CGAP

FOCUS NOTE

Doing Digital Finance Right: The Case for Stronger Mitigation of Customer Risks

No. 103
June 2015

Katharine McKee, Michelle Kaffenberger, and Jamie M. Zimmerman

Low-income consumers stand to benefit greatly from more accessible and affordable digital financial services (DFS)[1] offerings. Indeed, evidence from consumer research in 16 markets[2] analyzed for this paper indicates that customers highly value and benefit from many basic DFS. However, many users are not only new to both formal finance and technology, they also live precarious financial lives that allow little room for error. Enabling users to understand and mitigate risks and minimize potential losses when using these new products and services will be critical for DFS to meet users' expectations and needs and, in turn, achieve sustained financial inclusion.

Mitigation of customer risks is also important for financial service providers (FSPs) and the broader DFS ecosystem. Private investments will not pay off unless mass-market consumers come to trust the services and respond with high uptake and sustained, active use of diverse DFS. This has, so far, not proven easy: only one-third of registered mobile money users worldwide are active. Moreover, in some markets, use of over-the-counter (OTC) services dominates even where users can register for mobile money wallets (hereafter referred to as wallets) that offer more value-added features and services.

This Focus Note explores consumer risk in digital finance—particularly through the lens of lower-income and less-experienced consumers—by asking three related questions:

1. What risks do consumers and customers perceive and experience when using DFS?
2. What are the consequences of those risks for consumers, providers, and financial inclusion?
3. How can those risks be addressed?

The paper reviews available evidence on DFS consumers' risk perceptions and experiences, focusing on risks that can cause financial loss or other harm. Its main goal is to advance responsible digital finance by helping the diverse industry actors engaged in DFS delivery better understand which problems are most important from the consumer perspective and motivating them to strengthen risk mitigation practices. The paper analyzes consumer research findings from 16 countries, including surveys and qualitative research in nine countries, four country case studies, and other research. It also presents findings from an initial landscaping study of relevant risk mitigation efforts by FSPs, as well as observed consumer protection regulatory and supervision measures.[3]

The analysis finds seven key consumer risk areas. While many customers report high levels of satisfaction with DFS, accumulating evidence shows that consumers also perceive or encounter common problems that can open them up to risks including financial loss. These include the following:

1. Inability to transact due to network/service downtime
2. Insufficient agent liquidity or float, which also affects ability to transact
3. User interfaces that many find complex and confusing
4. Poor customer recourse
5. Nontransparent fees and other terms
6. Fraud that targets customers
7. Inadequate data privacy and protection

The findings also suggest that consumers' experience—or even perception—of these problems contributes to their taking various steps to "self-protect," from

1 This paper addresses consumer risks and how to mitigate them across the full range of DFS (including digital transfers, payments, stored value, savings, insurance, and credit), channels (such as mobile phones and automated teller machines [ATMs]), and financial service providers, including mobile network operators (MNOs or "telcos"), banks, nonbank financial institutions, e-money issuers, retailers, post offices, and others. It uses "customer" and "user" interchangeably; "consumer" also includes potential users. Annex 1 defines more terms related to types of DFS products, providers, and risk mitigation measures.

2 This total includes markets with consumer evidence used for the analysis in Section II (Bangladesh, Colombia, Cote d'Ivoire, Ghana, Haiti, Kenya, India, Indonesia, Nigeria, Pakistan, Peru, the Philippines, Russia, Rwanda, Tanzania, and Uganda). Section II offers details on the consumer research methodologies and sources. Studies from additional markets contributed to evidence cited in other sections of the paper.

3 The landscaping study drew on desk research and interviews with FSPs and other experts to identify illustrative risk mitigation solutions that were reported to be effective; the research effort did not assess their actual effectiveness or wider applicability. The discussion on regulation and supervision mainly drew on AFI (2014) and BCBS (2015).

limiting DFS uptake and use to dropping out of the market altogether. Fears and negative experiences may also be affecting the cross-sale of more advanced or higher-margin products, such as credit, savings, or premium-paid insurance.

While FSPs and other industry actors may lack the full picture on customer risks, they are increasingly aware of them and the need to improve mitigation. To date, many factors have constrained provider responses to customer risks: users, agents, and agent managers underreport problems and FSPs struggle with both inadequate risk monitoring systems and capacity constraints. However, FSPs are making progress on ideas and solutions to reduce customer-related operational risks and improve customers' awareness and ability to avoid risks. Some solutions can provide significant gains at low cost, such as better signage and improved call center procedures, while others such as more robust operating platforms or agent management models are often neither easy nor cheap. Each operator or firm must assess its priorities in light of its business objectives, investment capacity, and the availability of cost-effective solutions.[4] In addition to individual provider efforts, initiatives such as the GSM Association (GSMA) mobile money Code of Conduct[5] and DFS-related updating of the Smart Campaign's microfinance client protection principles (Arenaza 2014) represent industry-wide commitments to build awareness, better practices, and standards (see Annex 3 for more industry codes and standards that could contribute to strengthening customer risk mitigation in the financial inclusion space).

Beyond industry actors, other DFS stakeholders are beginning to actively promote responsible digital finance. Consumer protection is on the radar of regulators and supervisors with DFS mandates and roles, especially those charged with ensuring financial inclusion in fast-paced markets. The Alliance for Financial Inclusion (AFI),[6] the G20 Global Partnership for Financial Inclusion (GPFI), the global financial sector standard-setting bodies (SSBs),[7] and the G20-OECD Task Force on Financial Consumer Protection (OECD 2014) also have relevant work underway on proportionate and effective regulation and supervision. Meanwhile, development agencies and donors are helping support industry and policy efforts.

Section II of this paper summarizes evidence on the seven DFS consumer risk areas and describes self-protection behaviors reported by consumers. Section III frames five priority areas for industry actors to address common customer risks and problems, analyzes business considerations that will affect the pace and extent of improved risk mitigation practices, and offers brief illustrations of potential solutions. Section IV highlights areas for further action, including work by the research and development communities to generate evidence and practical insights, and selected cases where regulation might be justified to reinforce industry efforts or fill gaps that leave consumers exposed to avoidable or unacceptable risks. The concluding section V acknowledges that momentum toward a responsible digital finance ecosystem is growing. If these diverse initiatives succeed, they will make an important contribution to win-win-win outcomes for consumers, the providers that serve them, and societies seeking more inclusive financial systems.

II. Risk Perceptions and Experiences of DFS Customers

DFS are expanding rapidly in emerging markets and developing economies. GSMA reports that more than 120 mobile financial service businesses are now serving 300 million people in developing markets worldwide; the number of registered users grew by 42 percent from 2013, and these accounts

4 GSMA finds that early-stage investments by mobile money operators to build out the agent network and generate consumer awareness typically cost seven to eight times more than the revenue generated. Operations tend to break even after three years. Operators that make these investments can expect profit margins of about 20 percent in the more mature high-growth stage (Almazan and Vonthron 2014). Mobile money operations at Safaricom (Kenya) and Vodacom (Tanzania), e.g., reportedly generate returns of this nature (Zetterli 2015).

5 This principle-based Code was launched in late 2014 and has been endorsed by 12 leading MNO groups. It includes a substantial focus on customer risk mitigation (GSMA 2014c). See also Di Castri (2014).

6 See, e.g., the guidelines on consumer protection in DFS (AFI 2014) and on technology risks (AFI 2012).

7 The 2014 Second GPFI Conference on Standard-Setting Bodies and Financial Inclusion, hosted by the Financial Stability Institute at the Bank for International Settlements, focused on standard setting in the changing landscape of digital financial inclusion (GPFI 2014). The six SSBs participating in the conference were the Basel Committee for Banking Supervision (BCBS), the Committee on Payments and Market Infrastructures (CPMI), the Financial Action Task Force (FATF), the International Association of Deposit Insurers (IADI), the International Association of Insurance Supervisors (IAIS), and the International Organization of Securities Commissions (IOSCO). See also Lauer and Lyman (2015) and BCBS (2015).

Box 1. Characteristics of digital finance models that affect consumer risks

Three characteristics of DFS models are salient for analysis of consumer risks:

The use of agents. This is a core feature of most DFS deployments and is an important innovation for providing financial services that are accessible, affordable, and extended in a nonintimidating and familiar environment. Relying on agents, however, can be a double-edged sword. On the one hand, agents often assist DFS customers with transactions and problems, which can build trust and confidence to try something new. On the other hand, the extent of agent-assisted transactions can expose inexperienced customers to risks if agents and their employees have insufficient capacity, training, and support or are dishonest. DFS providers face difficult trade-offs in optimizing service quality while building out an agent network with substantial reach.

Reliance on technology and technical interface. The cost and reach advantages of mobile and other digital channels are also essential for progress on financial inclusion. Yet many DFS consumers are first-time users of formal finance who struggle, at least initially, with language barriers, complicated interfaces, and multi-step processes, particularly since most are using basic feature phones with limited interface options.[a] ATMs present similar challenges (CGAP 2014a). In addition, customers depend on sometimes unreliable mobile networks and DFS platforms for their transactions and the safety of their data and any stored funds.

Longer and more complex value chains. Development of the payments ecosystem through business partnerships and new players entering to take on specialized roles is also important for full financial inclusion to be achieved, including availability of value-added or advanced services such as bill pay, credit, or insurance. Governments and development agencies are also involved in some value chains as bulk payers. Data analytics firms can also be involved as they assist with services such as credit scoring. The number of entities involved directly or indirectly in delivering DFS affects customer risks and can result in gaps in oversight and liability. Effective coordination is needed to clarify who is ultimately accountable for ensuring customer welfare and to deliver transparent and effective complaints handling.

It is important to note that, while DFS increases some customer risks or shifts management of them to actors with less capacity to do so, it can also reduce other customer risks (e.g., physical insecurity from carrying cash, lack of confidentiality in obtaining a loan).

a. See, e.g., InterMedia (2014).

outnumber bank accounts in 16 countries (GSMA 2015). However, inactivity is high in many regions, reaching 91 percent of users in West Africa, and in many countries OTC is common,[8] limiting customers' access to more advanced, wallet-based services (GSMA 2014a).

How can we reconcile the contradictory facts of rapid DFS growth yet limited activity and consumer preferences such as for OTC? While answers are undoubtedly complex, probing the customer journey can offer clues to the areas that need priority attention (GSMA 2014b). Overall, the evidence shows that the risks consumers perceive and experience with DFS can harm their trust, uptake, and use of the services. The specific nature of the risks and their incidence, consequences, and impact on consumer behavior vary from one DFS market to another.

In Uganda, for example, some consumers report that while they are aware of mobile money, their perceptions of network and platform unreliability limit their willingness to use the services (Ogwal 2015). In Tanzania, some lapsed DFS users (those who have not used the service in more than 90 days) say poor recourse channels and resolution have driven them to transact only in cases of emergency since they do not want to risk a transaction error they cannot resolve (InterMedia 2014). Context matters in terms of the business model and type of DFS as well: in Bangladesh, users report that the complicated interface is an important driver of the high use of OTC, deterring them from registering for a wallet that can offer them more services and fuller inclusion (InterMedia 2014).

Methodology. The evidence presented in this section draws on analysis of nationally representative comparative surveys and qualitative research conducted in Bangladesh, Ghana, India, Kenya, Nigeria, Pakistan, Rwanda, Tanzania, and Uganda under the Financial Inclusion Insights (FII) study carried out by InterMedia for the Bill & Melinda Gates Foundation (BMGF) and for CGAP.[9] These data allow analysis of the frequency of specific

8 In Pakistan, 94 percent of mobile money users do OTC transactions, and in Bangladesh it is 84 percent (GSMA 2014a).

9 Sample sizes for the non-India FII surveys range from N=3,000 to N=6,000. The qualitative research included focus group discussions (Bangladesh, Nigeria, Pakistan, Tanzania, and Uganda); agent interviews and customer exit interviews (Bangladesh, Nigeria, Pakistan, Tanzania, and Uganda); and mystery shopping exercises (Bangladesh, Nigeria, Tanzania, and Uganda).

DFS user and nonuser risks and problems and offer insights on differences among demographic and geographic segments. The evidence also draws on findings from four CGAP country case studies conducted in mid-2014 by Bankable Frontier Associates in Colombia and by MicroSave in Bangladesh, the Philippines, and Uganda.[10] The markets were chosen for the diversity of business models, market maturity, geography, and other factors relevant to DFS consumer risk experience.[11] Finally, the paper draws on a thorough desk review of consumer risk evidence from additional sources, including CGAP studies in Colombia, Cote d'Ivoire, India, Russia, and Tanzania; Agent Network Accelerator (ANA) surveys;[12] and research by the United Nations Capital Development Fund (UNCDF), GSMA, Financial Sector Deepening Kenya, and others.

The evidence is limited in some important ways. It focuses on those types of DFS that are most relevant for financial inclusion rather than on the entire digital finance sector. Also, because many countries lack adequate quantitative data, it is impossible to determine the precise level of incidence of customer risks, limiting the generalizability of problems. Also, while it is true that agents also face numerous risks in providing DFS, examining these risks is beyond the scope of the paper.

Of the seven key areas of concern[13] identified among DFS customers across most markets studied, some—such as fraud—present a direct risk that can result in financial loss or other harm. Other concerns are less direct, as they create conditions that could result in loss or other harm. Network downtime, for example, can cause customers to leave money with agents to complete a transaction when the network is back up, exposing customers to possible fraud if the agent instead keeps the money. Each risk is discussed in more detail below.

1. Inability to transact due to network/service downtime

Risk-related issues include the following:

- Risky customer behaviors
- Interrupted and incomplete transactions
- Inaccessible funds
- Lack of confirmation messages

> **"Sometimes [mobile money services] are not operational....The money is in the phone, but when you want to withdraw, they tell you that the network is down."** *Urban man, Tanzania*

Inability to transact due to network downtime is the top consumer concern. Network unreliability both erodes trust in the service and can result in harm or risky customer behaviors. Users in multiple countries say they are afraid to conduct transactions because of the possibility of a network failure. Unreliability affects both nonusers (who may limit uptake when they hear of problems from others) and users (some of whom report limiting their activity as a result).

> **"What you do is you leave the agent with the money and they send it when the network is back so all you have to do is just call them to confirm that it has been sent."** *Rural woman, Uganda*

Frequent outages and unreliable networks or platforms result in four related problems. First, in several markets the prevalence of downtime results in risky customer behaviors such as leaving cash,

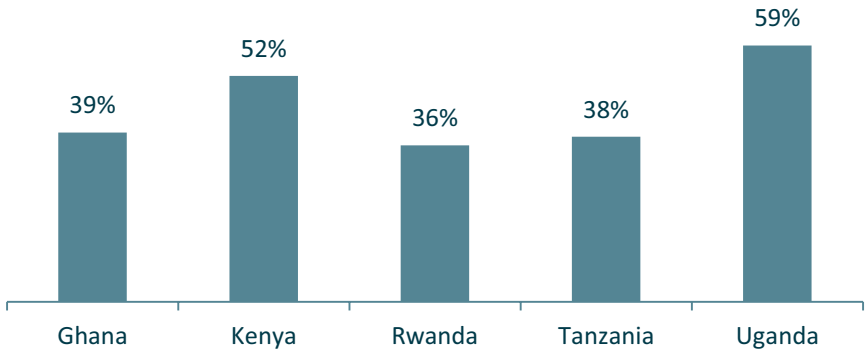
10 The studies included focus group discussions and interviews with DFS users and nonusers, covering a total of 224 participants in Bangladesh, 227 participants in Uganda, 215 participants in the Philippines, and 80 participants in Colombia. The studies also included interviews with DFS FSPs, agents, technical service providers, and regulators.

