice of checking databases (eKYC) rather than hardcopy documents grows (see Box 6). Some new systems (India and Pakistan) cover the great majority of the population and are approaching universal coverage. In Uganda, the enhancement of ID systems has coincided with a toughening of ID requirements for KYC. In 2013, the Mobile Financial Services Guidelines allowed for seven different types of ID documentation. However, this was reduced to two (the national ID document and passports for foreigners) by the Ugandan telecoms regulator in early 2017 because of security concerns and the wider availability of ID documentation.[76] Several challenges remain with the reliance on universal biometric identification, including the reach of the technology to unbanked populations and underserved areas, the accessibility of ID databases to financial services providers, and the costs of using these systems (unless provided at very low cost, as in India).

The benefits of advances in ID systems may obviate the need to accept a broad range of ID documentation, but not necessarily the need for tiered account structures. The latter are still required in many countries because of other requirements applicable to standard CDD, such as residential address verification.

Box 6. eKYC in India

India has established a KYC compliance option for use in electronic account opening: e-KYC. This service, provided by the Unique Identification Authority of India (UIDAI), uses biometric authentication to confirm the customer's identity. Under e-KYC, the customer's identity is verified when the UIDAI confirms that the biometric data provided by the customer match the biometric data recorded against that person's name. The customer may consent to the ID authority electronically transferring the data, including the individual's name, age, gender, and photograph, to the financial institutions and their agents (business correspondents). The AML/CFT Rules stipulate that e-KYC is to be accepted as a valid KYC process, provided that the financial institutions and their agents obtain express authorization from the customer for release of her or his ID information.[a]

a. Two recent events—judicial recognition of a constitutional right to privacy and a major data breach—are expected to usher in limits to data collection and access through the UIDAI (Aadhaar) system. RBI Master Direction, KYC (2016), sec. 17.

72 Small-value accounts have a balance ceiling of Rs. 50,000 (US$774). The bank accounts thus established can be used for PPIs, but only of the semi-closed-loop type (i.e., not equivalent to e-money) (RBI Master Direction, KYC [2016], sec. 3, 16, 22–24; RBI Master Circular, Pre-paid Payment Instruments [2016], sec. 6–7).

73 Bank of Ghana, Guidelines for E-Money Issuers in Ghana (2015), sec. 15.

74 Otherwise, reporting entities for AML/CFT purposes (e.g., regulated institutions and public companies) may use a simplified CDD process for customers in low-risk categories. Reglement n° 08/2016 DU 01 /12 / 2016 Régissant Les Émetteurs de Monnaie Électronique, art. 11.

75 In practice, many clients (e.g., in Tanzania) have managed to open e-money accounts with virtually any document.

76 The switch relates to MFS, thus affecting DFS, but not other financial services. The deadline was later extended to August 2017 to give providers sufficient time to re-register clients. Many people still needed ID documents at the time. Allowance was made for refugees, who could use an official ID from the Office of the Prime Minister.

3.4 Summary of experience

The following general patterns emerge from the countries' experience with risk-based CDD:

- The countries simplify CDD for lower-risk transactions, per FATF guidance, but vary in their approaches. The most common approach is to implement tiered CDD/KYC requirements for different types and scales of clients, accounts, and transactions. However, in some countries the tiered account structure applies only to a special type of DFS account (e.g., branchless banking accounts in Pakistan), which risks creating an uneven playing field between different types of channels or accounts used.
- Several countries have translated FATF standards on risk-based CDD into specific regulatory requirements and tiers. Others have simply incorporated the FATF standards into regulation without providing more guidance. In the latter situation, providers sometimes hesitate to use the allowed flexibility, and instead follow a risk-averse, cautious approach.
- While there has been a trend of increasing the range of accepted ID documentation for lower-tier accounts to reduce barriers for people without identification, the extent to which this wider acceptance is still needed depends on the quality and ubiquity of the ID system and the accessibility of ID databases.
- The countries diverge notably in their accommodation of account opening at agents or remotely/electronically (nonface-to-face), both of which are subject to specific FATF guidance. A few countries make use of advanced biometric ID systems to allow for e-KYC (India and Pakistan stand out in this regard) and have thus been able to make remote account opening much simpler despite the potentially higher AML/CFT risks.

4 Enabler 4: Consumer protection

Effective consumer protection is key to the credibility of DFS as a pillar of inclusive finance. Regardless of whether FCP must be fully in place before DFS can spread, it is a necessary ingredient in a sustainable, well-governed market.

Three characteristics of DFS models affect consumer risks (McKee, Kaffenberger, and Zimmerman 2015). First, the use of agents provides a first line of defense in case any problems occur. But they sometimes misinform or defraud customers. Second, technological interfaces make convenient access possible. Yet this comes at the cost of increasing dependence on their reliability and on users' understanding of technology—factors that can pose special challenges for less experienced customers. Third, longer and more complex value chains increase the number of entities involved in serving customers. This can create confusion about who is ultimately accountable and where customers can seek recourse. These factors underline the importance of consumer protection in DFS markets.

