Assessing risk in digital payments

Special Report
Financial Services for the Poor,
February 2015

Bill & Melinda Gates foundation

Table of Contents

About the Gates Foundation's Financial Services for the Poor program

The Bill & Melinda Gates Foundation is guided by the belief that every life has equal value. In developing countries, it focuses on improving people's health and giving them the chance to lift themselves out of hunger and extreme poverty.

The Gates Foundation's Financial Services for the Poor promotes these goals by aiming to connect people in the world's poorest regions with digitally based financial tools and services. A growing body of evidence suggests that access to the right financial tools at critical moments can determine whether a poor household is able to capture an opportunity to move out of poverty or to absorb a shock without falling deeper into debt. However, according to Global Findex, only 23% of poor consumers globally have access to formal financial accounts. Access for women and rural consumers tends to be even lower.

Our experience indicates that digital payments systems provide the most effective way to significantly expand poor people's access to appropriate financial services. Compared to cash, digital payments can foster broader reach, provide greater security, and offer more products tailored to poor consumer needs, all at lower cost. They also have the potential to supply the providers of digital payments with additional, non-payment sources of revenue, for example from the digital information collected. This, in turn, allows providers to offer payment services at a lower price.

Our approach has three mutually reinforcing objectives:

- Increasing poor people's capacity to weather financial shocks and capture income-generating opportunities
- Generating economy-wide efficiencies by digitally connecting large numbers of poor and low-income people to one another and to financial service providers, government services and businesses
- Reducing the amount of time and money that poor people must spend to conduct financial transactions

We are not focused on particular products, services, or distribution channels, but rather on finding innovative cost-effective ways to expand access to finance, and encourage markets to identify which products and channels are most effective to reach the poor. At the same time, we are aware that interventions in this and other areas too often involve technologies that are made available to the intended users, but then not adopted. To address this design-side challenge, we are supporting research and product design experiments to identify design features, price incentives, and marketing messages that will encourage poor people to adopt and actively use digital financial services. We are also supporting policy makers as they develop policies and regulations that facilitate these developments, and provide oversight and accountability.

We believe the combined effect of these interventions will accelerate the rate at which people can transition out of poverty and build their financial security. Our strategy recognizes that countries are at different stages in developing an inclusive digital financial system, and that any solutions must be appropriate for the cultural and economic context.

Preface

Financial inclusion stakeholders – including in-market regulators, standard-setting bodies, consumer advocates, and other market participants – agree that a considered approach to managing and regulating risk is necessary to underpin successful digital financial services.

However, risk is complicated terrain, even for conventional financial services, where banks are the dominant players, value chains are relatively well-understood, and terminology and risk management approaches have been established for years. Digital payments and broader digital financial services introduce added complexity, with new participants constantly entering the market, new products regularly introduced, and value chain dynamics in constant flux. A lack of common terminology and frameworks for identifying and assessing the associated risks complicates matters further.

Since digital payments form the foundation for digital financial services, an approach to managing and regulating their risk is the first step. Significant helpful literature exists that outlines the more common risks (such as fraud) associated with digital payments. However, we are not aware of any work that attempts to present a unified framework for risk in a way that is accessible to non-experts, but also meaningful to risk practitioners and industry participants. Such a framework would aid adoption of low-cost digital payments by aligning industry participants (e.g., banks and telecommunications companies), customers, and regulators on the risks associated with digital payments, and how to mitigate them.

This report aims to help accelerate this process, with a particular focus on digital payments serving the poor in developing countries. It has three primary objectives:

- Provide a common language and framework to guide dialogue on risk associated with digital payments, and its bearing on financial inclusion
- Examine whether inclusion of non-bank providers or development of innovative distribution channels creates new types of risk for consumers (particularly the poor), providers, or the financial system at large
- Describe approaches for assessing the economic impact of risk in digital payments from the perspectives of consumers, providers, and the system

In working towards these objectives, we have built our framework so it can be extended to risks associated with digital financial services beyond payments and to risks associated with overall provider sustainability. The ultimate goal of financial inclusion requires strong risk management and deliberate regulation across these areas as well as in digital payments.

We have adapted risk management approaches used in traditional financial services contexts to new sets of products and channels, to non-credit granting providers and to third-party agents, who work on behalf of payments services providers. We have made the approaches straightforward and compact to help communicate and structure complex risk ideas in accessible ways. Furthermore, rather than undertaking a detailed examination of specific markets, we have aimed to provide terminology, a framework, and approaches for identifying and assessing risks associated with digital payments that can be applied to any country, incorporating the individual idiosyncrasies of that market. We believe different stakeholders can apply these across widely varying markets and digital payments systems both today and as they evolve over time.