11 Uganda consists of an MNO-bank partnership model with nearly 15 million registered money users; from 2011 to 2013, it experienced rapid growth of 389 percent. Bangladesh is a hybrid market in which banks partner with MNOs or third parties to offer services. It has 15 million registered users, experienced rapid growth of 183 percent from 2013 to 2014, and is dominated by OTC transactions. The Philippines is a more mature market, driven by MNO-bank partnerships, with 27 million registered users but slower growth (34 percent from 2011 to 2013). Colombia's market is largely driven by banks using agents to facilitate DFS transactions; customers reached 5 million in 2013, with 62 percent growth over the previous two years.

12 Conducted by MicroSave's Helix Institute of Digital Finance with BMGF funding, ANA consists of nationally representative surveys of over 9,000 total DFS agents in Bangladesh, India, Indonesia, Kenya, Nigeria, Pakistan, Tanzania, and Uganda.

13 One concern that was not raised often by consumers was risk of loss due to the insolvency or failure of their DFS provider.

Figure 1. Percentage of mobile money users who have experienced service downtime when transacting



Source: InterMedia (2015).

personal identification numbers (PINs), and even phones with agents to complete a transaction when the network returns. Second, network downtime causes interrupted and incomplete transactions, which occur when a customer sends a transfer and the network drops service before the transfer is credited to the recipient's account (e.g., when there are integration gaps among multiple platforms processing a transaction). The transferred funds can be stuck in a technical "limbo" between the sender's wallet and the receiver's account, with both parties denied access to the funds until the network resumes service and the transaction can be completed. Third, users can temporarily lose access to their funds such as wallet balances and the ability to send transfers or cash out, a clear harm for any customer with urgent liquidity needs. Finally, network or platform unreliability can result in users not receiving real-time confirmations for completed transactions. Faced with uncertainty, the user may send the funds again, which in turn can result in two transaction fees and reliance on the recipient's good will for return of the money. In some such cases, the sender will call the recipient to confirm receipt. Conversely, customers may believe the payment went through when it did not and as a result fall behind on an important payment.

The Colombia case study showed that leaving money with agents when the network is down is so common it has its own colloquial name: Jineteo. This typically occurs when a bill pay customer cannot transact during downtimes and leaves cash with the agent to process the payment once service returns. Some agents instead use the cash and defer paying the user's bill (CGAP 2014f). This practice is a misuse of customer funds and puts them at risk if the agent forgets to pay the bill, does not have sufficient liquidity to pay when it is due, or simply chooses not to do so.

Solution example: MTN Uganda migrated to a new platform in late 2014 that it expects to substantially improve service reliability.

2. Insufficient agent liquidity or float

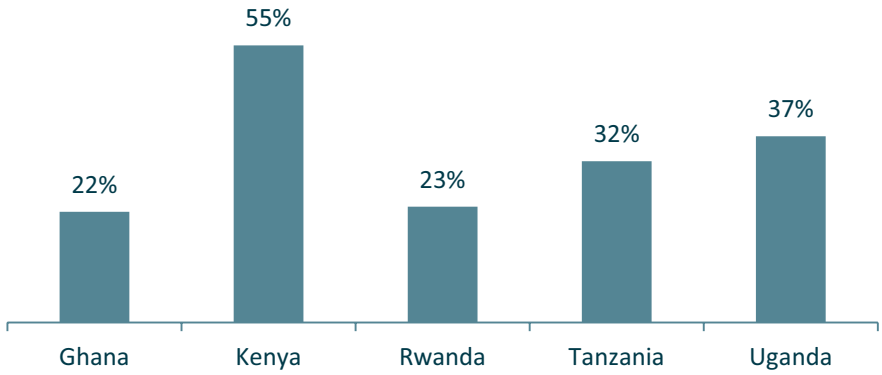
Risk-related issues include the following:

- Agent business-related causes
- Bulk payments
- Information privacy and security

Insufficient agent liquidity deprives users of access to their own money. It can also result in "split transactions," a practice in which a customer must perform multiple transactions, costing the customer through higher total transaction fees (in a tiered fee system). The FII surveys report this as the second most common problem among DFS users in many countries, following network downtime (Figure 2).

According to the ANA surveys (Helix Institute of Digital Finance 2014a), lack of liquidity in Tanzania results in denial of an average of five transactions per agent per day, equal to 14 percent of daily transactions. In Uganda the denial rate is three transactions per agent per day or 10 percent

Figure 2. Percentage of mobile money users unable to complete a transaction due to insufficient agent liquidity



Source: InterMedia (2015).

of daily transactions. In Kenya the rate is three transactions per day. These numbers represent a substantial proportion of attempted transactions.

Agent business-related causes

Agents report challenges in liquidity management, citing "fluctuations in client demand" as one of the greatest difficulties in maintaining appropriate cash and float levels. Other difficulties include having to close their store to rebalance, insufficient funds to buy more float, and the time required to travel to and wait at the rebalance point.[14] In addition, agents in many markets are targeted for robbery because of the cash they hold, incentivizing them to hold less. Fraudsters also target agents and their digital currency, which creates incentives for agents to keep less float in their account (Wright 2013).

Some agents intentionally manage their liquidity in a way that can result in customers being unable to transact. A study in Kenya showed some agents lie to customers about liquidity shortages to maximize revenue from each transaction[15] or to help other agents nearby, refusing to conduct certain transactions even when they do in fact have sufficient float (Jumah 2015).

Solution example: Pakistan's EasyPaisa analyzes data on airtime sales to verify the financial health and liquidity of a business before approving a retailer as an agent.

Solution example: In Bangladesh, employees of the agent aggregators, often referred to as "runners," deliver cash to agents regularly, providing more frequent rebalancing opportunities. As a result, agents deny a median of zero transactions per day due to lack of liquidity.

Bulk payments

Digital payment of social safety net transfers and bulk aid poses a special challenge, as found by a study commissioned by CGAP on behalf of the Better than Cash Alliance and with support from the UK Department for International Development (DFID) in Uganda, Kenya, the Philippines, and Haiti (Zimmerman et al. 2014; CGAP 2013b, 2013c, 2013d, and 2013e). Recipients of government-to-person (G2P) payments in a locality often receive their electronic transfers on the same day, and most want to cash out immediately, putting pressure on agent liquidity. The study found that generally only the first card- or mobile-based withdrawal in a pay period is free for G2P recipients, so multiple withdrawals and associated fees represent lost income. Given the very low income levels of most G2P social benefit recipients, extra fees and inaccessible funds are particularly problematic.

14 See ANA reports for Uganda, Kenya, and Tanzania (Helix Institute of Digital Finance 2014a).

15 The fee structure for M-PESA in Kenya is tiered. So, e.g., an agent receives the same amount of revenue from a transaction of Ksh. 3,501 through Ksh. 5,000. To both maximize revenue and maintain maximum float, an agent will claim to have insufficient liquidity for a transaction of Ksh. 4,000 or 5,000, offering to transact only Ksh. 3,550 to maintain the extra liquidity while earning the same revenue as with the larger transaction.

A study conducted by CGAP, MasterCard, and the World Food Programme (WFP) showed that WFP transfer recipients in eastern Kenya experienced similar cash-out challenges (Mazer and Baur 2014). Particularly in more remote areas, recipients would travel long distances to reach an agent, only to find that the agent lacked sufficient liquidity for them to cash out. Some beneficiaries left their ID, PIN, and program-issued card with the agent to withdraw money once the money arrived. Others pooled their cards and PINs as a group, and one person would travel to withdraw everyone's funds to save others from unsuccessful trips. In another variant, beneficiaries would electronically transfer funds to a single beneficiary, who would travel and collect the money. Such workarounds place recipient funds at risk, both from the agent and from the person who cashes out for all.

Digital bulk transfers tend to be more efficient or reliable than disbursing cash. The volume also offers benefits to the payments ecosystem. Typically, digital transfers also result in less leakage, which benefits recipients and can be more convenient. Addressing the problems described above would improve user experience, reduce potential financial harm, and enable leveraging these systems to promote financial inclusion.[16]

Unauthorized sharing of customer information and credentials

Insufficient agent liquidity can also compromise the confidentiality of customers' personal information. In Uganda, for example, some agents said that when they lack liquidity, they frequently call another agent, provide the customer's PIN, have the other agent complete the transaction, and then reconcile the amounts later (CGAP 2014c). This sharing of private information, clearly also a data security issue, can leave customers vulnerable to fraud and undermine trust that their financial matters are handled confidentially.

3. Complex and confusing user interface

Risk-related issues include the following:

- Difficulties operating services
- Assisted transactions, including PIN sharing
- Keystroke errors

> **"I'm not that educated, therefore, I don't understand the mobile menu."** *Man, Pakistan*

Complex and confusing menus and user interfaces make it difficult for consumers to operate DFS and can expose them to risks.[17] GSMA (2015) finds that a "lack of knowledge and confidence in their ability to use mobile financial services" is a critical barrier to broader uptake among women in particular.[18] In Russia, customer perceptions of how easy digital channels are to understand and use is seen as a key factor in further uptake and use (Imaeva et al. 2014; Lyman et al. 2013).

Difficulties operating services

In many countries, mobile money menus are in English or a formal style of the local language, creating a challenge for consumers who are illiterate or understand only colloquial language. ATM interfaces commonly present similar barriers.[19] Furthermore, most DFS menus require many steps, which users report finding difficult and confusing. In Bangladesh and other markets, user transactions via Unstructured Supplementary Service Data (USSD) require five to six steps and are time-limited, which can lead to time-out of the transaction (CGAP 2014e). Complicated and unintuitive menus and other user challenges with the technical interface were also reported in the Colombia case study.[20]

> **Solution example: M-PESA in India is available in Hindi, Bengali, Marathi,**

16 E.g., Equity Bank, the former payment service provider for WFP's Cash for Assets cash transfer program in Kenya realized that agents were changing their fees because of liquidity challenges. (Delayed program payments were requiring them to pay out multiple months' of transfers to recipients at once.) The bank modified its fee structure and agreement with WFP and committed to closer monitoring of liquidity needs.

17 See CGAP Country Case Studies (CGAP 2014c, 2014d, 2014e, and 2014f) and InterMedia (2014).

18 See also Shrader (2015) and CGAP (2014a).

19 In the Colombia country case consumers mentioned being confused when ATMs ask for additional two zeros for cents, which they do not use (CGAP 2014f). See also Seltzer and McKay (2014).

20 They also complain that the interface and menu differ when using a different (feature) phone. Some insert their SIM into another person's phone to make a transaction because the menu will not show properly on their own phone (CGAP 2014f).

Gujarati, and English, with additional languages planned.

Many customers also have difficulties creating and memorizing PINs, which is integral to transacting through most mobile money accounts and many card-based services. PINs are especially problematic for customers who are first-time users of both digital services and passwords. Not surprisingly, many choose easy numbers, write them down, or share them, which can place their accounts at risk or compromise the confidentiality of their financial affairs.[21] The country case studies revealed cases of agents suggesting or even providing PINs to customers. Using PINs and keeping them secret will grow in importance as more users maintain balances in their accounts and wallets.

Keystroke errors

Poor user interface can also result in financial loss when users make keystroke errors or other process mistakes that are then difficult to reverse or resolve. Such mistakes can result when customers do not understand the menu or rush through the many steps to complete a transaction before it times out. Sending money to a wrong number, for example, is particularly common. Menus that do not display the recipient's name when the phone/account number is entered exacerbate this problem.[22] "Repudiation" or reversal of mistaken transactions is generally a challenge. FSPs often insist that the responsibility for erroneous transfers rests with customers, particularly once the unintended recipient withdraws the money.

Assisted transactions

"My sister always withdraws and brings the money for me.... She tries to teach me, but I'm scared with all those buttons of messing up and losing money." *Woman, Colombia*

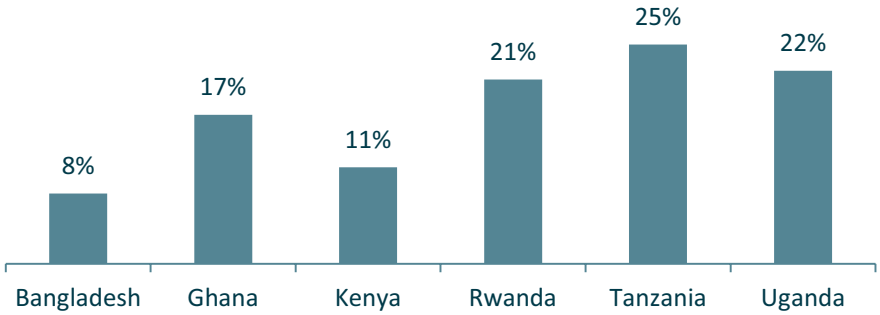
Customers often cope with poor user interfaces by seeking help from agents or others, such as family and friends. For registered users, this typically requires sharing their PIN or other account information. In East Africa, for example, registered users say they often have agents walk them through a transaction or conduct it for them on their phone because they cannot operate the menu independently (InterMedia 2014). Assisted transactions are particularly common with elderly customers or in rural areas where literacy levels are low. While transaction assistance can help customers cope with risks, such as by helping them avoid errors, it also can leave them vulnerable to misconduct, fraud, or losses from those from whom they seek help.

4. Inadequate provider recourse

Risk-related issues include the following:

- Unclear, costly, and time-consuming procedures
- Limited agent capacity
- Particular concerns for G2P recipients

Figure 3. Percentage of registered mobile money users who "usually" have someone else conduct transactions on their behalf



Source: InterMedia (2015).

21 Regarding predictable and agent-assigned PINs, see Uganda Country Case Study (CGAP 2014c) and Ogwal (2014).
22 See CGAP Country Case Studies (CGAP 2014c, 2014d, 2014e, and 2014f).

Box 2. Customer risk and OTC transactions

OTC transactions are a particular type of assisted transaction, in which the customer has the agent conduct the full transaction on his or her behalf on the agent's phone. Often, though not always, the customer does not have a registered DFS account. Many factors drive OTC transactions, including poor interfaces that deter independent use of wallets; customers who prefer that the agent transact on their behalf; customers not owning their own handset or SIM; lack of identification or other factors preventing customers from registering for their own account; agents who attempt to increase their revenues (e.g., by charging unauthorized cash fees for OTC); and providers who offer specific OTC products such as bill payments at the agent.[a]

OTC use is widespread in some markets, reaching 77 percent of all mobile money users in Bangladesh despite the fact that OTC transactions are legally not allowed (InterMedia 2015). In some countries, OTC use is common even among registered mobile money users. In Uganda, 58 percent of registered users say they "usually" use OTC services (InterMedia 2015). Once OTC use is established and users are familiar with it, nudging changes in their behavior and uptake and use of wallets may be difficult without considerable improvements in awareness and/or use cases and service offerings.

At times, OTC transactions may reduce risk for customers, while at other times they may increase it. When customers have an agent perform the transaction, risk of loss from wrong transactions and other mistakes may be lower. However, OTC transactions also expose users to potential agent misconduct or fraud, as well as payment of extra fees and loss of privacy. A study in Bangladesh showed that customers consider wallets more trustworthy than OTC as a transfer mode and that OTC users are more likely to be charged unauthorized fees (Chen and Islam 2014).