In this section, we cover the following essential components of the fourth enabler:

- Consistent, comprehensive, targeted consumer protection rules for DFS. Frequently, only general or patchwork rules exist without clear adaptation to DFS needs.
- Rules on transparency and market conduct in providers'—and their agents'—dealings with customers.
- Requirements for providers to establish systems for handling customer complaints.
- Standards of service availability and/or digital platform reliability that balance protection of customers and irrevocability of transactions.

4.1 Scope and consistency of consumer protection rules

The complexity of DFS poses a challenge for financial consumer protection. Several bodies of law and regulation intersect. But for FCP to be effective for DFS clients, the legal/regulatory framework must cover all relevant providers, channels, and products—and do so consistently.

Although the countries in our study have not achieved this goal yet, they are making inroads. To address the priority of getting the DFS market on its feet, regulators in these countries have been focusing on issues related to the first three enablers. Meanwhile, regulators have relied on existing FCP norms. Typically, limited (and often belated) attention has been given to FCP issues specific to DFS. Where

Table 6. Consumer protections in DFS

Rules, coverage	Disclosure rules: Key terms, forms	Complaints
Bangladesh		
General and institution-specific: Banks and regulated financial institutions, PSPs, electronic fund transfers (EFTs), agents	- Customers must be notified of charges and fees, changes of terms and conditions, value-added services - Transparency in all terms and conditions relating to all banking products and services - All regulated financial institutions must have a Customer Charter in each branch - Dispute resolution mechanisms should be part of the contract agreement	- Banks/financial institutions and PSPs shall establish formalized complaint procedures; the same applies for EFTs - All financial institutions: Zonal customer service and complaints management cells deal with all complaints received directly from customers - Customer can register complaint with central bank
Ghana		
Activity-specific rules: EMIs and agents	- Display fees and service charges - Bank of Ghana provides standard summary sheet - Risk information provided to customers - Specify minimum contract content and written agreement	- EMI to have a functional dispute and complaints resolution desk - Right of appeal to Bank of Ghana - 40 days to file complaint; resolution within 5 days
India		
Institution-specific rules: Banks, payment banks, PPI issuers, mobile banking, agents (business correspondents)	- Interest rates, fees, and charges to be disclosed via website, branches, help-line or help desk - Contracts should be easily understood; product price, risks, terms, and conditions to be clearly disclosed	- Grievance machinery required for banks, payment banks, PPI issuers - Option to appeal to Banking Ombudsman
Pakistan		
Activity- and institution-specific: General rules for all banks (commercial, Islamic, and microfinance banks) and specific rules for banks offering branchless banking; agents	- Banks required to publish their schedule of charges for branchless banking activities quarterly - All contracts shall clearly specify that the bank is responsible for agents' acts or omissions	- Banks must have a consumer redress cell and centralized complaint management system - Receiving and processing a complaint should not take more than 7–10 days (depending on its nature)
Rwanda		
General and institution-specific: EFT providers, EMIs, PSPs, banks and other financial institutions, agents	- Institutions shall define standards for responsible pricing, transparency; disclosure is duty of financial institution and agent - EMI must submit a copy of the standard customer service agreement to the National Bank of Rwanda	- Financial institutions, EFT providers, PSPs, and EMIs to have complaint procedures - Right of appeal to senior management of the institution or the National Bank of Rwanda, or other body authorized.
Tanzania		
Institution-specific rules: PSPs, agents	- Full disclosure of relevant information such as pricing, charges, and fees - Terms and conditions should be fair, legible, and understood by the client	- PSP to establish consumer redress plan with adequate resources - Appeal to competition commission or communication authority - Redress within a reasonable time and no later than 30 days
Uganda		
General rules: All regulated financial institutions and their agents Specific rules for mobile money providers	- Fees, charges, penalties, and any other consumer liability or obligation to be disclosed - Customers should be able to access fees through their phones - Written contract is mandated	- Mobile money providers: Effective procedures to be in place - Banks to train agents in complaint handling - Response within 60 days

such rules have been adopted, they usually have been activity- or institution-specific rather than comprehensive and uniform. Despite this, the majority of DFS markets in the countries studied have thrived. Our assumption in presenting FCP as an enabler is that, as in other financial services markets, the lack of effective consumer protections poses significant risks to vulnerable consumers as well as to the medium- to long-term stability and integrity of the DFS market.

FCP rules relevant for DFS may be embedded in general consumer laws, FCP legislation or guidelines, banking regulations, or regulations on payments or e-money. The result tends to be an uneven patchwork of regulation. (See Table 6 for an overview of DFS consumer protection frameworks.)