This report contributes to the discussion started by our *Fighting poverty profitably: Transforming the economics of payments to build sustainable, inclusive financial systems* (2013). That report offered an extensive analysis of the economics of payment systems around the world. It concluded that digital technologies can significantly reduce the cost of payment systems, and make them more efficient, sustainable, and accessible to poorer consumers, while at the same time boosting revenues for financial providers by supporting activities, both financial and non-financial, that generate non-payments revenue. Risk is a contributing part of the equation.

We have developed the perspectives in this report based on three primary activities. First, we drew on the latest risk management thinking in banking, payments, and other areas, including manufacturing and capital-intensive industries. Second, we assessed risk in digital payments in India and Kenya, two large markets with different payments system structures and levels of maturity. Kenya is the most developed mobile money market in the world. In India, emerging digital payments are linked largely to bank accounts, and increasingly enabled by a universal ID system. To examine these two systems, we conducted field visits to more than 10 organizations across the value chain. Third, we supplemented our fact base with research on digital money and agent banking in Tanzania, Uganda, Nigeria, Ghana, Indonesia, Pakistan, Bangladesh and Brazil.

After a brief summary of the key findings emerging from this work, the body of this report first offers a framework for understanding digital payments systems and the risks inherent in them. Next, the report discusses three broad categories of risk. Section I covers operational risk and Section II covers solvency and liquidity risk, both in digital payments. Section III provides an overview of other risks associated with digital financial services beyond payments and overall provider sustainability. Our report concludes with some advice and implications for stakeholders who choose to embark on the journey to improving financial inclusion.

Summary of findings

While this work focuses on establishing an organizing framework and tools for identifying and assessing risk issues relating to digital payments, it also reveals some findings that we hope can contribute to development of sustainable digital financial services that serve poor people at scale. We summarize these findings here:

1. **While digital financial services do not introduce major new risks beyond those that exist in traditional payments and in the financial system at large, we see the transfer of old risks both to new consumers and to new players in the value chain, who must quickly learn how to understand and effectively manage these risks.** We will see old risks transferred to new consumers as financial inclusion objectives are achieved. In addition, as digital payments value chains expand to include an increasing number of non-bank providers, these new participants will be subjected to risks that traditionally affected financial service providers only. Furthermore, the risk that exists is distributed among a growing number of participants. These institutions will need to measure, monitor and report new quantities (e.g., liquidity ratios) and can look to hire people from the banking industry with relevant experience. Regulators can help through explicit supervision in these new areas and by encouraging or requiring providers to articulate their appetite for operational risk and for solvency and liquidity risks.

2. **Despite the emergence of new players, products, services, and distribution channels, risk management approaches used in traditional contexts remain useful.** As in traditional approaches, we quantify the size of risks by weighing their severity, if they do occur, and the likelihood that they will occur. Also in digital payments as in traditional contexts, systematic yet flexible tools can be applied across widely varying markets today and as they evolve over time. In operational risk, an approach that identifies risks where they arise in business processes is both actionable and flexible. Such an approach can be applied to a wide variety of payment systems across many different markets to understand the system-specific risks to providers, consumers, and the financial system at large. For solvency and liquidity risk, an approach built around the payments value chain provides structure to a potentially complicated discussion. Providers and regulators can use such an approach to understand risks to providers, consumers, and the financial system at large, and to help stakeholders have meaningful, directed conversations.

3. **Operational risks are the largest risk type – to providers and consumers – and their size can be analyzed in terms of three types of process breakpoints – technology failure, human error and malfeasance**. The largest type of operational risk to consumers (accounting for both severity and likelihood) is human error on the part of consumer, provider, or both. Such errors can cause money to be deposited or sent to the wrong account. The greatest risk to providers is malfeasance, and is driven largely by the risk of a hack into a provider's back-end accounts that drains all user funds. While technology failure is the smallest risk for both providers and consumers today, as processes become ever more digitized, the most important operational risks to both consumers and providers shift from such one-off human error and malfeasance to systemic technology risk and technology enabled large-scale fraud (e.g., a system hack). In total, financial losses to providers from operational risks are similar to those to consumers, or an estimated $1.00-to-$3.00 per year per consumer. Since this figure is just an average, some consumers could suffer significantly more. Providers may also lose more after accounting for longer-term effects of foregone future revenue from customer attrition. This means that provider and consumer interests in managing risk are relatively well-aligned, particularly if providers account for likely foregone future revenue due to customer attrition arising when adverse events occur. As a result, one role for regulators may be to help providers articulate their risk appetite, accounting for expected future revenues.