OTC transactions—whether driven by customer preference or agents or both—also poses challenges to DFS providers in terms of revenue assurance, agent compliance with policies and procedures, and/or customer progression to more advanced services.[b]

a. According to Chen and Islam (2014), it is paramount to offer customers a clear value proposition for wallets, such as offering more value/services (e.g., savings, credit, clean water, solar power, insurance), reducing prices (currently wallet fees are similar to actual OTC charges), using local languages and simplifying the customer interface.
b. See, e.g., Wright (2014).

> **"[When my mobile recharge did not go through at the agent] I had to go to [the MNO] office… It was just 10,000 pesos (US $5) but it's annoying! I waited for three days for them to answer my complaint but I [never got it resolved]. This experience led me to worry: what it if happens when I'm paying my bills?"** *Man, Colombia*

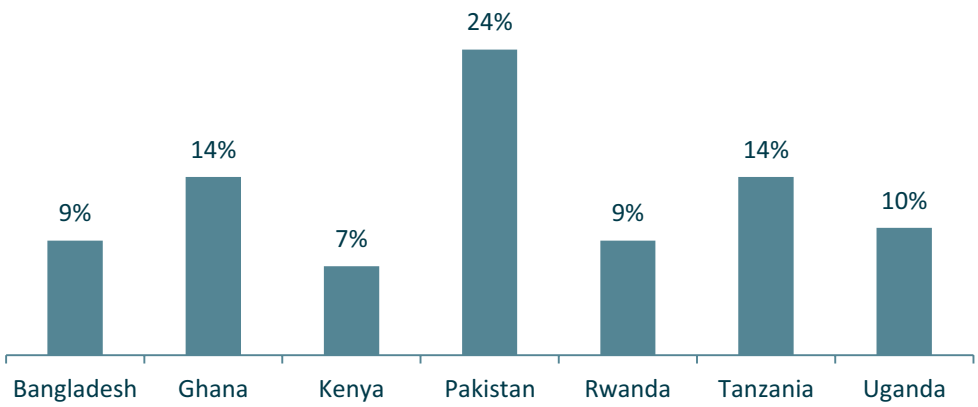
Weaknesses in customer recourse arrangements by FSPs and their business partners and poor performance in resolving complaints and queries are foundational issues in consumer protection. This is a significant concern in many countries and was cited as a barrier to DFS use by consumers in Bangladesh, Colombia, Tanzania, and Uganda.[23] Nonusers reported that negative word-of-mouth and perceptions of poor recourse reduce their willingness to try services. Users in multiple markets reported that since they cannot resolve problems even with simple transfers, they do not want to risk making a mistake with a more complex service such as bill payment.

Unclear, costly, and time-consuming procedures

Problems with recourse take many forms. First, customers report they are unclear on how to complain and to whom. If they pursue a complaint, they often encounter inadequately trained call center representatives who are unable to resolve it. Customers in nearly all markets studied reported long hold times when calling helplines, and in some markets they are charged for airtime. In addition, calls often drop due to poor network quality, requiring the user to call back and explain the problem anew. In some fraud cases, fraudsters capitalize on long hold times: by the time the user gets through to report the crime, the fraudster has already transferred proceeds from the scam out of the wallet.[24] Visiting customer care centers generally entails transport costs and time lost to travel and waiting. When multiple parties are

23 See CGAP Country Case Studies (CGAP 2014c, 2014d, 2014e, and 2014f) and InterMedia (2014).
24 Interview with Mercy Buku, independent consultant, former senior manager, Money Laundering Reporting, Risk Management, Safaricom Kenya.

Figure 4. Of mobile money users who have experienced a service problem in the past six months, the percent who reported it to customer care



Source: InterMedia (2015).

involved in delivering the service (e.g., a telco, a payment service provider, and a bank for bill payments), customers report being shuffled around. Overall, customers report low use of recourse channels, due to a combination of the unclear process, expense, and difficulties.

Solution example: Tigo-Ghana guarantees its customers are given feedback on the progress of their resolution not later than an hour after complaining. Full resolution of complaints is aimed to be given within 24 hours, and customers receive a ticket number and regular updates (Tigo Ghana 2015).

Role of agents

"[The mobile money provider] does not care about us anymore. If I call the territory manager for any help, the reply is that we have to be careful about transactions ourselves. They are transferring the risk onto us. They don't help us when we have made a mistake." *Mobile money agent, Bangladesh*

Evidence in the FII research and CGAP country case studies suggests that DFS customers often look to agents to resolve problems. In Ghana, for example, 61 percent of mobile money users say they turn to an agent, and in Rwanda 52 percent report doing so (InterMedia 2015). Agents, however, are not always trained or equipped for this role, the data-sharing required may make customers susceptible to fraud, and agents may lack incentives to spend time performing this function. Often agents must call the same helpline as customers would, thus incurring lost time and airtime while on hold. ANA surveys in Uganda, Tanzania, and Bangladesh indicate that agents consider dealing with customer service when something goes wrong as the second most burdensome issue (after the risk of fraud) (Helix Institute of Digital Finance 2014a). According to FII and other research, agents often direct customers either to another agent or to customer care centers.

Solution example: Bancolombia has created a dedicated call center for agents, making it easier for them to resolve their own and customers' complaints.

Particular concerns for G2P recipients

CGAP's 2014 study of electronic G2P payments in low-income countries revealed recourse mechanisms as a particular weak spot (Zimmerman et al. 2014). Recourse and support options were often unclear to recipients, making it difficult to solve problems or get answers to questions they had about their payments. G2P recipients also worried that if they complained they could lose their transfers, a misperception that made them

reluctant to report problems. These difficulties undermined the financial inclusion and efficiency objectives of using e-payments for the schemes.

Example solution: In 2014, WFP in Kenya launched a new service hotline with a call-back function. To inform beneficiaries WFP offered training on the hotline, leaflets, and posters at merchants. Two staff with extensive language abilities track beneficiary calls via a customer relationship management system.

5. Nontransparency of fees and other terms

Risk-related issues include the following:

- Opaque or inadequate disclosure of fees and other terms
- Suspicions of overcharging

"The charging rate is not standard because in some places when withdrawing TSh 10,000 ($6.25), you are charged TSh 1,200 ($0.75) while in another place you are charged TSh 2,000 ($1.25). There are posters…but the way they are written is different from what the agent says." *Rural woman, Tanzania*

Lack of transparency leaves consumers without a full understanding of the prices, terms, and conditions of the financial services they are using. It also makes them more vulnerable to other risks, such as agent misconduct and price fraud (i.e., charging unauthorized fees).

Opaque or inadequate disclosure of fees and other terms

Many customers say fee structures are confusing, and they don't know how much a transaction should cost. In many markets customers said agents charge varying fees, and they are unsure which fees are authorized. For example, mystery shopping in Uganda and Bangladesh showed that fee charts are frequently not displayed at agent shops (InterMedia 2014). In Tanzania, research showed that while agents typically display fee charts, the amounts charged can differ from those on the chart. Customers report agents often display old fee charts and only verbally explain current fees (InterMedia 2014). Consumers in the Philippines report lack of confidence that they are being charged fairly, which is exacerbated in part by the fact that agents are allowed to change the fees (CGAP 2014d). Customers also voice concerns that ATMs do not inform them about withdrawal fees, including when they use the ATM of another provider. In a donor-to-person cash transfer program in Kenya, for instance, beneficiaries explained that they do not like using an ATM since they do not know which fees apply for withdrawals.[25]

Research in Kenya and Tanzania showed that fees for third-party transactions conducted through mobile money (such as bill payment) are particularly opaque. For example, an unpublished CGAP survey of 500 low-income Nairobians found that 35 percent of bill pay users thought the service was free, despite audits of their M-PESA transaction records confirming they had been charged for the services. Since the fees are not disclosed, users would know about them only if they examined their account balance before and after the transaction and noticed a lower balance, or if their balance was insufficient to cover both the transaction and the fees. There have also been cases where third-party service providers use the MNO platform for bill payments and then overcharge the customer for services or register the customer for unwanted services, deducting daily charges for them.[26]

The terms for DFS, especially more complex services, such as credit or insurance, are also often poorly disclosed. In Rwanda, only about half of borrowers report knowing their loan terms and the interest they pay on loans (InterMedia 2015). In Kenya, the M-Shwari savings and credit product provides terms and conditions through a web link, even though many users lack access to the internet. In Tanzania consumers report confusion about the relationship between mobile money and nonfinancial services offered by telcos.[27]

25 Some also mentioned having heard from others that ATM fees are very high, even though ATM fees are actually lower than those charged by agents (unpublished CGAP research).

26 Interview with Mercy Buku, independent consultant, formerly senior manager, Money Laundering Reporting, Risk Management, Safaricom Kenya.

27 Interview with Kennedy Komba, National Payment Systems advisor, Bank of Tanzania.

Suspicions of overcharging

Poor fee transparency in particular can lead users to suspect agent misconduct and can harm the reputation of DFS and FSPs. In Uganda, for example, the FII research showed that inadequate fee transparency has led some customers to believe all fees charged by agents are fraudulent (InterMedia 2014). In Russia, poor transparency of fees and conditions is in the top four concerns limiting DFS uptake (Imaeva et al. 2014; Lyman et al. 2013). Actual charging of unauthorized fees by agents is addressed in the next subsection.

6. Fraud perpetrated on the customer

Risk-related issues include the following:

- FSP internal employee fraud and fraud by external parties
- Agent fraud

Fraud is a less commonly reported yet existing threat. Consumers can lose money and providers can suffer reputation risk.[28] Perceptions of fraud were high in the markets covered by the CGAP country case studies, though actual experiences of fraud were low. This suggests that word-of-mouth about even a few instances can have wide impact. Perceptions of fraud are a problem in other countries as well. In Côte d'Ivoire, for example, users who receive digital payment of crop proceeds reported withdrawing all their funds immediately and carrying the funds to their microfinance institution to deposit, because they fear fraud and perceive this as a more secure option. FII data support this finding on perception versus reality; for example, only 2 percent of Ugandan mobile money users in the survey reported experiencing fraud, but in the qualitative research perceptions of fraud were much more commonly reported (InterMedia 2014, 2015). The perceptions of fraud are likely to harm use: some Bangladeshi wallet holders, for example, say they do not keep a balance to avoid losing money to fraud (CGAP 2014e). This trust gap could also impede uptake of products such as mobile savings.

FSP internal employee fraud and fraud by external parties

DFS provider employees may use their position to gain access to private customer information and then use this to target certain customers, gain account access, or otherwise obtain client funds. Third parties, such as employees of companies providing outsourced services or unaffiliated fraudsters, generally contact customers directly to fraudulently obtain account information or use other means, such as hacking into accounts, to access accounts or ultimately obtain funds (Mudiri 2012). Some of the forms such frauds can take include the following:

1. *SIM swaps,* which occur when a fraudster has a customer's phone number moved ("swapped") to a different SIM, changes or otherwise learns the PIN associated with that user's mobile money account, and withdraws the balance.
2. *Social engineering scams*, including fraudulent SMS messages or calls (e.g., phishing) that request or otherwise aim to obtain a customer's PIN, other information, or a money transfer. Examples include claims of erroneous transfers and promotion or job application scams.
3. *Caller ID spoofing*, which causes a false phone number to appear on the caller ID and then requests information or otherwise scams the customer.
4. *Counterfeit ATMs* that read and copy card numbers, false facades, hidden surveillance cameras that record PINs, skimming, and the presence of fraudsters at machines to "help" customers who experience difficulties (Lubitz 2008).
5. *Unauthorized account access by employees*, which can be gained through one's position in the FSP or poor internal security that can result in lost funds or unauthorized access to customer information. Hacking by external fraudsters is much less common than internal fraud.

Consumers described a variety of experiences with these types of fraud in the CGAP country case studies and the FII qualitative research. In

28 This Focus Note looks specifically at fraud that harms customers, rather than fraud that harms agents or providers.

Bangladesh, users reported receiving fraudulent calls claiming they won the lottery and requesting a money transfer to "access" their winnings. Others said a caller claimed to be a call center representative who needed customer information. Some customers in Bangladesh reported their mobile wallet balance had disappeared, which they thought resulted from someone hacking into their account.

In Uganda, customers reported receiving fraudulent SMS messages saying money had been deposited into their account, followed by a call requesting they "return" the money sent by "mistake." Another study found this as well, with urban users in particular having experienced this type of fraud and many saying they lost money as a result (EIB and UNCDF 2014). Such fraudulent reversal requests were once the top social engineering scam in Kenya but have been reduced significantly through aggressive awareness campaigns.[29]

Nigerians report widespread fraud and scams via mobile phones, such as airtime credit "disappearing," scams by third parties via SMS, charges for services to which the user has not subscribed or for unsubscribed services, and charges for undelivered SMS. This leads to significant lack of trust among the general population in MNOs and services offered through mobile phones. Focus group participants expressed fears of hackers breaking into accounts and stealing money (InterMedia 2014).

Solution example: Safaricom M-PESA uses SMS alerts, radio announcements in local dialects, newspaper ads and other efforts to improve customer awareness of fraud tactics.

Solution example: Providers in Tanzania implemented a "quarantine" following a SIM swap during which the associated mobile money PIN cannot be changed. Some operators now have in place "IMSI locking," a systems solution that locks the SIM and blocks access to the account until the customer has satisfied the mobile money staff that the SIM swap was legitimate and they have the SIM in hand, at which point the new SIM will be linked to the account.

Agent fraud

Agents can commit fraud in various ways. One method is to split a single transaction into multiple transactions to increase commissions.[30] For example, an agent may tell a customer that he does not have enough float and advise the customer to return later to complete the transaction. This can result in extra fees for customers, who may or may not understand what has happened. Research in Kenya showed some agents conduct partial transactions to manage their float and maximize revenues (Jumah 2015). Another method is to access and use agent records for fraudulent purposes. For example, an agent could access another agent's log book, used to record transactions, gain information about customers, and use that information for fraudulent purposes.[31]

Finally, agents can charge unauthorized fees. Unauthorized fees, particularly for OTC transactions, are commonly reported in many markets. They can take multiple forms such as agents charging extra fees when conducting transactions and charging for services that should be free. Even when mobile money business processes are set up to deduct the correct fees electronically, for example, agents can overcharge customers by requiring extra fees paid in cash for cash-in or by short-changing the customer on cash-out. In Uganda, DFS users report agents charging for registration, even though there should be no registration fee, and users widely suspect agents of charging unauthorized fees for transfers (InterMedia 2014). According to a UNCDF study,

29 Interview with Mercy Buku, independent consultant, formerly senior manager, Money Laundering Reporting, Risk Management, Safaricom Kenya.

30 In a tiered pricing structure, agents are paid a flat fee for each band of transaction sizes and can therefore receive a higher total commission by making multiple transactions. This is opposed to a percentage-based fee structure, where the total fee is the same whether the transaction is completed all at once or with multiple transactions. There are commercial benefits to the former, so many providers do not want to switch to percentage based simply to avoid fraud.

31 Information in log books can also be used for other types of fraud, such as fraudulent registration in political parties (interview with Mercy Buku, independent consultant, former senior manager, Money Laundering Reporting, Risk Management, Safaricom Kenya).

Box 3. Are customers able to make informed and "rational" self-protection decisions?

It is a commonly accepted principle that consumers should bear some responsibility for risk mitigation. However, the evidence strongly suggests that consumer efforts are often suboptimal. For example, consumer perceptions of risks and their consequences are not always well aligned with those they actually face, as in the case of fraud where perceptions are substantially higher than what customers actually report experiencing. Consumers may be limiting their use of services that actually present lower risks of financial loss and harm than informal alternatives.