General FCP rules are set in banking laws and regulations in several of the countries studied. These apply in some form (that may not always be clear) to DFS providers that are licensed or authorized by the banking regulator or that handle banking products. Usually, there are also specific rules by institution or function, such as those applying to EMIs or the use of agents. For example, Uganda applies its Financial Consumer Protection Guidelines to all types of regulated financial services providers and their agents, and additional FCP provisions are incorporated into its Mobile Money Guidelines. Bangladesh takes a similar approach, providing general guidelines for all regulated financial institutions and more specific rules for MFS.

In other cases, there is no comprehensive FCP framework. Kenya, for example, has incorporated consumer guidelines in the prudential standards for banks, but these do not apply to PSPs. Rwanda does not have a general FCP law, but DFS-specific FCP rules are incorporated in the regulations on EMIs (2016). Similarly, in Tanzania, there is no FCP regulatory framework that covers the whole financial sector, but specific rules are included in the National Payments System Act and in regulations on e-money (2015) and agent banking (2017). Côte d'Ivoire and Ghana follow a similar fragmented approach (see Box 7).

Box 7. The lag between DFS development and FCP reform

The speed of DFS development, along with reforms to the first three enablers, tends to leave in its wake a range of "catch-up" work to fill in and harmonize FCP standards. In Côte d'Ivoire, for example, disparate consumer protection rules are embedded in banking, microfinance, payments, e-money, and e-commerce legislation.[a] The same agent may handle mobile money accounts (for bank and nonbank issuers), bill payments (for PSPs), and OTC transfers (for banks)—each of which is subject to different FCP rules.

Similar issues arise in Ghana, where a comprehensive framework for consumer recourse applies to all financial services providers (including EMIs).[b] But the framework for disclosure is more fragmented, with a specific regulation on credit products (other than credit cards)[c] and disclosure provisions included in the e-money guidelines (but no rules specified for savings products). Protections against error and fraud in payments services are insufficient. There is a significant push underway in Ghana to address these issues, and both WAEMU and Côte d'Ivoire are reforming their FCP framework.

a. The financial services regulations are issued by WAEMU, which is also encouraging member countries to set up financial sector ombudsman institutions. See Meagher (2017).
b. The Consumer Recourse Mechanism Guidelines for Financial Service Providers (2017).
c. The Disclosure and Product Transparency Rules for Credit Products and Services (2017).

Separate FCP rules for different providers or services may produce gaps, loopholes, and regulatory arbitrage. This situation may pose less of a risk in markets where banks dominate the DFS sector. (However, this approach may not be preferred for other reasons). India, for example, has a consumer charter that states broad FCP principles that apply to the banking sector, including payments banks.[77] In general, however, there is a clear case for a harmonized approach to defining FCP rules for DFS. The first step in achieving this is to ensure that the financial regulator exercises authority over FCP. A second goal is to adapt general FCP standards to the specific needs of DFS customers and ensure that all types of providers and channels are covered. It is also critical to require, as many of the 10 countries do, that financial services providers ensure compliance with FCP standards when they deliver their services through agents.

77 The Charter of Customer Rights provides model principles to be incorporated by banks into their board-approved policies and monitored by the central bank (https://rbidocs.rbi.org.in/rdocs/content/pdfs/CCSR03122014_1.pdf). The Charter applies to payments banks in the absence of specific regulatory provisions for the latter.

FCP rules are mostly concerned with transparency, recourse and complaints handling, and service delivery standards. Each of these will be discussed in turn. As discussed in Section 1, fund safeguarding rules are another important measure to protect customers.

4.2 Transparency

Transparency rules relate to the disclosure of terms, use (and content) of consumer agreements, and application of these standards at points of service, including agents.

Disclosure includes general information about services and products, and specific information about individual transactions. These requirements appear in regulations specific to payment services and e-money/mobile money—and in most cases, they also appear in general FCP rules.

The countries studied require providers to post general information on products, including fees, commissions, and other costs. Several countries (Ghana, Kenya, Pakistan) require this information to be displayed physically in main offices and at branches and agent locations. Alternatively (or additionally), the rules may require such information to be published through widely used media such as the internet or newspapers with broad circulation. Internet disclosure, for example, is required in India and Bangladesh.[78] While this will become more relevant with increased smartphone adoption, many consumers either (*i*) are unable to access terms posted on the web through their mobile or computers or (*ii*) find it inconvenient to do so (because they would have to switch to another device to find the information). Providing summary terms through commonly used channels such as SMS would address the latter point (Mazer and Fiorillo 2015).