4. **The largest risk associated with solvency and liquidity is the ability of consumers to access their funds in case of a "run on the bank" rather than the actual safety of those deposits.** This is especially true because a run on the bank with new value chains in digital payments could potentially include a "run on the telco" or "run on the agent network." The details of such an event would likely be quite market specific.

5. **Payment system adjacent revenues ("adjacencies") provide profit vital to the economics of serving poor users, but also introduce new risks that digital payments providers must learn to manage to support sustainable yet inclusive financial services.** Adjacencies include revenues from broader financial services – including long-term savings, lending, and insurance products – as well as non-financial adjacencies – including approaches to acquiring new customers, reducing customer attrition, and powering other businesses with consumer insights gleaned from payments data. A common approach to understanding associated risks will help stakeholders to work together to develop and support sustainable adjacent products.

The ACTA Framework

The four-part ACTA framework introduced in our report *Fighting poverty profitably: Transforming the economics of payments to build sustainable, inclusive financial systems* provides a simple way to understand payment system activities and the underlying market dynamics.

- **Account.** Account activities cover the primary relationship that a customer has with a provider, including opening new accounts and maintaining existing ones. Accounts provide a secure, accessible store of value. Examples include current accounts (also known as chequing accounts) and mobile money accounts.
- **Cash-in-cash-out (CICO).** To use the payment system, customers must be able to deposit and withdraw cash into and from their payment accounts. CICO networks provide these services. Components include bank branches, ATMs and individual money agents. This report primarily considers cash-in-cash-out activities at individual agents since this is the place at which CICO in digital payment and banking models differs from that of traditional payments and banking.
- **Transactions.** These are direct transfers of funds between accounts. In general, transactions include debit and credit card payments, credit transfers, direct debits, and mobile money transfers. This report focuses on transfers initiated by mobile phone (e.g., transfers via mobile money) as well as transfers initiated at individual agents.
- **Adjacencies.** These are activities, both financial and non-financial, that generate non-payments revenue for payment system providers. Financial adjacencies include interest earned on balances held, and the spread between the interest that the institution pays on savings accounts vs. what it charges for loans. Non-financial adjacencies include strategies to help companies acquire new customers, reduce customer attrition, cross-sell services, improve collections, or power other businesses with consumer insights. These revenue streams are vital for overall payment systems economics.

Ultimately, providers make money by charging customers – those paying, being paid, or both – for some combination of the activities under these four elements. A system is profitable in aggregate as long as total revenues from the underlying activities exceed total associated costs. From the perspective of providers, risk plays a role in the system economics: Risk events can lead to losses – a type of cost – and decreased system use by users – a cause of foregone future revenue. On the other hand, mitigating risk can add incremental costs to providers.

A framework for risk in digital payments

Context

From the perspective of a consumer, a payment system provides ways to hold money in an account and then transfer it, to withdraw or deposit cash, and to receive funds from other accounts. Both a current account at a bank (e.g., a chequing account) and mobile phone-based mobile money are examples of such accounts. Users with a current account, for example, can withdraw and deposit cash at bank branches or at ATMs, and they can make or receive payments either with a cheque, a debit card or via an account-to-account transfer. Mobile money – M-PESA in Kenya is a well-known example – has similarities, particularly from a user perspective. A consumer stores mobile money credit with a mobile money provider – often a mobile network operator. She can withdraw and deposit cash in return for this credit with an agent or possibly at an ATM. She can also transfer money to or from a different account using an interface on her phone.

From the perspective of the financial system at large, a payment system is a set of instruments, banking procedures, and, typically, interbank funds transfer systems that ensure the circulation of money. The full payment system in a country is the collection of all ways these things can happen. This picture is complex, involving many participants (e.g., banks, mobile-money operators, processors), channels for accessing cash or making transactions (e.g., ATMs, point-of-sale terminals, on-line interfaces, mobile phones) and payment instruments that can be used to make transactions (e.g., credit transfers, debit cards, credit cards).