Ugandan customers report agents charging for deposits and say agents charge differing fees for the same services, leading them to suspect many of the fees are improper (Ogwal 2015). In Tanzania, DFS users also suspect agents of charging improper fees, and many say the fees agents charge do not match the fee posters in agent shops (InterMedia 2014).

Part of the suspicion about unauthorized fees is likely due to poor fee disclosure, making the fees unclear. More data are needed to determine the extent of actual versus perceived overcharging, though even the perception of overcharging leads to less trust in agents and in DFS.

Solution example: Telenor EasyPaisa in Pakistan combined a tiered commission model with a minimum deposit to reduce split transactions.

7. Data privacy and protection

Risk-related issues include the following:

- Compromised safety of digital data
- Poor understanding of new uses of personal data
- Unforeseen outcomes, such as identity theft or money laundering

As consumers take up DFS, many are creating digital footprints for the first time, and the resulting data have potential value for companies, governments, and individuals themselves. For example, a number of providers are beginning to use mobile data[32] to create credit scores and offer loans to customers without requiring collateral (Chen and Faz 2015).

Box 4. Under what conditions are unauthorized fees fraudulent?

In some countries, unauthorized fees are so common customers consider them a "cost of doing business." Does this make them less fraudulent? According to most common definitions of fraud, unauthorized fees qualify as fraud perpetrated against customers. For example, one study on mobile money fraud used this definition:

> "[Fraud is] the intentional and deliberate action undertaken by players in the DFS ecosystem aimed at deriving gain (cash or e-money) and/or denying other players revenue and/or damaging the reputation of other stakeholders" (Mudiri 2012).

In some cases, however, customers consider extra fees to be legitimate payment for services rendered. In Bangladesh, for example, where many customers have agents perform OTC transactions for them rather than registering an account and performing transactions themselves, customers often consider the unauthorized cash fees to be a payment to the agent for the time and effort involved in conducting the transaction.

Whether an unauthorized fee is considered fraud by customers may depend on their awareness of proper fees and their willingness to pay for what they consider extra services. Some markets, such as Kenya, that demonstrate higher discipline and enforcement around transparency have lower levels of suspicion of and overcharging by agents.

Compromised safety of digital data

Customers are concerned about the safety of their data and the potential for it to be compromised. Customers in the country case studies said they had received fraudulent calls and SMS messages and that the callers had information about them that could have been obtained only if the caller had access to their private information. They suspected employees of the DFS provider had gained unauthorized access to their account and used that information for fraud.

Poor understanding of new uses of personal data

As new services are developed that use mobile call records and payments data, some consumers express concern about the safety, privacy, and use of their data

32 Such as call and SMS records and mobile money transaction data.

for such purposes. A recent study conducted by CGAP showed consumers in Tanzania worried about how their data might be used by such a service and what information would be accessed. They also expressed confusion over what kind of information is included in mobile data and concerns that accessing mobile data includes listening in on phone calls and reading text messages (it does not). In this case, simple SMS messages and informational materials were effective in improving basic understanding of digital data and combatting misconceptions, though user understanding was still limited. Perhaps unsurprisingly, the study also showed that customers were willing to allow this single-use access to their data in exchange for the possibility of getting a loan or financing on better terms (Mazer et al. 2014).

Poor understanding of data uses can be exacerbated by poor practices in ensuring that customers are provided, can access, and are in a position to understand data provisions in DFS terms and conditions. Often customers are required to accept terms and conditions found only on a website, which is impractical for many, particularly low-income or rural customers who typically lack access to internet and internet-enabled phones (Cook and McKay 2015).

Unforeseen outcomes

A lack of data privacy can harm customers in a number of other ways that the average customer may be unable to conceive of or foresee. For example, stolen data can be used for identity fraud or other criminal purposes, as well as harming any developing credit profile the user may have. Lack of data privacy can pose nonfinancial risks as well, such as access by government entities to sensitive personal data or its use for political purposes. Personal data have value that may evolve into a new class of assets even for lower-income customers.

Box 5. Emerging customer risk areas

The DFS landscape is constantly changing, and the risks consumers face evolve along with the products. The evidence reveals that in addition to the seven current risks explored in this paper, a new generation of challenges is on the horizon. Here are three examples:

Digital delivery of more complex products. As less familiar or more complex DFS—such as mobile credit or mobile insurance—enter the market and sometimes scale very rapidly, extra attention will be needed to ensure clients understand important terms, conditions, and risks. This is all the more challenging in light of limitations of information provided on the screen of a basic handset. For example, when mobile credit borrowers "virtually" complete all their loan requirements from their phone, they may not have (or take) an opportunity to ask clarifying questions about pricing, repayment requirements, or consequences of late or nonrepayment. Mobile insurance is growing fast in multiple markets and may also challenge consumer understanding, especially since the policy is typically bundled with another service or offered as a reward for payment activity. Agents typically used by customers may know little about these new, more complex products if they do not receive specific training.

Smartphone use and financial apps. GSMA predicts that four out of every five smartphone connections will be in developing countries by 2020; 61 percent of the mobile finance deployments it tracks are now available via an app (GSMA 2014e and 2015). This trend has the potential to enhance the customer experience and reduce customer risks in some of the main areas identified in this research while also raising new consumer risk concerns. For example, the rich user interface and enhanced functionality of smartphones is potentially far more intuitive and user-friendly than the current USSD menus used by 86 percent of mobile money services. Consumers might also benefit from increased competition, since diverse FSPs could offer DFS through apps without having to partner with a telco (Mas and Porteous 2014). However, new or different risks may also arise in this ecosystem, such as new forms of fraud, or unauthorized access to customer data, especially if current user behavior, such as weak PIN use, persists and as more players partner to deliver DFS. The potential for malware may also merit attention.

Additional data privacy and protection concerns. Expanded use of digital data for financial services delivery is nascent. On the privacy front, neither providers nor customers can yet assess with much certainty the trade-offs that will surface among principles related to data ownership, processing, storage, and security. The challenge of achieving consensus and putting in place balanced and practical data governance measures should not be underestimated. New disclosure methods will be needed to inform clients more meaningfully about their rights and the ways their data might be used. On the security front, additional effort will almost certainly be needed to ensure that nonpublic customer data are protected from outside hackers and other unauthorized access and use. These challenges extend far beyond digital finance, of course, and it could be helpful to engage with data experts and advocates in adjacent fields.

Customer Self-Protection against DFS Risks. The evidence analyzed for this section revealed various ways DFS customers self-protect against actual or perceived risks. While some self-protection measures may be effective, such as keeping one's PIN secret, others fail to adequately protect customers and can suppress use and activity levels. Reported self-protection behavior and attitudes include the following.

Not leaving money in the system. Some customers limit the balance kept in their mobile wallet to avoid perceived risks—such as money "disappearing." They typically do this by cashing out as soon as they receive a transfer.

Limiting the ways they use the service. Some customers report using DFS only in emergencies and keeping the number of transactions to a minimum, due to difficulties they have experienced such as losing money as a result of keystroke errors. Some users also report limiting the types of services they access (e.g., only checking account balances or conducting money transfers) due to perceived risks with other services (De Koker and Jentzsch 2013).

Using OTC transactions rather than mobile wallets. Many customers explain OTC use as a self-protection mechanism. Customers in Bangladesh and Uganda report that they consider it safer to have an agent complete an OTC transaction than to transact themselves and risk making a costly mistake (InterMedia 2014).

Qualitative research shows that Colombian users often blame themselves if something goes wrong, despite reporting common DFS self-protection practices.[33] They also say they do not feel entitled to or confident in complaints handling processes. In fact, consumer research in multiple markets confirms cultural barriers to seeking recourse and a general lack of confidence among lower-income or less experienced consumers that complaining will yield results (Chapman and Mazer 2013).

Ultimately, customer self-protection represents a small part of a much larger effort that is required from others, including providers, regulators, and other stakeholders who are likely to have superior information about risks and their consequences. The next sections explore the roles of—and suggest priorities for—providers and other DFS stakeholders, both independently and collectively, to more effectively mitigate consumer risks.

III. Five Priorities for Industry to Identify, Test, and Scale Solutions

The diverse consumer-side evidence reviewed for this Focus Note strongly suggests that providers can and should take action to improve the safety, reliability, and performance of DFS products, channels, and systems for their customers. Doing so may not only help reduce barriers many people face in taking up and transacting more intensively. It may also be a precondition for mass uptake of the higher-margin services, such as credit, that are central to the longer-term business case for many providers.

Leadership by DFS providers and other industry actors is most needed and timely in five priority areas:

1. Improve service reliability and robustness
2. Make the customer interface more user friendly
3. Strengthen agent quality, management, and liquidity
4. Combat customer-affecting fraud
5. Improve handling of complaints, queries, and redress

Each priority area explores types of actions that are being or could be taken. While it is outside of the scope of this paper to offer guidance on best practices or implementation strategies, illustrative examples of FSP-led solutions that are reported to address these priorities are offered.

1. Improve service reliability and robustness

As the number one complaint among DFS customers, reducing network downtime should be a top priority for FSPs and their third-party service providers. Improving system reliability—to

33 Such as "never travel to an agent alone," "do not speak loudly (at the agent)," and "cover your hand when typing your PIN" (CGAP 2014f).

Table 1. Provider examples to improve service reliability and robustness

Solution areas	Examples in Action
Internal coordination for problem solving	Airtel Uganda's mobile money platform team deals directly with the IT/GSM team through a dedicated IT team member, to determine which problems are platform problems and which are GSM problems, helping identify problems geographically and improve efficiency of addressing them.
Regular network system testing and real-time monitoring	Airtel Money Uganda combines incremental and full system backups with a system-uptime monitoring tool that provides alerts and reports.
	In Nigeria, a study found predictive/condition-based maintenance is more effective than traditional preventive/scheduled maintenance approaches for maintaining GSM reliability (Ubani and Nwakanma 2013).
Reliable platform that can integrate smoothly with other ecosystem players	Late in 2014, MTN-Uganda made a switch to a new platform that is expected to markedly improve overall service reliability.
	The company also added 117 new 2G sites and 130 new 3G sites in the first half of 2014 (MTN Uganda 2014).
	Airtel India has invested heavily in state-of-the-art cable systems expected to improve Airtel Money operations with network resilience and redundancy (Bharti Airtel 2014).
	MobiCash in Bangladesh leverages a network of 60,000 airtime resellers and other mobile communication products and infrastructure throughout the country (Noor and Shrader 2015).
	Telecel-Zimbabwe found a dedicated USSD platform for mobile money services reduced service interruptions.[a]
Prices and business rules that ensure adequate bandwidth allocation	Prices per USSD session range from US$0.01 in Nigeria, to US$0.06 in Kenya and South Africa (CGAP 2014b).

a. Interview with Cloud Nhau, sales manager, Mobile Financial Services of Telecel Zimbabwe.

enable consistent access to services and accounts, timely settlement, and transaction verification—is a complex task, however. In some models, fast-growing DFS services must compete for platform capacity and investment with other business lines. Joint ventures or outsourcing arrangements are also common, resulting in more complex functionality and communication/coordination demands across the parties' systems.

Opportunities and developments in this area include the following:

- Conduct regular network system testing and real-time monitoring and have adequate business continuity and contingency plans in place.[34]
- Operate mobile money on a reliable platform that integrates smoothly with other ecosystem players.
- Set prices and business rules to ensure adequate bandwidth allocation for DFS and set more practical USSD session time-outs and service interruptions (Hanouch and Chen 2015; Mazer 2015).
- Carefully establish relationships and responsibilities among players at service inception.[35]

For FSPs engaging with third-party providers that operate a DFS platform or service, it is critical to ensure the above points are discussed and integrated into the relationship and contractual agreements. FSPs need to ensure their customers are still protected as they transact across multiple platforms, even though the FSP does not fully control reliability of the service.

2. Make the customer interface more user friendly

User-interface improvements can increase value to both customers and providers since complex and confusing interfaces introduce opportunities for customer loss, suppress activity levels, and contribute to OTC rather than independent mobile wallet or other digital interface-based transactions. In the near term, providers will need to weigh the financial and technical feasibility of some of these measures against the potential benefits; in the longer run, additional cost-effective solutions may be coming on line. When FSPs are engaging with third parties to use their platforms to provide

34 See, e.g., Parada and Bull (2014) and GSMA (2015).
35 Contract provisions and compensation arrangements can reinforce the ongoing commitment of parties (Lake 2013).

Table 2. Provider examples to make the customer interface more user friendly

Solution areas	Examples in action
Menus and instructions in local language	Airtel Money Uganda offers its menu in Luganda as well as in English.
	M-PESA in India is available in Hindi, Bengali, Marathi, Gujarati, and English, and more regional languages are planned.
	Tigo Chad uses IVR to convey messages and instructions for mobile money (GSMA forthcoming).
Reduced USSD timeouts	Tigo Kilimo in Tanzania modified its menu, replacing open-ended questions with multiple-choice questions that were easier and quicker to answer.
	Eko in India has a one-step process that is easy for customers to navigate.
Reduced keystroke errors	DBBL in Bangladesh creates a customer's account number by adding a "check digit" to the end of the mobile number. If the sender enters the wrong account number, it is unlikely the check digit will match (CGAP Country Case Study, Bangladesh, 2015 [unpublished]).
	Airtel Money in Uganda displays the recipient's name when the customer inputs the phone number.
PIN alternatives	In Colombia, Daviplata creates a temporary PIN sent by SMS for G2P recipients that can be used at an ATM or agent within a short time window.
	Novopay India is a mobile payment company that uses the Aadhaar biometric scanner to allow people to conduct banking transactions from neighborhood shops (Indiatimes 2015).

DFS to end-customers, reviewing user interface functionality is critical.

Opportunities and developments in this area include the following:

- Offer the menu in local languages.
- Use interactive voice response (IVR) to convey messages and instructions for mobile money, including to users with literacy challenges.
- Decrease USSD timeouts by extending sessions, introducing inactivity timers between each menu or transaction rather than time-outs,[36] or designing a more intuitive, navigable menu (Mazer 2015; Noor and Shrader 2015).
- Redesign interfaces and processes to reduce keystroke errors, for example, by incorporating simple triggers to help customers confirm they are sending money where they intended ("check digit" or integration with address book to display the recipient's name before sending).
- Consider alternatives to PINs, such as biometrics or tokenization.
- Work toward developing more intuitive mobile applications on smart phones.
- Apply human-centered design and user acceptance testing, including pre-roll-out pilots and testing.[37]

3. Strengthen agent quality, management, and liquidity

Agents are the front line of contact for most DFS customers. The majority perform this role with integrity. Indeed, access to a sufficient number of well-trained, well-supervised, and well-supported agents is a key element in many of the solutions highlighted in this paper. Recent ANA research finds that agents who disclose service fees and who are well informed about the terms and conditions of their services process a higher number of transactions per day and have a competitive advantage compared to less transparent and knowledgeable agents (Anthony and Balasubramanian 2015). To the extent that customers can shift to other agents when they suspect or encounter overcharging, other agent misconduct, or poor service quality, this could help bring up standards of conduct, reduce customer risks, and improve customer value over time. In many markets, however, there is not sufficient agent penetration for customers to exercise choice.

Competition alone may be insufficient to ensure good conduct. Improved agent management, reinforced with appropriate incentives, can help improve

36 Interview with Khurram Sikander, Digital Payments senior advisor at Enclude Solutions.

37 This includes continually assessing customer needs through customer segmentation and diversifying the product base so as to cater to the needs of each segment.