In addition, some of the countries studied require providers to take positive steps to ensure that customers are informed of specific terms and conditions. Thus, in Kenya and Tanzania, the provider has an affirmative duty to notify the customer of the terms of an impending transaction.[79] Kenya reinforced this duty in 2016, when its Competition Authority ruled that all financial services providers that use digital channels must present consumers full information on costs, before they use the service, on the same screen on which the consumer is transacting (Mazer 2016). Uganda requires providers to disclose charges to clients via mobile phone (without specifying how this would be done on a feature phone), and to provide a copy of the agreement being entered at the time a mobile money account is opened.[80] Post-transaction notifications may also be mandated. Several countries (Ghana, Uganda, Myanmar) require the financial services provider or its agent to provide a confirmation notice to clients for each transaction. These must include information such as the type and amount of the transaction, the fees charged, the transaction reference, and details of the recipient of an outbound transfer or the sender of an inbound transfer.

A minority of the 10 countries (Uganda and Ghana) require providers to explain key terms and conditions to the client before the client signs a contract.[81] In Côte d'Ivoire, WAEMU regulations require that the conditions for the use of payment instruments and accounts be clearly explained to the customer at the time the account is opened, and that they also be incorporated into the agreement.[82]

DFS regulations in most of the countries studied do not stipulate a standard disclosure format. An exception is the Bank of Ghana's issuance of a standard summary sheet for use in disclosure of e-money account terms. A related requirement has to do with the predictability of terms and conditions, including charges. Some of the countries address this in regulation—Uganda, for example, requires a minimum of 30 days' notice of any changes.[83]

Often, the minimum content of general disclosure is defined. Typically, this includes at least a list of

78 India: Policy Guidelines on Operation of Prepaid Payment Instruments, sec. 14; Model Customer Rights Policy, art 2; Business Correspondent Guidelines, art. 9. Bangladesh: Guidelines for Consumer Services and Complaint Management, arts. 2.05 and 2.09.
79 Kenya: National Payment System Regulation 2014, art. 37. Tanzania: National Payment System Act 2015, art. 51; Electronic Money Regulations 2015, art.44.
80 Mobile Money Guidelines, Part II. 12.b.
81 Uganda: Mobile Money Guidelines, Part II. 12.b. Ghana: E-money Guidelines sec. VI.27
82 Payments Regulation 2002, art. 15. Côte d'Ivoire's national E-Commerce Law (2013) provides standards on advertising, offers, contract provisions, transparency of prices, and disclosure of identifying information on the seller of goods and services.
83 Mobile Money Guidelines, Part II. 12.b.

fees and charges, but it may also include other information such as the principal's liability related to the service (Pakistan), the terms and conditions of the service (India and Tanzania), the customer charter (Bangladesh), and general information on the risks of products and services (Ghana and India).

Most of the 10 countries studied apply some form of contract standards to DFS providers. Several require a written contract (which may be electronic, e.g., in Côte d'Ivoire, Ghana, and Myanmar), and some also mandate (or prohibit) certain contractual provisions. There are a few countries (including India and Tanzania) that require contracts to be in clear, simple language. In a few other countries, the customer must be given a copy of the draft contract to review (Côte d'Ivoire) or a copy of the signed contract to keep (Uganda). Standard customer agreements may need regulatory approval (Rwanda), although this does not appear to be formally required in most countries.

All the countries studied have rules on the display of the agent's identification, name (and often the phone number) of the principal, and charges and fees for different products and services. Most countries forbid the agent to alter the principal's fee schedule or to charge additional fees, and many require agents to post written notice that they are not allowed to charge extra fees. Ghana and Uganda, moreover, expressly prohibit the agents' conducting transactions on behalf of the client (in effect, representing both sides of the transaction) and require agents to post a statement to that effect.[84] In some cases, agents must post information on where to file complaints (see Section 4.3).

Although this analysis focuses on the foundations of FCP in the DFS field, it is clear that regulations on transparency also touch on "next generation" issues of market conduct—for example, requiring prior disclosure of certain actions. Two further aspects of market conduct are nevertheless worth mentioning here, given their importance for FCP and the overall credibility of DFS: data protection and fraud mitigation rules (see Box 8).

4.3 Customer recourse and complaints handling

Increasingly, financial sector regulators are requiring providers to establish a mechanism for receipt and handling of customer complaints. All 10 countries studied incorporate this principle into regulation and apply it in some form to DFS. As with other FCP components, this one is covered in different legislative texts, whether on banking, e-money, payments, or consumer protection. The treatment of this issue appears consistent across most of the 10 countries studied, but the potential for gaps and conflicts does arise. WAEMU, for example, has such a provision in its e-money regulation but not in its banking or payments legislation.[85]

Box 8. Protecting client data and controlling fraud

Data protection and fraud mitigation could be considered "next generation" FCP issues, but they are becoming increasingly salient as DFS markets develop. In both areas, controls are being developed, but are often not (yet) consistent or comprehensive.

Collection, storage, and analysis of client data are critical to the evolution of DFS models, especially those involving credit. Most countries require financial services providers to keep client information confidential and, in some cases, to ensure that their agents do so as well. Uganda, for example, requires the provider to disclose to the client (before entering into the agreement) the conditions under which client data are kept Some countries, but not all, require prior customer consent for the use of such data. Recent breaches of financial data security raise questions as to how much confidence should be placed in the protections adopted.

DFS regulation must address DFS's susceptibilities to fraud. Providers are generally held liable for loss or harm from fraud (unless due to the negligence of the customer), and some countries require active steps to mitigate fraud. Bangladesh, for example, shields customers from liability for losses caused by the fraud or negligence of PSP officers or agents, companies involved in networking arrangements, and merchants linked to the card or other communication system. WAEMU requires that such a liability provision be written into an e-money account agreement. In Pakistan, branchless banking providers must institute customer awareness programs about fraud, and prevention must include the blacklisting of agents that have been involved in fraud.

84 Ghana: E-money Guidelines VI.27, Agent Guidelines V.21 and 22. Uganda: Mobile Money Guidelines, Part II. 12.a and 12.b.

85 WAEMU member countries such as Côte d'Ivoire are committed to establishing comprehensive financial ombudsman institutions based on a regional model—a step in the direction of harmonization across the financial sector.

The content of regulations dealing with complaints varies. Several countries (India, Myanmar, Kenya, Tanzania) require providers to have effective or adequate complaint mechanisms. Many specify that the procedures should be easy to use and the information for customers easy to understand. Most of the countries require DFS providers to accept complaints in person, on the phone, or by email—and to provide customers with the appropriate contact information. WAEMU regulations state that complaints systems must be accessible through multiple communication channels—to both customers and merchants/payees.[86] Given the importance of agents for customer-facing interaction, most of the countries direct agents to provide information about complaints handling. Ideally, consumers should be able to access the redress system through a toll-free phone number, in person, and by written communication, as well as through the channels available for the product in question (e.g., SMS, USSD, and web).

The internal details of how the complaints unit responds to complaints received are not addressed by regulation in most of the 10 countries studied (except in Ghana and India). In most of the countries, the regulator has fixed a maximum turnaround deadline for provider responses in each stage of the complaint process. In Ghana and Tanzania, complaints must be tracked, with receipts (complete with reference numbers) issued to the complainant.[87]

In addition, all 10 countries designate an appeal route for complainants, either to the financial regulator (the majority), to the competition or telecom regulators (sometimes as an alternative to the financial regulator, as in Tanzania and Rwanda), or to an ombudsman.[88] India adopted a Banking Ombudsman Scheme (2006), under which complaints and appeals are received. Pakistan did so as well, but its scheme covers only microfinance and Islamic banks. An ombudsman scheme is also being set up in WAEMU (where national financial ombudsman institutions are called *observatoires*).

Most countries require providers to keep track of complaints, retain complaints documentation for a minimum period (often six years, as in Ghana), and report data on complaints and resolutions to the regulatory authority.

4.4 Service delivery standards

DFS operates on the premise that access to digital connections and transaction services should be continuous and largely free of interruption. Thus, a majority of the 10 countries studied have a general requirement of service availability. Only a few countries specify a threshold—for example, Ghana requires EMIs to ensure 99.5 percent service availability, with any disruption (actual or anticipated) promptly communicated to customers, while Uganda sets a floor of 95 percent system uptime.[89] Côte d'Ivoire and Pakistan have a general requirement of consistent availability. There is little evidence as to how these requirements have been implemented and enforced in practice.

Regulators wish to ensure speed and reliability. Thus, several countries require providers to have a digital platform that meets minimum quality and security standards. Rwanda, for example, expressly states the provider's liability for any damages suffered by a consumer due to the provider's failure to comply with reliability standards. Similarly, in Bangladesh, a PSP is liable to its customer for a loss caused by the failure of an electronic funds transfer (EFT) system to complete a transaction accepted by a terminal in accordance with the customer's instruction. Kenya exempts the provider from liability for nonexecution of payments in limited circumstances and, otherwise, requires it to correct any such failure without delay.[90] Such provisions are typically found in regulations on payments or on electronic transactions/EFT.

DFS regulation must balance the need for certainty—irrevocability—in transactions against the need to allow for correction of mistaken or unauthorized transactions. A component of this is for providers to ensure speedy resolution of such mistakes (ideally before recipients withdraw funds) by directing queries to a call center team dedicated to this task.