Table 3. Provider examples to strengthen agent quality, management, and liquidity

Solution areas	Examples in action
Detailed agent selection criteria	Pakistan's Easypaisa analyzes data on airtime sales to verify financial health and liquidity of the business before approving a retailer as an agent.
High-quality induction training and regular refresher training	MTN Uganda provides six hours of training in the field for each new frontline employee of a cash-in/cash-out agent.
	Safaricom's M-PESA requires each new owner/manager to attend a full-day training in Nairobi.
	Orange in Côte d'Ivoire combines a half-day training in regional hubs with later field visits.
	Airtel Uganda organizes regular "field meets" where up to 500 agents get refresher training.
Strengthened liquidity management	In Bangladesh, cash and float are delivered to agents by an employee of the aggregator, resulting in more frequent rebalancing and fewer denied transactions than in East Africa (McCaffrey and Khan 2014).
	Vodacom Tanzania's master agents have toll-free numbers for agents to easily communicate liquidity needs.
	Airtel Uganda has numerous measures to help agents manage float, including aggregators that deliver float to agents, partnerships with 13 banks where agents can access float without waiting in lines, and super agents that the agent can visit to buy float.

transparency and compliance with conduct rules and procedures; reduce fraud perpetrated by agents on customers; improve data handling; and improve customer choice, empowerment, and recourse when things go wrong. For many FSPs the agent network is the key operational expense. They face difficult choices in deciding how to balance the quality of their agent network with extending their service footprint and maintaining the viability of the business for agents. Existing models are often stressed by scale, additional DFS offerings, and other market dynamics.

Opportunities and developments in this area include the following:

- Develop selection criteria that reflect the more complex role of DFS agents versus traditional airtime retailers (e.g., skills and assets required for satisfactory know-your-customer (KYC) processes, customer training and support, financial record-keeping, fraud detection).
- Improve quality and cost-effectiveness of induction training and deliver regular refresher training.
- Set reasonable float requirements to balance reach with capacity and strengthen the liquidity management model over time.
- Use alerts to inform agents of float balances.
- Explore cash-balancing service options to support agents that regularly struggle to rebalance.
- Strengthen agent management and oversight.[38] Leverage agent aggregation points and agent network managers to serve as a secondary level for agent training and customer redress.
- Introduce and enforce graduated agent sanctions for compliance violations.[39]

4. Combat customer-affecting fraud

Fraud can result in a DFS customer's direct loss of funds, so effective fraud controls are critical for consumer trust. More complex digital products such as savings and credit will increase fraud opportunities, incidence, and dollar value. Many DFS providers lack data analytic capacity to detect suspicious trends in behavior and transactions, which is a key building block for fraud monitoring and management systems. Adequate data handling practices are also integral to preventing fraud such as identity theft. Greater attention to fraud that affects users is thus prudent and important for consumer confidence, revenue assurance, and the reputation of DFS overall and provider brands more specifically.

38 For example, through automated onsite inspection protocols, offsite system checks, or mystery shopping for compliance.

39 E.g., suspension, termination, and blacklisting of agent assistants and directors, as well as claw-back of fraudulently earned commissions. Safaricom's M-PESA achieved a large reduction in OTC (known as "direct deposit" in Kenya) by implementing commission claw-back measures.

Table 4. Provider examples to combat customer-affecting fraud

Solution areas	Examples in action
Improve customer awareness of fraud schemes	Safaricom's M-PESA uses SMS alerts, radio announcements in local dialects, newspaper ads, and other efforts to improve customer awareness.
	MTN Uganda uses social media to learn of new fraud schemes from customers.
	Colombian FSPs advocate consumer self-protection, informing customers about risks, how to protect themselves, and where to complain (CGAP 2014f; Ahmed and Gomez 2015).
	Banco WWB in Colombia mandates that agents and sales officers provide product security tips to customers upon opening an account or registering for mobile money (CGAP 2014f; Ahmed and Gomez 2015).
	In Kenya the PIN Yako Siri Yako (Your PIN Your Secret) campaign for M-PESA achieved significant gains in customer awareness and behavior.
Introduce measures to reduce unauthorized SIM swaps	In Tanzania, providers have imposed a "quarantine" period after switching SIM cards in which the mobile money PIN cannot be changed.
	ABSA in South Africa places a temporary hold on a customer account if it becomes aware of a SIM swap. The customer has 36 hours to authenticate and advise ABSA if the SIM swap was legitimate.
Ensure agent relationship and commission structures incentivize ethical behavior	Finamerica in Colombia requires agents to work two years as a community leader before being able to perform transactions. Community leaders coordinate financial education and other community development activities on behalf of Finamerica (CGAP 2014f).
	Telenor Pakistan's Easypaisa combined a tiered commission model with a minimum deposit amount to reduce split transactions.
Data analytics and sharing for fraud detection	Safaricom Kenya developed more sophisticated data analytics measures over time. In Tanzania, mobile money operators and banks each have coordination initiatives to combat fraud.
Data handling	F-Road in China uses a SIM overlay card, in which a thin SIM is placed on top of the customer's regular SIM, so that financial activity is tied to the overlay card while phone activity is tied to the regular SIM. The data sent through the overlay card are encrypted, so only the FSP has access to the data.
	Banco WWB in Colombia set up its mobile banking process to ensure data security by leaving no information, notifications, or geolocation information on clients' phones (CGAP 2014f).

Opportunities and developments in this area include the following:

- Combat phishing, fraudulent calls and messages, and caller ID spoofing through more effective customers' awareness and measures that improve their ability to recognize and resist fraudulent messages. Investment in mass-market campaigns that address these issues may pay off for the business or the sector.[40]
- Introduce measures to reduce SIM swaps and detect related scams.[41]
- Improve data protocols and controls to prevent access by fraudsters and other unauthorized parties.
- Improve agent vetting, training, and monitoring in this area; block agents' accounts when fraud is reported or suspected; and sanction individuals once fraud is proven.[42]
- Ensure that the agent model and commission structures incentivize ethical conduct, for example, by rewarding active use over registration, to the extent that activity can serve as a rough proxy for customer satisfaction.[43] Direct, sustained,

40 Examples from Colombia, Kenya, and other markets include transmitting simple fraud prevention awareness messages by text, holding road shows, encouraging the media to highlight cases of fraud and prevention measures, and partnering to sponsor TV ads and commercial programming such as evening soap operas that showcase common scams.

41 Such as freezing mobile money accounts for a period of time and requiring revalidation in-person at a customer care center, or sending alerts to an alternative customer contact if a SIM is swapped.

42 Carry out ongoing transaction monitoring to detect fraud patterns and facilitate the profiling, arrest, and prosecution of fraudsters; cooperate with law enforcement agencies in identifying and prosecuting fraudsters.

43 Multiple experts interviewed for this research observed that operators may hesitate to crack down too hard on agents charging unauthorized fees when they are trying to build out the agent network and agent profitability is not yet widely achieved or proven without this extra revenue.

long-term relationships by FSPs with their agents improve service quality, agent reliability, and compliance with service quality standards and consumer protection principles.
- Improve training of call center staff to escalate and handle fraud cases, and create effective feedback loops with the FSP's internal fraud mitigation systems.
- Strengthen data analytics capacity for fraud detection. Develop mechanisms for coordinated sharing of data and information among FSPs to better detect and respond to fast-moving frauds.
- Ensure business partners and merchants are also trained on fraud prevention measures.

5. Improve handling of complaints, queries, and redress

For nonbank DFS providers, the demands placed on their recourse systems by fast-scaling financial services are quite different from those associated with their core telecommunications services or other retail operations. Because recourse is important to consumers and affects all the other risk areas, providers will need to carefully examine appropriate recourse options for their DFS business line (Chapman and Mazer 2013). Customers transitioning from OTC to wallets will need the skills and confidence to manage recourse without the assistance of agents. As DFS beyond payments come on line, they will generate new recourse demands, including more need for call center and other customer support staff to help the customer navigate recourse when multiple parties are involved in DFS delivery.

Opportunities and developments in this area include the following:
- Communicate clearly to customers that they should complain when they have a problem and how best to do so (and to which party).
- Better equip agents through training and scripts to help address simple customer problems. Provide agents with a dedicated hotline so they can help the customer get a timely response and hand off more complex or important cases (e.g., suspected fraud, repudiation).
- Improve service standards for recourse, such as a commitment to timely resolution of most complaints and a tracking system that issues tickets and regular updates to customers.

Table 5. Provider examples to improve handling of complaints, queries, and redress

Solution areas	Examples in action
Better equip agents to help address problems	In Colombia, Bancolombia created a dedicated agent hotline.
Designated and specialized call center staff	Digicel in Haiti trained and allocated call center staff specifically for their Tcho Tcho Mobile (TTM) money service, through which government social cash transfers were paid. Digicel doubled the TTM-dedicated call center staff.
	Davivienda in Colombia has hired former G2P beneficiaries to work in the call center, creating jobs and relieving pressure on the call center from increased complaints after taking on G2P distribution (CGAP 2014f).
	In Tanzania, providers revised their policies on who can carry out "wrong-number" reversals (e.g., transferring this function from the headquarters finance department to the call center).
High service standards	Tigo-Ghana aims for full resolution of customer complaints within 24 hours, and customers receive a ticket number and regular progress updates. The system triggers an emergency procedure for unresolved complaints affecting more than five customers within a 30-minute window.
	Customers of Eko (India) can lodge complaints at numerous touch points, including agents, customer care centers, or the call center, and can track the status of their cases on their mobile (Chapman and Mazer 2013).
	WFP in Kenya launched a new hotline. To inform beneficiaries it offered training, leaflets, and posters at merchants. Two staff with wide-ranging language abilities track calls via a CRM system.
Communication about recourse options	Telecel-Zimbabwe uses radio and road shows.

Box 6. Industry is taking the initiative on responsible digital finance

While many FSPs are already acting on customer risk mitigation, collective action among firms or cross-industry efforts may further improve the efficacy, efficiency, and scope of these measures. A noteworthy global example of this is GSMA's new mobile money code, which is intended to be applied industry-wide and has gained endorsement from 12 large MNO groups[a] representing more than 82 mobile money deployments operating in 51 countries. Once these industry-wide minimum requirements are translated into global standards, the groups and their operating companies will pilot them. After a period of self-assessment, signatories will then be subject to external verification of their adherence to the standards. The code's eight principles address common challenges:

1. Safeguard customer funds against risk of loss
2. Maintain effective mechanisms to combat money laundering and terrorist financing
3. Equip and monitor staff, agents, and entities providing outsourced services to ensure that they offer safe and reliable services
4. Ensure reliable service provision with sufficient network and system capacity
5. Take robust steps to ensure the security of the mobile network channel
6. Communicate clear, sufficient, and timely information to empower customer to make informed decisions
7. Develop mechanisms to ensure that complaints are effectively addressed and problems are resolved in a timely manner
8. Collect, process, and/or transmit personal data fairly and securely

The code aims to ensure at a high level that services are sound, the channel is secure, and the customer is treated fairly. It mirrors quite closely the priorities suggested by the consumer evidence presented in Section II and the priority action areas for industry outlined in this section. Other promising examples of industry initiatives are noted in Annex 3.

a. Airtel, Avea, Axiata, Etisalat, Millicom, MTN, Ooredoo, Orange, Telenor, Telma, Vodafone, and Zain (GSMA 2014c).

- Categorize customer complaints and designate specialized staff with scripts and procedures for the most common problems.
- Separate DFS call center function and recourse policies, procedures, and standards from other business lines.

Individual providers will need to assess their priorities and available cost-effective solutions in light of their business model and objectives. Each FSP will need to analyze which customer risk mitigation measures are most important and feasible based on their business model, product line, and goals. Solutions do not come without a cost, and some (e.g., enhanced agent oversight or network/platform capability) are more complicated and expensive to address than others (e.g., better signage, customer communication, or call center procedures). Developing a clear business case that demonstrates the benefits—such as cost savings, revenue assurance, revenue gains from increased activity levels and cross-sale, and indirect benefits like reduced churn or savings on airtime distribution—can help justify these investments. Protecting the company's reputation is another consideration, and often an important one for telco, banking, or retail groups with major brand value. And in some settings, action in these customer risk areas will also be motivated by the need to comply with new regulations or to reduce the chance of the regulator imposing additional or more onerous business conduct or service requirements.

Given competing investment priorities and the time it takes to achieve scale and robust revenues, additional spending to improve customer risk mitigation may not be an easy sell. More attractive avenues may exist to optimize revenue and bandwidth in the short term. Yet, GSMA reports that mobile financial services investment is trending up and profitability is improving.[44]

IV. Complementary Action Needed from Regulators and Other Actors

Risks are unavoidable in the delivery of financial services, digital or otherwise. The evidence and analysis points to common problems that can erode consumer trust, impact overall customer activity,

44 Eighty percent of respondents to the GSMA mobile financial services survey reported they had maintained or increased their investment. For example, half had already migrated to an improved platform or planned to do so in 2015 (GSMA 2015).

and affect the pace and type of DFS growth. FSPs hold the primary responsibility for preventing and resolving customer-facing problems and may be better positioned than other parties to identify related risks and mitigate them. And indeed, the solutions landscaping research conducted for this paper suggests growing industry awareness and initiative to tackle this agenda.

However, further intervention is also needed to motivate and reinforce industry self-regulation and protect consumers. Regulators and supervisors can and should introduce balanced and well-tailored measures in support of responsible digital finance.

While growing pains are inevitable in innovative and rapidly expanding markets, some problems pose unacceptable risks to low-income and vulnerable consumers. Adequate solutions may not be readily available or they may not be widely adopted in the course of normal market development. For example, in financial markets worldwide we observe problems such as opaque product pricing and unfair contract terms that persist due to weak incentives for FSPs to address them. Other complex problems—such as tracking fast-moving fraud or maintaining adequate data security as the value chain extends—may require either substantial effort beyond what market actors are willing to invest or collective action that is difficult to organize without external support. Market conduct and consumer protection regulations aim to address such market failures.

Regulators in many markets are taking action to better understand and mitigate risks associated with different DFS products, services, and delivery channels (see Box 7). Before approving a new mobile money scheme, the Colombian Financial Superintendence requires DFS providers to submit a plan identifying consumer risks and mitigation solutions (CGAP 2014f). Countries such as Bangladesh, Pakistan, and Tanzania have put in place formal industry dialogue and coordination processes. In Kenya the regulator convenes regular stakeholder forums to discuss market trends and issues such as FSP measures to address various types of fraud and agent compliance violations. Peru offers another relevant example of close supervisor-industry cooperation. To advance financial inclusion, the banking association launched "Modelo Peru," a private-sector project to develop an open e-money platform—also open to nonbank FSPs including telcos and microfinance institutions—that will ensure transparency (e.g., plain-language disclosure of transaction fees before PIN entry) and data security protections for the lower-income consumers it seeks to serve. This work has proceeded in close coordination with the banking supervisory agency.

Additional regulators and supervisors with financial inclusion mandates and roles—especially those charged with overseeing high-growth DFS markets—are adopting new measures (such as sector-specific rules for DFS)[45] and adapting existing market conduct and consumer protection regimes to respond to evolving consumer risks. Proportionate and well-enforced rules can reinforce industry risk mitigation measures and standards by codifying acceptable practices, which in turn can build consumer confidence and minimize reputation risk in DFS overall. They can ensure more consistent and widespread adherence to good practices and a more competitive marketplace. They may be needed to address gaps where consumers face significant risks but industry action falls short, whether due to weak incentives, coordination failures, or FSPs' lack of capacity and knowledge.

Development agencies and researchers can also contribute to responsible digital finance by helping fill gaps in knowledge and supporting improved identification and promotion of effective provider practices and regulation.