86 This requirement is stated in the BCEAO e-money instruction (art. 30), but not in the rules on OTC transfers.
87 Ghana: E-Money Guidelines VI.27. Tanzania: Mobile Banking Transactions, Annex III.
88 In addition, the courts might be another option for appeals, but their usefulness and effectiveness to the consumer varies widely.
89 Ghana: E-money Guidelines VI.27; Uganda: Mobile Money Guidelines, Part II. 6.a.iv.
90 Rwanda: Electronic Transactions Law. Art. 51. Bangladesh: Regulations on Electronic Fund Transfer 2014. Arts. 5, 8–12. Kenya: National Payment System Regulation 2014. Part II.15, 28

A majority of the 10 counties studied have regulatory provisions in this area. In some cases (Myanmar), providers have a general duty to inform customers of the risks of mistake or loss, and to notify them of their rights and responsibilities. In other countries, the rules specify how and under what conditions customers may demand the revocation of a transaction. For example, in India, banks that offer mobile banking services must notify customers of the timeframe and the circumstances in which any stop-payment instructions can be accepted. Kenya has a similar rule for PSPs that provides that a transfer can be revoked only in line with the dispute resolution protocols formally established by the PSP. (Bangladesh follows a comparable approach.) Pakistan requires these issues to be stated in the customer agreement, along with the contact information for customers to report unauthorized transfers. In case of dispute, both Pakistan and Bangladesh place the burden of proof on the provider to show that a disputed transfer was authorized by the customer.

In the countries studied, regulators have established that digital payments are irrevocable unless the receiving party consents to the return of the money. Irrevocability sometimes depends on the availability of a validation protocol that allows senders to confirm the recipient before sending a transfer. Clear prior disclosure of the parties' rights and responsibilities is critical in any case.

4.5 Summary of experience

The following general patterns emerge from the 10 countries' experience in this area:

- Convergence exists on regulations governing matters such as required disclosures, complaint handling, and irrevocability of transactions, although details vary and there is still substantial room for adopting international standards or good practices from other countries.
- Remaining areas of divergence exist with respect to establishing standard disclosure formats and financial ombudsman institutions.
- Piecemeal regulatory development produces inefficiencies and other challenges. Most countries have institution- or product-specific FCP rules rather than comprehensive rules. The framework of rules ideally should cover all relevant channels and providers in a consistent manner. DFS should be subject to general FCP rules and more specific rules targeted to DFS (e.g., e-money, payments, delivery via agents). To date, the countries studied have fallen short of this standard.

Conclusion

We have analyzed how the countries in the study have addressed the basic enablers in their regulatory frameworks for DFS. What are the lessons of their experience?

The importance of the four basic regulatory enablers is consistently established in research and policy discussions. There is wide agreement that the enablers are necessary (but not sufficient) for DFS to reach its potential and achieve long-term sustainability. Experience indicates that uptake is greater when at least three of the basic enablers are in place than in their absence, but showing a strict causal relationship is difficult for several reasons.[91] There is less evidence that the fourth enabler—consumer protection—is a necessary condition for markets to take off. However, consumer protection issues need to be addressed to guarantee the healthy development of markets as they mature.

This research provides comparative case study analyses that can serve to inform discussion and guide policy development. The country experiences show that each country has used its own approach to set up the enablers. They demonstrate the ways in which an activity that is at least superficially simple for the user must be engineered through detailed regulatory measures that take into consideration each country's contextual foundation. That context is formed by the influences of the market, the political economy, the broader regulatory system, the level of technological development and innovation, and cultural and historical experiences. In the end, the rules that govern DFS often inhabit different bodies of legislation and reflect the

91 First, whether any one of the enablers is in place is not a binary, yes-no question, as each of them comprises a range of key regulatory decisions. Second, regulation is only one, albeit important, element of the DFS ecosystem (and perhaps more readily identified as a contributor to failure than to success). Third, our sample of countries is too small and idiosyncratic to measure or attribute outcomes with any rigor. Last, regulatory changes are in many cases too new to have had full effect, and the absence of other sufficient conditions poses a constraint. For examples of an approach to build an index of the regulatory environment for financial inclusion and derive overall country scores, see EIU (2016) and Rojas-Suarez and Pacheco (2017). Such an approach comes with its own challenges, which are not discussed here.

historical evolution of financial sector legislation. Going forward, there needs to be a clearer and more consistent set of rules that govern each of the four enablers.

Our research shows patterns that help explain results. Few areas in a regulated economy can truly be described as "build it and they will come." This appears especially true of DFS. The spectacular successes in a country such as Kenya probably owe more to an aggressive first mover dragging the market and the regulators along with it than to a systematic process of *a priori* framing. Regulatory frameworks in some other countries considered here reflect a similar dynamic. Often, as with regulation permitting nonbank e-money issuance, there is a build-up of pressure by prospective players, but the market cannot operate until either the rules are in place or the regulator issues a "no objection." In other areas, such as FCP, rapid market development leaves gaps that allow risks to accumulate until policy makers and regulators can provide a patch—or craft a more comprehensive solution.