Providers and regulators have acknowledged that they do not understand well enough how and how frequently consumer risks impact low-income DFS market segments. They need more and better data and analysis on the incidence of different risks in different markets, business models, and

45 E.g., new DFS regulations have been issued in countries including Colombia, India, Kenya, and Liberia in the past year (GSMA 2015).

Box 7. Responsible digital finance on the agenda of regulators

Regulatory and supervisory experience in addressing DFS customer risks beyond safeguarding of customer funds[a] is relatively new but emerging. Recent publications by AFI and BCBS reveal substantial alignment in the topics and practices to be prioritized. AFI's 2014 guidelines for supervisors on protecting DFS consumers proposed three common objectives for regulation and supervision: (*i*) consumers receive sufficient information to make informed financial decisions; (*ii*) rules prevent unfair practices by FSPs; and (*iii*) consumers have access to recourse mechanisms to resolve disputes. The guidance focuses on six specific vulnerabilities that open DFS consumers up to risks, with associated rules or other measures to address each risk area:

- Inadequate or incomplete information—disclosure and recourse rules and standards
- Technology-related risks—minimum standards in product design
- Agent conduct—standards for agent selection, training, and oversight; incentives for good conduct; review of contract templates for agents and outsourced agent network managers; clear communication to customers that FSPs are liable for conduct of their agents
- Limited consumer exposure to and experience with new services and service providers—adequate operational risk management systems to ensure safety and soundness of the business, business model, and customer funds
- Customer data privacy concerns—rules on customer data ownership, confidentiality, collection, sharing, correction, and control mechanisms
- Third party and outsourcing—FSP retention of liability when it delivers services through telcos or agents, including responsibility for creating and maintaining an adequate complaints handling and recourse mechanism

A recent BCBS "range of practice" report examined implementation of measures relevant for DFS and financial consumer protection. For example, prudential regulators increasingly require FSPs to analyze the operational risk involved before launch of a new product, service, or delivery channel aimed at financial inclusion. Most supervisory authority respondents reported attending to cybercrime and security, disputed transactions, data security breaches specifically related to the use of mobile phones or other mobile devices, and loss of customer funds due to agent fraud. The survey also revealed several "emerging priorities" to address the most common consumer protection issues related to regulating nonbank e-money issuers or distributors, including complaints handling rules (46 percent), protection of data privacy and confidentiality (43 percent), prohibition of unfair or abusive practices (39 percent), provision to the consumer of a copy of signed agreement (39 percent), pricing transparency (29 percent), and setup of a complaints handling unit or function (29 percent).

a. The 2013 survey covered regulatory and supervisory practices related to financial institutions that are relevant financial inclusion. BCBS received 52 valid responses representing 59 jurisdictions (including the eight-member West African Economic and Monetary Union) that were evenly spread across country income groupings.

b. Jurisdictions commonly address safeguarding customer funds through rules regulating which providers are allowed to offer DFS, capital requirements, segregation and intermediation of funds, and other measures to protect customers' stored mobile money value by ensuring that relevant actors are solvent and maintain adequate liquidity. (See, e.g., Tarazi and Breloff 2010). Such rules are highly relevant to protesting consumers' welfare but fall outside the scope of this paper, which focuses on adequacy of product offerings, business conduct, and operational risk management.

DFS products, including on models beyond mobile money (since the available evidence is heavily skewed toward this sector). Consumer research[46] and mystery shopping can generate direct information on consumer perceptions and experience.[47] Consumer-focused organizations can help with research and advocacy on common problems, queries, or complaints. By sourcing and applying behavioral insights, providers and regulators can find better ways to nudge consumers toward more effective self-protection and help probe beyond the overall picture of DFS growth to understand drivers of trust, uptake, and use.

V. Toward a Responsible Digital Finance Ecosystem

DFS innovations and market developments offer exciting opportunities for lower-income people with inadequate financial service options. Along with great scope for continued expansion, there are some clear barriers if DFS is to realize its potential. All stakeholders—FSPs, other industry actors, regulators and supervisors, development agencies, consumer advocates, researchers, and consumers themselves—have a role to play in making digital finance work for the poor. DFS providers need to generate more and better solutions and proactively

46 See, e.g., Seltzer and McKay (2014).
47 See Mazer et al. (forthcoming).

adopt emerging industry standards. Regulators need to invest in deeper understanding of the business models and products, monitor evolving risks, and put in place effective and proportionate measures to reinforce industry efforts and address gaps. Governments, providers, and others need to cooperate to improve consumer awareness and capability initiatives. Consumers need more confidence, choice, and voice to self-protect and realize the gains that DFS offers them (Koning and Cohen 2015).

The success of responsible digital finance initiatives can make an important contribution to win-win-win outcomes for consumers, the providers that serve them, and societies seeking more inclusive financial systems.

References

AFI (Alliance for Financial Inclusion). 2012. "Mobile Financial Services: Technology Risks." Bangkok: AFI Mobile Financial Services Working Group, Guideline Note, September. http://www.afi-global.org/sites/default/files/pdfimages/AFI_MFSWG_guidelinenote_TechRisks.pdf

———. 2014. "Mobile Financial Services: Consumer Protection in Mobile Financial Services." Bangkok: AFI Mobile Financial Services Working Group. Guideline Note No. 2. March. http://www.afi-global.org/sites/default/files/publications/mfswg_guideline_note_7_consumer_protection_in_mfs.pdf

Ahmed, Wajiha, and Natalia Gomez. 2015. "Papayas and Digital Finance: Emerging Consumer Risks in Colombia." Washington D.C.: CGAP, January. http://www.cgap.org/blog/papayas-and-digital-finance-emerging-consumer-risks-colombia

Almazan, Mireya, and Nicolas Vonthron. 2014. "Mobile Money for the Unbanked. Mobile Money Profitability: A Digital Ecosystem to Drive Healthy Margins." London: GSM Association, November. http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2014/11/2014_Mobile-money-profitability-A-digital-ecosystem-to-drive-healthy-margins.pdf

Anthony, Leena, and Karthik Balasubramanian. 2015. "The Better Service Agents Provide, the More Business They Do." Nairobi: Helix Institute of Digital Finance, March. http://helix-institute.com/blog/better-service-agents-provide-more-business-they-do

Arenaza, Sonia. 2014a. "Digital Financial Services and Microfinance: State of Play. A Framing Note to Inform the Evolution of the Client Protection Standards." Washington D.C.: Accion and Smart Campaign, August. http://www.smartcampaign.org/storage/documents/Tools_and_Resources/20140821_EoS_DfS_MFIs.pdf

———. 2014b. "Potential Risks to Clients When Using Digital Financial Services. An Analysis Report to Inform the Evolution of the Client Protection Standards." Washington D.C.: Accion and Smart Campaign, September. http://www.smartcampaign.org/storage/documents/Tools_and_Resources/EoS_Risk_identification_and_analysis_vSA_AR_LT.pdf

BCBS (Basel Committee on Banking Supervision). 2015. "Range of Practice in the Regulation and Supervision of Institutions Relevant to Financial Inclusion." Basel: BCBS, January.

Bharti Airtel. 2014. "E-commerce and E-business." Presentation. New Delhi: Bharti Airtel. http://www.slideshare.net/nitishbaweja/implementation-of-e-commerce-in-airtel

CaLP (Cash Learning Partnership). 2013. "Protecting Beneficiary Privacy. Principles and Operational Standards for the Secure Use of Personal Data in Cash and E-Transfer Programmes." Oxford: CaLP. http://www.cashlearning.org/downloads/calp-beneficiary-privacy-web.pdf

CGAP (Consultative Group to Assist the Poor). 2013a. "Fraud and Customer Protection in Mobile Money: Framing Study [Tanzania]." Unpublished. Washington D.C.: CGAP.

———. 2013b. "Electronic Payments with Limited Infrastructure. Uganda's Search for a Viable E-Payments Solution for the Social Assistance Grants

for Empowerment." Washington D.C.: CGAP, March. http://www.cgap.org/sites/default/files/eG2P_Uganda.pdf

———. 2013c. "Helping Ti Manman Cheri in Haiti. Offering Mobile Money-Based Government-to-Person Payments in Haiti." Washington D.C.: CGAP, July. http://www.cgap.org/sites/default/files/eg2p_Haiti.pdf

———. 2013d. "Cash for Assets. World Food Programme's Exploration of the In-Kind to E-Payments Shift for Food Assistance in Kenya." Washington D.C.: CGAP, September. http://www.cgap.org/sites/default/files/eG2P_Kenya.pdf

———. 2013e. "Striving for E-payments at Scale. The Evolution of the Pantawid Pamilyang Pilipino Program in the Philippines." Washington D.C.: CGAP, November. http://www.cgap.org/sites/default/files/eG2P_Philippines.pdf

———. 2014a. "Financial Inclusion for the Poorest Women in Pakistan." Presentation. Washington, D.C.: CGAP, 10 January. http://www.slideshare.net/CGAP/financial-inclusion-for-the-poorest-women-in-pakistan

———. 2014b. "Mobile Payments Infrastructure Access and Its Regulation: USSD." Commissioned to Genesis Analytics. Washington D.C.: CGAP, May. http://www.cgap.org/sites/default/files/Working-Paper-Mobile-Payments-Infrastructure-Access-and-Its-Regulation-May-2014.pdf

———. 2014c. "Emerging Consumer Risks in Digital Financial Services in Uganda." CGAP Country Case Study. Washington D.C.: CGAP, October.

———. 2014d. "Emerging Consumer Risks in Digital Financial Services in the Philippines." CGAP Country Case Study. Washington D.C.: CGAP, October.

———. 2014e. "Emerging Consumer Risks in Digital Financial Services in Bangladesh." CGAP Country Case Study. Washington D.C.: CGAP, October.

———. 2014f. "Emerging Risks to Consumer Protection in Branchless Banking: Key Findings from Colombia Case Study." CGAP Country Case Study. Washington D.C.: CGAP, December. http://www.cgap.org/sites/default/files/Working-Paper-Colombia-Emerging-Risks-to-Consumer-Protection-Dec-2014.pdf

CGAP, MicroSave, and BFA (Bankable Frontier Associates). 2014. "Consumer Protection and Emerging Risks in Digital Financial Services. Perspective from Bangladesh, Uganda, Colombia, and the Philippines." Presented at the Responsible Finance Forum in Perth, Australia, 28 August. https://www.responsiblefinanceforum.org/wp-content/uploads/140828_CGAP-Presentation.pdf

Chapman, Megan, and Rafael Mazer. 2013. "Making Recourse Work for the Base-of-the-Pyramid Financial Consumers." Focus Note 90. Washington D.C.: CGAP, December. http://www.cgap.org/sites/default/files/Focus-Note-Making-Recourse-Work-for-Base-of-the-Pyramid-Financial-Consumer-Dec-2013_1.pdf

Chen, Gregory, and Pial Islam. 2014. "Bangladesh Consumer Insights: Is a Transition to Mobile Wallets Underway?" Presentation. Washington, D.C.: CGAP and pi Strategy, March. http://www.slideshare.net/CGAP/is-a-transition-to-mobile-wallets-underway-in-bangladesh

Chen, Gregory, and Xavier Faz. 2015. "The Potential of Digital Data: How Far Can It Advance Financial Inclusion?" Focus Note 100. Washington D.C.: CGAP, January. http://www.cgap.org/sites/default/files/Focus-Note-The-Potential-of-Digital-Data-Jan-2015_1.pdf

Cook, Tamara, and Claudia McKay. 2015. "How M-Shwari Works: The Story So Far." Forum 10. Washington, D.C.: CGAP and FSD Kenya.

De Koker, Louis, and Nicola Jentzsch. 2013. "Financial Inclusion and Financial Integrity: Aligned Incentives?" *World Development*, vol. 44, issue C: 267–80. http://econpapers.repec.org/article/eeewdevel/v_3a44_3ay_3a2013_3ai_3ac_3ap_3a267-280.htm

Dias, Denise, and Katharine McKee. 2010. "Protecting Branchless Banking Consumers: Policy Objectives and Regulatory Options." Focus Note 64. Washington, D.C.: CGAP. http://www.cgap.org/gm/document-1.9.47443/FN64.pdf

Di Castri, Simone. 2014. "Mobile Money Users at Center of New GSMA Code of Conduct." Blog. Washington D.C.: CGAP, November. http://www.cgap.org/blog/mobile-money-users-center-new-gsma-code-conduct

EIB (European Investment Bank) and UNCDF (United Nations Capital Development Fund). 2014. "Digital Financial Services in Africa: Beyond the Kenyan Success Story." Luxembourg: EIB, December. http://www.eib.org/attachments/country/study_digital_financial_services_in_africa_en.pdf

Gilman, Lara, and Michael Joyce. 2012. "Managing the Risk of Fraud in Mobile Money." London: GSMA, October. http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/10/2012_MMU_Managing-the-risk-of-fraud-in-mobile-money.pdf

GPFI (Global Partnership for Financial Inclusion). 2014. "Issues Paper: Digital Financial Inclusion and the Implications for Customers, Regulators, Supervisors and Standard-Setting Bodies." 2nd GPFI Conference on Standard-Setting Bodies and Financial Inclusion: Standard Setting in the Changing Landscape of Digital Financial Inclusion. Basel, 30–31 October. http://www.gpfi.org/sites/default/files/documents/Issues%20Paper%20for%20GPFI%20BIS%20Conference%20on%20Digital%20Financial%20Inclusion.pdf

Grameen Foundation, GSMA, and InterMedia. 2014. "Use of Mobile Financial Services among Poor Women in Rural India and the Philippines." Case Study. Washington D.C.: Grameen Foundation, February. http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2014/07/Use-of-Mobile-Financial-Services-Among-Poor-Women-in-Rural-India-and-the-Philippines.pdf

GSMA (GSM Association). 2012. "Mobile Privacy Principles. Promoting a User-Centric Privacy Framework for the Mobile Ecosystem." London: GSMA, March. http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/gsmaprivacyprinciples2012.pdf

———. 2014a. "2013 State of the Industry Report on Mobile Financial Services for the Unbanked." London: GSMA, February. http://www.gsma.com/connectedwomen/wp-content/uploads/2014/02/SOTIR_2013.pdf

———. 2014b. "Mobile Privacy: Consumer Research Insights and Considerations for Policymakers." London: GSMA, February.

———. 2014c. "Code of Conduct for Mobile Money Providers." London: GSMA, November. http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2014/11/Code-of-Conduct-for-Mobile-Money-Providers.pdf

———. 2014d. "Mobile Money Risk Toolkit." London: GSMA, June.