As for the individual enablers, some broad insights arise from the study. Experience from the African countries shows the importance of EMIs in the first enabler. Even in those countries that have not set up a separate licensing framework for e-money issuance, nonbanks have found other ways to play a leading role in DFS by acquiring or setting up banks (Pakistan) or taking advantage of the license of their parent bank (Bangladesh).[92] The second enabler, the use of agents, seems to be the most consistently observed in practice. In all 10 countries, the liability of the principal for its agents' actions is a key tenet that allows the regulator to focus its attention on the principal. In most cases, there is substantial flexibility (as there should be) regarding who can be an agent. The third enabler, risk-based CDD/KYC, is strongly influenced by the desire to comply with FATF guidance. The shift toward risk-based rules at global and national levels, combined with ID system developments, is starting to allow for more flexible DFS outreach. Consumer protection, the fourth enabler, comes into the picture rather late, and has a less obvious role in jump-starting DFS markets. But its importance for safety and trust-building, which are crucial for long-term sustainability of DFS, is increasingly recognized. In all this, one must bear in mind that other conditions besides these enablers, including policies in such areas as competition and interoperability, play a role in shaping DFS access.

Ultimately, the quality of the regulatory framework depends at least as much on the capacity of policy makers and regulators as on the content of the rules. The demands on regulators have grown. The rise of cryptocurrencies and FinTech innovations pose new questions that regulators are struggling to answer. With these other priorities claiming attention, policy makers and regulators are not always tightly focused on enabling digital financial inclusion.

Yet there does appear to be a collective learning process. This happens both within and across countries as the frontier of good practice moves outward and demand grows for peer countries to share the lessons of experience. Some of the 10 countries studied (Myanmar) have only recently adopted specific regulations for DFS and have been able to learn from the earlier experience of other countries. Others (Ghana) can look back on many years of experience with DFS regulation and learn from past mistakes. Still others (Pakistan) have been able to improve their regulatory framework gradually over time. In general, piecemeal approaches have yielded patchwork regulation, but recent years have seen more consistent, systematic approaches. Thus, as we have tried to show here, evidence is at hand to guide policy makers in creating a framework that truly enables DFS and allows regulators to focus their attention on the areas of highest risk.

References

Alliance for Financial Inclusion (AFI). 2016. "Digital Financial Services: Basic Terminology." Guideline Note No. 19. Kuala Lumpur: AFI, August.

Arabehety, Pablo Garcia, Gregory Chen, William Cook, and Claudia McKay. 2016. "Digital Finance Interoperability & Financial Inclusion: A 20-Country Scan." Working Paper. Washington, D.C.: CGAP, December.

BCBS (Basel Committee on Banking Supervision). 2016. "Guidance on the Application of the Core Principles for Effective Banking Supervision to the Regulation and Supervision of Institutions Relevant to Financial Inclusion." Basel: BCBS, September.

Burjorjee, Deena, and Barbara Scola. 2015. "A Market Systems Approach to Financial Inclusion: Guidelines for Funders." Washington, D.C.: CGAP, September.

92 The Indian experience of awarding a limited purpose banking license (a payments bank license) is still relatively recent and it remains to be seen whether the fact that payments banks are a type of bank allows for similar flexibility and market take-off as an EMI license.

CGD (Center for Global Development). 2016. "Financial Regulations for Improving Financial Inclusion: A CGD Task Force Report." Washington, D.C.: CGD.

CPMI (Committee on Payments and Market Infrastructure) and World Bank Group. 2016. "Payments Aspects of Financial Inclusion." Basel: CPMI and World Bank Group, April.

Dias, Denise, and Stefan Staschen. 2017. "Data Collection by Supervisors of Digital Financial Services." Working Paper. Washington, D.C.: CGAP.

Dias, Denise, Stefan Staschen, and Wameek Noor. 2015. "Supervision of Banks and Nonbanks Operating through Agents: Practice in Nine Countries and Insights for Supervisors." Working Paper. Washington, D.C.: CGAP, August.

de Koker, Louis, and John Symington. 2011. "Conservative Compliance Behavior: Drivers of Conservative Compliance Responses in the South African Financial Services Industry." Cape Town: CENFRI. http://dro.deakin.edu.au/view/DU:30039928

di Castri, Simone. 2013. "Mobile Money: Enabling Regulatory Solutions." London: GSMA, February.

EIU (Economist Intelligence Unit). 2016. "Global Microscope 2016: The Enabling Environment for Financial Inclusion." New York, NY: EIU.

Evans, David, and Alexis Pirchio. 2015. "An Empirical Examination of Why Mobile Money Schemes Ignite in Some Developing Countries but Flounder in Most." Chicago: University of Chicago Coase-Sandor Institute for Law and Economics.

FATF (Financial Action Task Force). 2012. "International Standards on Countering Money Laundering and the Financing of Terrorism & Proliferation—The FATF Recommendations." Paris: FATF, February.

———. 2013. "Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services." Paris: FATF, June.

———. 2014. "Guidance for a Risk-Based Approach: The Banking Sector." Paris: FATF, October.

———. 2016. "Guidance for a Risk-Based Approach: Money or Value Transfer Services. Paris: FATF, February.

———. 2017. "FATF Guidance: Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion with a Supplement on Customer Due Diligence." Paris: FATF, November.