———. 2014e. "Smartphones to Account for Two Thirds of World's Mobile Market by 2020 Says New GSMA Intelligence Study." London: GSMA, September. http://www.gsma.com/newsroom/press-release/smartphones-account-two-thirds-worlds-mobile-market-2020/

———. 2015. "2014 State of the Industry Report on Mobile Financial Services for the Unbanked." London: GSMA, February. http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2015/03/SOTIR_2014.pdf

Hanouch, Michel, and Gregory Chen. 2015. "Promoting Competition in Mobile Payments: The Role of USSD." Brief. Washington D.C.: CGAP, February. http://www.cgap.org/sites/default/files/Brief-The-Role-of-USSD-Feb-2015.pdf

Helix Institute of Digital Finance. 2014a. "Agent Network Accelerator Surveys." See country reports 2013 for Uganda, Kenya, Tanzania, Nigeria, Bangladesh, and Indonesia. Nairobi: Helix Institute of Digital Finance, January. http://www.helix-institute.com/data-and-insights

———. 2014b. "Emerging Trends for Mobile Money Agent Networks & Implications on Client Protection." Nairobi: Helix Institute of Digital Finance, May. http://www.helix-institute.com/data-and-insights/emerging-trends-mobile-money-agent-networks-implications-client-protection

ID3 (Institute for Data Driven Design). 2014. "The Windhover Principles for Digital Identity, Trust and Data." Boston: ID3, November. https://idcubed.org/home_page_feature/windhover-principles-digital-identity-trust-data/

Imaeva, Guzelia, Irina Lobanova, and Olga Tomilova. 2014. "Financial Inclusion in Russia: The Demand-Side Perspective." Moscow: CGAP, August. http://www.cgap.org/sites/default/files/Working-Paper-Financial-Inclusion-in-Russia-Aug-2014.pdf

IMTFI (Institute for Money, Technology & Financial Inclusion). 2013. "Digital Payment Client Uptake: Warning Signs." Irvine, Calif.: IMTFI, June. http://www.imtfi.uci.edu/files/docs/2013/imtfi-dpcu-digital-loresFINAL.pdf

Indiatimes. 2015. "Mobile Payment Startups and Banks Use Technology to Tap Rural India." *The Economic Times of India*. Gurgaon: Indiatimes. http://articles.economictimes.indiatimes.com/2015-01-01/news/57581220_1_bank-accounts-state-bank-ezetap

InterMedia. 2014. "Financial Inclusion Insights (FII) Reports." See reports for Bangladesh, India, Pakistan, Kenya, Nigeria, Tanzania and Uganda. Washington D.C.: InterMedia. http://finclusion.org/fii-blog/fii-reports/

———. 2015. "Financial Inclusion Insights (FII) Data." Bangladesh, Pakistan, Kenya, Tanzania, Uganda, Rwanda, Ghana. Washington D.C.: InterMedia.

IPC (Information and Privacy Commissioner). 2011. "Privacy by Design. The 7 Foundational Principles." Toronto: IPC. https://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

ISF (Information Security Forum). 2014. "The 2014 Standard of Good Practice for Information Security." London: ISF. https://www.securityforum.org/shop/p-71-173

ISO (International Organization for Standardization). 2015. "ISO/DIS 12812-1. Core Banking—Mobile Financial Services, Part 1: General Framework." Geneva: ISO. http://www.iso.org/iso/catalogue_detail?csnumber=59844

ITU (International Telecommunication Union). 2014. "Regulation and Consumer Protection in a Converging Environment." Geneva: ITU, March. https://www.itu.int/ITU-D/finance/Studies/consumer_protection.pdf

Jumah, Jaqueline. 2015. "The 'I Don't Have Enough Float' Quandary!" Blog. Nairobi: Helix Institute of Digital Finance, February. http://helix-institute.com/blog/%E2%80%9Ci-don%E2%80%99t-have-enough-float%E2%80%9D-quandary

Koning, Antonique, and Monique Cohen. 2015. "Enabling Customer Empowerment: Choice, Use, Voice." Brief. Washington D.C.: CGAP, April. http://www.cgap.org/sites/default/files/Brief-Enabling-Customer-Empowerment-Mar-2015_0.pdf

Lake, Andrew J. 2013. "Risk management in Mobile Money: Observed Risks and Proposed Mitigants for Mobile Money Operators." Washington D.C.: International Monetary Fund. http://www.ifc.org/wps/wcm/connect/37a086804236698d8220ae0dc33b630b/Tool+7.1.+Risk+Management.pdf?MOD=AJPERES

Lamb, Jason, and Sacha Polverini. 2015. "Assessing Risk in Digital Payments. Special Report Financial Services for the Poor." Seattle: Bill & Melinda Gates Foundation, February. https://docs.gatesfoundation.org/documents/Assessing%20risk%20in%20digital%20payments%20FSP.pdf

Lauer, Kate, and Timothy Lyman. 2015. "Digital Financial Inclusion: Implications for Customers, Regulators, Supervisors, and Standard-Setting Bodies." Brief. Washington D.C.: CGAP, February. http://www.cgap.org/sites/default/files/Brief-Digital-Financial-Inclusion-Feb-2015.pdf

Lubitz, Lenny. 2008. "5 ATM Scams That Can Break the Bank." Oakland: Investopedia. http://www.investopedia.com/articles/pf/08/avoid-atm-scams-atm-fraud.asp

Lyman, Timothy, Stefan Staschen, and Olga Tomilova. 2013. "Landscaping Report: Financial Inclusion in Russia." Brief. Washington D.C.: CGAP, January. http://www.cgap.org/publications/landscaping-report-financial-inclusion-russia

Mas, Ignacio, and David Porteous. 2014. "How the Spread of Smartphones Will Open up New Ways of Improving Financial Inclusion." Blog. Washington D.C.: The Brookings Institution, 2 December. http://www.brookings.edu/blogs/techtank/posts/2014/12/2-smartphones-financial-inclusion

Matthews, Brett. 2014. "Oral Information Management Tools: Lighting the Path to Financial Inclusion." Toronto: My Oral Village, October. http://savings-revolution.org/doclib/Oral%20Information%20Management%20Tools%2010%2014.pdf

Mazer, Rafael. 2015. "USSD Access: A Gateway and Barrier to Effective Competition." Blog. Washington D.C.: CGAP, February. http://www.cgap.org/blog/ussd-access-gateway-and-barrier-effective-competition

Mazer, Rafael, and Silvia Baur. 2014. "Merchant Incentives in the Shift to Cashless Food Aid." Blog. Washington D.C.: CGAP, November. http://www.cgap.org/blog/merchant-incentives-shift-cashless-food-aid

Mazer, Rafael, Jessica Carta, and Michelle Kaffenberger. 2014. "Informed Consent: How Do We Make It Work for Mobile Credit Scoring?" Washington, D.C.: CGAP, August. http://www.cgap.org/sites/default/files/Working-Paper-Informed-Consent-in-Mobile-Credit-Scoring-Aug-2014.pdf

Mazer, Rafael, Xavier Gine, and Cristina Martinez. Forthcoming. "Mystery Shopping for Financial Services Technical Guide." Washington D.C.: CGAP.

McCaffrey, Mike, and Evelyne Matibe. 2014. "The Status of Agents in Kenya: Proliferation, Dominance, Evolution and Impact." Nairobi: The Helix Institute of Digital Finance, June. http://www.helix-institute.com/blog/status-agents-kenya-proliferation-dominance-evolution-impact

McCaffrey, Mike, and Maha Khan. 2014. "Bangladesh Pioneering Unique Models & Innovations for Agent Networks." Nairobi: The Helix Institute of Digital Finance, November. http://helix-institute.com/blog/bangladesh-pioneering-unique-models-innovations-agent-networks

McKee, Katharine, Estelle Lahaye, and Antonique Koning. 2011. "Responsible Finance: Putting Principles to Work." Focus Note 73. Washington D.C.: CGAP, September. http://www.cgap.org/sites/default/files/Focus-Note-Responsible-Finance-Putting-Principles-to-Work-Sep-2011.pdf

MTN Uganda. 2014. "MTN Group Interim Results for the Period Ending 30th June 2014 Show Continued Improvement for MTN Uganda as It Reaches the 10 Million Subscriber Landmark." Press release, 7 August. Kampala: MTN Uganda. http://www.mtn.co.ug/About-MTN/News-Room/2014/August/MTN-Group-Interim-results-for.aspx

Mudiri, Joseck L. 2012. "Fraud in Mobile Financial Services." Luknow, India: MicroSave, December. http://www.ifc.org/wps/wcm/connect/42f4348042366eee8309af0dc33b630b/7.5+Fraud_in_Mobile_Financial_Services_JMudiri.pdf?MOD=AJPERES

Noor, Wameek, and Leesa Shrader. 2015. "Telenor's Shared Agents: Digital Finance Catalyst for Bangladesh?" Blog. Washington D.C.: CGAP, February. http://www.cgap.org/blog/telenor%E2%80%99s-shared-agents-digital-finance-catalyst-bangladesh

OECD (Organisation for Economic Co-operation and Development). 2011. "G20 High-level Principles on Financial Consumer Protection." Paris: OECD, October. http://www.oecd.org/daf/fin/financial-markets/48892010.pdf

———. 2014. "Effective Approaches to Support the Implementation of the Remaining G20/OECD High-level Principles on Financial Consumer Protection." Paris: OECD, September. http://www.oecd.org/daf/fin/financial-education/G20-OECD-Financial-Consumer-Protection-Principles-Implementation-2014.pdf

Ogwal, Isaac. 2014. "Survival of the Fittest: The Evolution of Frauds in Uganda's Mobile Money Market." Blog. Luknow, India: MicroSave, August. http://blog.microsave.net/survival-of-the-fittest-the-evolution-of-frauds-in-ugandas-mobile-money-market-part-i/

———. 2015. "Uganda: Tracing the Customer Journey." New York: UNCDF MM4P, February. http://www.uncdf.org/sites/default/files/Documents/bn2_uganda_v7.pdf

Parada, Marcia, and Greta Bull. 2014. "In the Fast Lane: Innovations in Digital Finance." Washington D.C.: International Finance Corporation, May. http://www.ifc.org/wps/wcm/connect/d2898b80440daa039453bc869243d457/In+The+Fast+Lane+-+Innovations+in+Digital+Finance+IFC.pdf?MOD=AJPERES

PCI SSC (Payment Card Industry Security Standards Council). 2015. "PCI SSC Data Security Standards." Wakefield: PCI SSC. https://www.pcisecuritystandards.org/security_standards/index.php

Radcliffe, Daniel, and Rodger Voorhies. 2012. "The Digital Pathway to Financial Inclusion." Seattle: Bill & Melinda Gates Foundation, December.

Seltzer, Yanina, and Claudia McKay. 2014. "What Human-Centered Design Means for Financial Inclusion." Washington D.C.: CGAP, October. http://www.cgap.org/sites/default/files/CGAP_Insights_into_Action_final.pdf

Shrader, Leesa. 2015. "Digital Finance in Bangladesh: Where Are All the Women?" Blog. Washington D.C.: CGAP, February. http://www.cgap.org/blog/digital-finance-bangladesh-where-are-all-women

Tarazi, Michael, and Paul Breloff. 2010. "Nonbank E-Money Issuers: Regulatory Approaches to Protecting Customer Funds." Focus Note 63. Washington D.C.: CGAP, July. http://www.cgap.org/sites/default/files/CGAP-Focus-Note-Nonbank-E-Money-Issuers-Regulatory-Approaches-to-Protecting-Customer-Funds-Jul-2010.pdf

Tigo Ghana. 2015. "Process of Complaints Handling." Accra: Tigo Ghana. http://www.tigo.com.gh/people/process-complaints-handling

Ubani, E. C., and I. C. Nwakanma. 2013. "Effectiveness of Maintenance Policies for Cellular System Infrastructure Project." *International Journal of Scientific Engineering and Technology*, 2(10): 953–60, October. http://ijset.com/ijset/publication/v2s10/IJSET_2013_1004.pdf

World Bank. 2014. "Diagnostic Reviews of Consumer Protection and Financial Literacy." Diagnostic Reviews for Rwanda, Pakistan, Kyrgyz Republic, Indonesia and the Philippines. Washington D.C.: World Bank. http://responsiblefinance.worldbank.org/diagnostic-reviews

———. 2015. "Paraguay Diagnostic Review of Consumer Protection and Financial Literacy, Volume 1. Key Findings and Recommendations." Washington D.C.: World Bank, January. http://responsiblefinance.worldbank.org/~/media/GIAWB/FL/Documents/Diagnostic-Reviews/Paraguay-CPFL-DiagReview-Volume-I-FINAL.pdf

———. Forthcoming. "Zimbabwe Diagnostic Review of Consumer Protection and Financial Literacy, Volume 1. Key Findings and Recommendations." Washington D.C.: World Bank.

Wright, Graham. 2013. "Why Rob Agents? Because That's Where the Money Is." Blog. Luknow, India: MicroSave, August. http://blog.microsave.net/why-rob-agents-because-thats-where-the-money-is/

———. 2014. "Over the Counter Transactions—Liberation or a Trap? Part III." Blog. Luknow, India: MicroSave, December. http://blog.microsave.net/over-the-counter-transactions-liberation-or-a-trap-part-iii/

Zetterli, Peter. 2015. Tanzania: Africa's Other Mobile Money Juggernaut. Blog. Washington, D.C.: CGAP, March. http://www.cgap.org/blog/tanzania-africa's-other-mobile-money-juggernaut

Zimmerman, Jamie, and Eric Tyler. 2014. "How Responsible Is Digital Finance? 10 Global Insights." Blog. Washington D.C.: CGAP, December. http://www.cgap.org/blog/how-responsible-digital-finance-10-global-insights

Zimmerman, Jamie, Kristy Bohling, and Sarah Rotman Parker. 2014. "Electronic G2P Payments: Evidence from Four Lower-Income Countries." Focus Note 93. Washington, D.C.: CGAP, May. http://www.cgap.org/sites/default/files/Focus-Note-Electronic-G2P-Payments-April-2014.pdf

Zollmann, Julie. 2014. "Kenya Financial Diaries: Shilingi Kwa Shilingi—The Financial Lives of the Poor." Nairobi: FSD Kenya, August. http://www.fsdkenya.org/pdf_documents/14-08-08_Financial_Diaries_report.pdf

Annex 1: Glossary

Advanced services	See Value-added services
Check digit	A check digit is a number that is added to the end of a customer's phone number to create their account number. If a sender enters the wrong phone number by accident, it is likely that the check digit will not match, thus reducing wrong transactions.
Customer risk	The possibility that a customer will experience harm that includes financial loss, lack of access to own accounts or stored value, unfair, abusive, or discriminatory conduct from FSP staff, agents, or outsourced service providers, or exposure to other immediate or future risks such as loss of privacy and security of personal data, harassment by private parties or government-affiliated entities or individuals, unaware involvement in illegal activity, etc.
Digital financial services (DFS)	There is no common widely used definition of DFS. This paper defines DFS broadly to include the full range of products (including digital transfers, payments, stored value, savings, insurance, credit, and more), channels (such as mobile phones and ATMs), and providers including mobile network operators (MNOs or "telcos"), banks, nonbank financial institutions, and e-money issuers, retailers, post offices, and others.
Financial customer/user/ consumer	This paper uses the terms "customers" and "users" interchangeably to refer to those who use one or more DFS. "Consumers" is a broader term as it includes potential users who may also face certain risks, such as lack of transparency as they shop for DFS, and whose trust and behavior may be affected by experience reported by users.
Financial service providers (FSP)	Financial service providers (FSPs) include mobile network operators (MNOs) or "telcos," banks, nonbank financial institutions, e-money issuers, retailers, post offices, and others. Note that many would not traditionally be considered "financial institutions." Note also that one FSP entity (e.g., a bank) may own one or more other FSPs (e.g., e-money issuers).
Fraud	Fraud is "the intentional and deliberate action undertaken by players in the DFS ecosystem aimed at deriving gain (cash or e-money) and/or denying other players revenue and/or damaging the reputation of other stakeholders" (Mudiri 2012).
Mobile financial services	Mobile money plus other mobile-delivered services such as bill pay, savings, insurance, and credit.
Mobile money	Use of the mobile phone and a network of transaction points outside of bank branches to transfer money and make payments (GSMA 2015).
Mobile money wallets	Also referred to as e-wallets or digital wallets, these are money accounts that allow stored value and are accessed through the mobile phone.
Mystery shopping	Mystery shopping is an exercise used to measure the adequacy of practices relative to disclosure and information provision, sales, business conduct, complaints handling, etc. Mystery shopping involves training actual or potential consumers to fill a certain profile. The shoppers then conduct one or more real-life shopping visits (which might include assessment of service options only or actual registration or receipt/purchase of a financial service) to one or multiple FSP points of service.
Network/platform problems	Network or platform problems take many forms: the customer's phone may not be able to connect to the base station due to a network failure; mobile network congestion may block the connection between the phone and the platform; platform congestion may limit the number of concurrent transactions; or there may be downtimes with third-party service providers using the mobile money platform to offer services, such as for retail payments or hospital fee payments. In addition, for USSD-based systems, the time allowed per USSD session is generally limited. If the transaction times out before completion, many customers mistakenly believe the network is down when in fact the USSD session has terminated.
Over-the-counter transactions (OTC)	Over-the-counter (OTC) transactions occur when customers do P2P by transacting in cash with an agent who executes the electronic payment on their behalf.
Responsible digital finance	As applied to DFS, the term "responsible" in this paper refers to product features, business processes, and policies that protect customers and balance their interests and benefits with providers' long-term viability (McKee et al. 2011).
Value-added services/ products	Most DFS providers offer first-generation services and products such as cash-in and cash-outs, P2P transfers, and airtime top-ups, while a few are experimenting with second-generation products or value-added products, such as savings, loans, microinsurance, P2B transfers, bill payments, consumer product financing, salary disbursements, e-commerce, and pensions (EIB 2014).

Annex 2: Findings from the FII Surveys: Problems Customers Experience and Their Use of Recourse

	Bangladesh[a]	Ghana	Kenya	Pakistan	Rwanda	Tanzania	Uganda
Total who report experiencing at least one problem	22%	59%	87%	19%	53%	69%	81%
Percent who experienced each problem in the past six months							
Agent was absent	5%	21%	43%	4%	25%	31%	39%
Agent was rude	1%	6%	11%	2%	6%	6%	10%
Agent had insufficient liquidity to complete transaction	2%	22%	55%	1%	23%	32%	37%
Agent refused to perform transaction for no reason	0%	2%	4%	0%	2%	2%	4%
Agent overcharged for transaction	3%	3%	2%	0%	1%	5%	11%
Agent did not give all the cash that was owed	1%	3%	3%	1%	0%	4%	6%
The network was down	5%	39%	52%	2%	36%	38%	59%
The agent's system was down	1%	n/a	51%	6%	n/a	42%	42%
It was very time consuming	2%	13%	24%	2%	1%	9%	19%
Did not receive a receipt (such as SMS receipt)	10%	7%	37%	6%	3%	8%	20%
Agent charged for making deposit	1%	3%	2%	2%	1%	2%	10%
Agent asked for PIN	1%	13%	6%	7%	1%	3%	15%
Agent was dismissive of women	0%	1%	2%	0%	4%	0%	1%
Agent defrauded me or assisted others in defrauding me	0%	0%	1%	0%	0%	0%	2%
Unsecure agent location	0%	1%	4%	0%	1%	0%	3%
Percent who reported the problem to customer care	9%	14%	7%	24%	9%	14%	10%
Percent who were satisfied with the resolution	54%	78%	89%	65%	94%	74%	79%

Source: InterMedia (2015).

a. In Bangladesh and Pakistan, qualitative and other research suggests that some numbers, including agent overcharging and network downtime, reported here are lower than actual. Factors such as consumer interpretations of problems, cultural biases, or other factors may have contributed to under reporting in these countries

Annex 3: Illustrative Standards and Codes of Conduct Relevant for Responsible Digital Finance

Interest is growing in exploring the potential for private or public principles, codes of conduct, standards, or "good practices" to improve mitigation of DFS customer risks.[48] Table A3-1 offers examples of specific standards, codes, and principles that aim at mitigating risks to customers using DFS. The alphabetical list of initiatives is not exhaustive, nor is the inclusion of any specific example meant as validation of its effectiveness. (In addition, at the global policy level, AFI, GPFI, the financial sector SSBs, and the G20-OECD have relevant work underway to provide guidance on application of regulatory and supervisory principles and standards to DFS products, channels, and providers.)

Table A3-1. Good practice and standards initiatives

Code	Year of launch	Content
AFI *Guideline Note on Consumer Protection in Mobile Financial Services*	2014	This guideline identifies consumers' vulnerabilities, risks, constraints, and costs associated with the provision of mobile financial services at four different stages of the transaction: (*i*) marketing, (*ii*) registration, (*iii*) transaction, and (*iv*) transaction and complex value-added. The guideline note concludes with implications and responsibilities for providers and financial regulators. (AFI 2014)
Cash Learning Partnership (CaLP) *Principles for Ethical Cash Transfers*	2013	The CaLP principles and operational standards focus on data handling, with a particular focus on enabling agencies engaged in the delivery of cash (e.g., e-transfers) to address risks inherent in their access to and use of beneficiary data. The eight CaLP principles address: 1. Respect 2. Protect by design 3. Understand data flows and risks 4. Quality and accuracy 5. Obtain consent or inform beneficiaries as to the use of their data 6. Security 7. Disposal 8. Accountability (CaLP 2013)
G20/OECD *G20 High-level Principles on Financial Consumer Protection*	2011	The G20 Finance Ministers and Central Bank Governors called on OECD, the Financial Stability Board, and other relevant international organizations to develop common principles on financial consumer protection to complement—not substitute for—existing international principles and/or guidelines: 1. Legal, Regulatory, and Supervisory Framework 2. Role of Oversight Bodies 3. Equitable and Fair Treatment of Consumers 4. Disclosure and Transparency 5. Financial Education and Awareness 6. Responsible Business Conduct of FSPs and Authorized Agents 7. Protection of Consumer Assets against Fraud and Misuse 8. Protection of Consumer Data and Privacy 9. Complaints Handling and Redress 10. Competition (OECD 2011)

48 This was also a key opportunity identified by participants at the first Global Forum on Responsible Digital Finance, which convened experts from industry, regulation, development agencies, consumer advocates, and the research community (Perth, Australia, 2014).

Table A3-1. Good practice and standards initiatives

Code	Year of launch	Content
G20/OECD *Effective Approaches to Support the Implementation of the Remaining G20/OECD High-Level Principles on Financial Consumer Protection*	2014	The Effective Approaches to Support the Implementation of the G20 High-Level Principles of Financial Consumer Protection provide policy makers, regulators, and supervisors, and FSPs, their authorized agents and consumers, with relevant, practical, and evidence-based examples on how the principles can be implemented by identifying certain underlying assumptions, common effective approaches, and "innovative" or "emerging effective approaches" (OECD 2014).
Groupe Spéciale Mobile Association (GSMA) *Code of Conduct for Mobile Money Providers*	2014	This Code of Conduct outlines eight common business principles to enable the development of safe and responsible digital financial services: 1. Safeguard customer funds against risk of loss 2. Maintain effective mechanisms to combat money laundering and terrorist financing 3. Equip and monitor staff, agents, and entities providing outsourced services to ensure that they offer safe and reliable services 4. Ensure reliable service provision with sufficient network and system capacity 5. Take robust steps to ensure the security of the mobile network and channel 6. Communicate clear, sufficient, and timely information to empower customers to make informed decisions 7. Develop mechanisms to ensure that complaints are effectively addressed and problems are resolved in a timely manner 8. Collect, process, and/or transmit personal data fairly and securely (GSMA 2014c)
Groupe Spéciale Mobile Association (GSMA) *Mobile Privacy Principles*	2012	The Mobile Privacy Principles of GSMA act as a framework, informing separate standards and codes to address specific privacy issues, such as location privacy, transparency, notice, and choice mechanisms. Such codes or standards should identify proportionate and effective measures to ensure that mobile users' privacy is protected, either in general or in specific contexts or service scenarios. The nine principles are as follows: 1. Openness, transparency, and notice 2. Purpose and use 3. User choice and control 4. Data minimization and retention 5. Respect user rights 6. Security 7. Education 8. Children and adolescents 9. Accountability and enforcement (GSMA 2012)
Information and Privacy Commissioner Ontario, Canada *Privacy by Design (PbD) principles*	2009, Updated in 2011	Based on seven Foundational Principles, PbD was first developed in the 1990s by the Information and Privacy Commissioner of Ontario. This solution has gained international recognition as a global privacy standard. The principles are as follows: 1. Proactive not Reactive; Preventative not Remedial 2. Privacy as the Default Setting 3. Privacy Embedded into Design 4. Full Functionality—Positive-Sum, Not Zero-Sum 5. End-to-End Security—Full Lifecycle Protection 6. Visibility and Transparency—Keep It Open 7. Respect for User Privacy—Keep It User-Centric (IPC 2011)
Information Security Forum (ISF) *The Standard of Good Practice for Information Security*	2014	Updated annually, the Standard of Good Practice for Information Security covers the complete spectrum of information security arrangements that need to be made to keep business risks associated with information systems within acceptable limits, and presents good practice in practical, clear statements. In addition to information security, the standard addresses cyber resilience, supply chain security, mobile device security, data privacy in the cloud, and critical infrastructure (ISF 2014).

Table A3-1. Good practice and standards initiatives

Code	Year of launch	Content
Institute for Data Driven Design (ID3) *Windhover Principles for Digital Identity, Trust, and Data*	2014	The Windhover Principles represent a principles-based framework collaboratively written with public and private stakeholders to ensure secure personal identity, trust, and access to shared open data on the internet: 1. Self-Sovereign Identity and Control of Personal Data 2. Transparent Enforcement and Effective Lite Governance 3. Insuring Trust and Privacy 4. Open Source Collaboration (ID3 2014)
International Organization for Standardization (ISO) *ISO Mobile Financial Services Standards, ISO 12812*	Expected 2015/ 2016	Since late 2009, the working group has set out to define the core procedures needed when accessing users' deposit and credit accounts, focusing on transfers of value and leveraging and extending existing ISO standards for payment capabilities. The standard ISO 12812 will address 1. Security and data protection for mobile financial services 2. Financial application management 3. Mobile person-to-person payments 4. Mobile person-to-business payments 5. General requirements for mobile banking applications (ISO 2015)
International Telecommunication Union (ITU) *ITU DFS Working Group on Consumer Experience and Protection*	2014	In 2014 ITU initiated a focus group on DFS with the objective to identify technology trends in DFS over the coming years, describe the ecosystem for DFS in developed and developing countries and the respective roles and responsibilities of the stakeholders in the ecosystem, and establish liaisons and relationships with other organizations that could contribute to the standardization of DFS. Moreover, it seeks to identify successful use cases for implementation of secure DFS, including in developing countries, with a particular focus on the benefits for women, and works toward creating an enabling framework for DFS (ITU 2014).
Payment Card Industry Security Standards Council (PCI SSC) *Payment Card Industry Data Security Standards (PCI DSS)*	2013	PCI DSS provides an actionable framework for developing a robust payment card data security process, including prevention, detection, and appropriate reaction to security incidents such as fraud. The standard also includes PIN Transaction Security (PTS) requirements, which contain a single set of requirements for all PIN terminals, including POS devices, encrypting PIN pads, and unattended payment terminals (PCI SSC 2015).
Smart Campaign, Accion *Consumer Protection Principles for Digital Microfinance (Updates)*	Expected 2015/ 2016	The Smart Campaign began a work stream to understand the potential emerging risks to clients when using DFS and how best to mitigate those risks. It works in partnership with Accion and under the management of an Evolution of Standards Working Group. The updated Consumer Protection Principles for DFS will be based on and complement the existing seven Client Protection Principles and provide practical tips for DFS providers how to mitigate these risks (Arenaza 2014).
World Bank Group *Global Good Practices for Financial Consumer Protection*	2012, Updates in 2014, 2015	The World Bank Group is updating its diagnostic tool, the Global Good Practices for Financial Consumer Protection, including specific attention to responsible digital delivery of financial products and services.[a]

a. See Paraguay (World Bank 2015), Zimbabwe (World Bank forthcoming), Rwanda, Pakistan, Kyrgyz Republic, Indonesia, and the Philippines (World Bank 2014).

Annex 4: Acronyms

AFI	Alliance for Financial Inclusion
ANA	Agent Network Accelerator Project of the Helix Institute for Digital Finance (MicroSave)
ATM	Automated Teller Machine
BCBS	Basel Committee for Banking Supervision
BMGF	Bill & Melinda Gates Foundation
CaLP	Cash Learning Partnership
CGAP	Consultative Group to Assist the Poor
CPMI	Committee on Payments and Market Infrastructures
D2P	Donor to Person
DFID	UK Department for International Development
DFS	Digital Financial Services
EIB	European Investment Bank
FATF	Financial Action Task Force
FII	Financial Inclusion Insights
FSP	Financial Service Provider
G2P	Government to Person
GPFI	G20 Global Partnership for Financial Inclusion
GSMA	Groupe Spéciale Mobile Association (Global System for Mobile Communications Association)
IADI	International Association of Deposit Insurers
IAIS	International Association of Insurance Supervisors
ID3	Institute for Data Driven Design
IMSI	International Mobile Subscriber Identity
IMTFI	Institute for Money, Technology & Financial Inclusion
IOSCO	International Organization of Securities Commissions
ISF	Information Security Forum
ISO	International Organization for Standardization
ITU	International Telecommunication Union
IVR	Interactive Voice Response
KYC	Know Your Customer
MNO	Mobile Network Operator
OECD	Organisation for Economic Co-operation and Development
OTC	Over the Counter
P2P	Person to Person
PbD	Privacy by Design
PCI DSS	Payment Card Industry Data Security Standards
PCI SSC	Payment Card Industry Security Standards Council
PIN	Personal Identification Number
SIM	Subscriber Identity Module
SSB	Standard-Setting Bodies
TTM	Tcho Tcho Mobile
UNCDF	United Nations Capital Development Fund
USSD	Unstructured Supplementary Service Data
WFP	World Food Programme

No. 103
June 2015

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 P3-300
Washington, DC
20433 USA

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

Email:
cgap@worldbank.org

The authors of this Focus Note are Katharine McKee, CGAP senior adviser; Michelle Kaffenberger, senior research consultant; and Jamie M. Zimmerman, senior policy consultant. The authors would like to thank the following colleagues who reviewed the Focus Note and provided invaluable inputs: Mercy Buku (independent consultant); Carol Caruso (Accion International); Louis de Koker (Deakin University); Khurram Sikander (Enclude Solutions); Jonathan Morduch (Financial Access Initiative); Simone di Castri, Lara Gilman and Jeremiah Grossman (GSMA); Leesa Shrader (independent consultant); Isabel Barres (Smart Campaign, Center for Financial Inclusion); and Jennifer Chien, Denise Dias, Rosamund Grady and Ivo Jenik (World Bank). The following CGAP colleagues also provided advice and support throughout the research and writing process: Camille Busette, Greg Chen, Gerhard Coetzee, Juan Carlos Izaguirre, Antonique Koning, Timothy Lyman, Rafael Mazer, Claudia Vonderohe McKay, Anna Nunan, Corinne Riquet and Olga Tomilova. We extend a special thanks to Silvia Baur (CGAP) and Eric Tyler (independent consultant) for their terrific research support.

The suggested citation for this Focus Note is as follows: 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.

Print: ISBN 978-1-62696-072-5
pdf: ISBN 978-1-62696-073-2
epub: ISBN 978-1-62696-074-9
mobi: 978-1-62696-075-6