Garcia Arabehety, Pablo, Juliana Fontal Díaz, and Nidia Ruth Reyes Salomón. 2016. "Colombia's Recipe for 100% Agent Coverage: Aggregation & Sharing." Blog post, 9 May. http://www.cgap.org/blog/colombia%E2%80%99s-recipe-100-agent-coverage-aggregation-sharing

GPFI (Global Partnership for Financial Inclusion). 2016. "Global Standard-Setting Bodies and Financial Inclusion: The Evolving Landscape." Washington, D.C.: GPFI, March.

Greenacre, Jonathan, and Ross Buckley. 2014. "Using Trusts to Protect Mobile Money Customers." *Singapore Journal of Legal Studies*, 59–78.

ITU (International Telecommunication Union). 2017. "ITU-T Focus Group on Digital Financial Services: Main Recommendations." Geneva: ITU, March.

Izaguirre, Juan Carlos, Tim Lyman, Claire McGuire, and Dave Grace. 2016. "Deposit Insurance and Digital Financial Inclusion." Brief. Washington, D.C.: CGAP, October.

Lyman, Timothy R., Gautam Ivatury, and Stefan Staschen. 2006. "Use of Agents in Branchless Banking for the Poor: Rewards, Risks, and Regulation." Focus Note 38. Washington, D.C.: CGAP, October.

Lyman, Timothy R., Mark Pickens, and David Porteous. 2008. "Regulating Transformational Branchless Banking: Mobile Phones and Other Technology to Increase Access to Finance." Focus Note 43. Washington, D.C.: CGAP, January.

Malady, Louise, Ross Buckley, and Cheng-Yun Tsang. 2015. "Regulatory Handbook: The Enabling Regulation of Digital Financial Services." UNSW, December.

Mas, Ignacio. 2015. "Shifting Branchless Banking Regulation from Enabling to Fostering Competition." *Banking & Finance Law Review*, Vol. 30, No. 2.

Mazer, Rafe. 2016. "Kenya Ends Hidden Costs for Digital Financial Services." Blog post, 2 November. http://www.cgap.org/blog/kenya-ends-hidden-costs-digital-financial-services

Mazer, Rafe, and Alexandra Fiorillo. 2015. "Digital Credit: Consumer Protection for M-Shwari and M-Pawa Users." Blog post, 21 April. http://www.cgap.org/blog/digital-credit-consumer-protection-m-shwari-and-m-pawa-users

Mazer, Rafe, and Philip Rowan. 2016. "Competition in Mobile Financial Services: Lessons from Kenya and Tanzania." Washington, D.C.: CGAP, January.

McKee, Katharine, Michelle Kaffenberger, and Jamie M. Zimmerman. 2015. "Doing Digital Finance Right: The Case for Stronger Mitigation on Customer Risks." Focus Note 103. Washington, D.C.: CGAP.

Meagher, Patrick. 2017. "Regulatory Framework for Digital Financial Services in Côte d'Ivoire: A Diagnostic Study." Working Paper. Washington, D.C.: CGAP.

Porteous, David. 2006. "The Enabling Environment for Mobile Banking in Africa." Boston: BFA, May.

Rashid, Naeha, and Stefan Staschen. 2017. "Applying the RIA Lite Methodology: An Example from Pakistan." Working Paper. Washington, D.C.: CGAP, October.

Rojas-Suarez, Liliana, and Lucía Pacheco. 2017. "An Index of Regulatory Practices for Financial Inclusion in Latin America: Enablers, Promoters and Preventers." Working Paper 17/15. Madrid: BBVA Research.

Tarazi, Michael, and Paul Breloff. 2010. "Nonbank E-money Issuers: Regulatory Approaches to Protect Customer Funds." Focus Note 63. Washington, D.C.: CGAP.

Tsang, Cheng-Yun, Louise Malady, and Ross Buckley. 2017. "Promoting Financial Inclusion by Encouraging the Payment of the Interest on E-Money." *UNSW Law Journal* 40 (4).

No. 109
May 2018

Please share this Focus Note with your colleagues or request extra copies of this paper or others in this series.

CGAP welcomes your comments on this paper.

All CGAP publications are available on the CGAP Web site at www.cgap.org.

CGAP
1818 H Street, NW
MSN P157-700
Washington, DC
20433 USA

Tel: 202-473-9594
Fax: 202-522-3744

Email:
cgap@worldbank.org

The authors of this Focus Note are Stefan Staschen, who leads CGAP's work on DFS regulation and supervision, and Patrick Meagher, a CGAP consultant. The authors wish to thank Veronica Trujillo for extensive research support and Denise Dias, Xavier Faz, Jeremiah Grossman, and Juan Carlos Izaguirre for reviewing this paper.

Suggested citation:
Staschen, Stefan, and Patrick Meagher. 2018. "Basic Regulatory Enablers for Digital Financial Services." Focus Note 109. Washington, D.C.: CGAP.

ISBN: 978-1-62696-081-7