Despite the complexity, all payment system business processes fall under the four core elements of the ACTA framework[1] – Account, Cash-in-cash-out, Transactions, and Adjacencies. This framework offers a view of payment activities from the perspective of consumers, while also helping us understand the economics of these activities, and how they fit together. Account activities cover the primary relationship that a consumer has with a provider, including opening new accounts and maintaining existing ones. Cash-in-cash-out (CICO) activities allow consumers to deposit and withdraw cash from their payment accounts (e.g., bank branches, ATMs and individual money or bank agents). Transactions are direct transfers of funds between accounts (e.g., debit and credit card payments, credit transfers, direct debits, and mobile money payments). Adjacencies are activities, both financial and non-financial, that generate non-payments revenue for payment system providers (e.g., interest earned by a bank on account balances held, reduced customer attrition or cross-selling of services). (See sidebar for more information on ACTA).

Our experience indicates that digital payments systems can serve the poor successfully by making the economics work for providers, and ensuring sufficient consumer demand. To do so, they must meet several criteria, all of which have a risk-related component:

- **Robust functionality.** Customers will only use new products and services that are reliable and easy to use. This requires an available telecommunication channel, simple product design, and high-quality front-line customer service, all of which technology can help support.
- **Open.** The more participants in the digital payment value chain, the greater the system functionality. For a digital platform to accommodate a diversity of trusted parties capable of serving the poor, it must allow various pieces of software to interface

[1] See *Fighting poverty profitably: Transforming the economics of payments to build sustainable, inclusive financial systems* (Special Report, Financial Services for the Poor, 2013)

(application program interfaces, or APIs), and it must offer services that allow providers to join the system cheaply and easily. However, including more participants may also increase the system's vulnerability, particularly as networks and products become inter-operable.

- **Secure.** Customers should be able to trust that their money and data will be secure. However, several factors can undermine customers' and regulators' confidence in new products and services. These include, among others, breach of data privacy, loss of funds from fraudulent activities or weak identification mechanisms, and gaps allowing criminal organizations to launder money through the mobile channel. A security breach can lead to costly upgrades to the system, fines, litigation, and loss of customer trust that might last years. The system should have services and capabilities that detect and limit fraud, safeguard customer privacy, and watch for money laundering or other signs of criminal activity. Importantly, however, providers may need to make trade-offs between full security and low cost and/or robust functionality.
- **Low cost.** Payment system providers need sufficiently low costs and a high probability of attractive returns. Risks, regulation, and their management can affect providers' costs significantly in multiple ways. Operational losses and regulatory fines both impose direct costs. Systems and processes deliberately designed to minimize or control risk can cost more, either upfront or on an ongoing basis. Complying with regulation and maintaining functions to ensure and test such compliance adds expense continuously. Risk-related contributions to provider costs can meaningfully influence the prices ultimately charged to consumers.

Organizing framework for risk in digital payments

In our experience, while stakeholders in digital payments recognize the important role of risk, they may not share common terminology and frameworks for identifying and assessing it. A common language becomes increasingly important as new players enter the market, additional products and services are developed (e.g., stored-value accounts or cash-in-cash-out services), and standard practices are altered to make products or services accessible to formerly unserved populations (e.g., risk-based know your customer (KYC) requirements).

To help overcome these challenges, we introduce a straightforward organizing framework to simplify consideration of risks in digital payments. Our framework segments the many types of risk into three categories, and considers their impact on three constituencies. The three categories of risk are:

I. **Operational risks.** These risks result from inadequate or failed internal processes, people, and systems, or from external events.[2]

II. **Solvency and liquidity risks.** Solvency risk occurs when an institution cannot fully meet its debts as they come due, even by selling all its assets, while liquidity risk occurs when an institution does not have sufficient liquid assets (e.g., cash) to meet its debts. These risks often intermingle, so for the purposes of this paper we do not distinguish between them in detail, except when the nature of the outcome depends on the details.[3]

---

[2] Operational risk is often conjoined with other risk types. For example, if a bank loses money by offering a loan to a consumer unworthy of credit due to an error in back-office processing of loan applications, this loss has both operational risk and credit risk components.

[3] To understand the link between solvency and liquidity risk, note that banks can lose access to short-term funding (exposing them to liquidity risk) when markets expect that they will be insolvent. On the other hand, banks that rely more on short-term funding are both exposed to greater liquidity risk and need to raise more capital to

III. **Other risks.** In order for providers to operate profitably while serving poor people, they will need to add adjacent revenue-generating activities to the basic payment system. These "adjacencies" include financial services such as long-term savings, lending, and insurance products, which introduce additional types of risk, such as credit and interest rate risk. In addition, all providers encounter risks linked to profitability, strategic risk, and reputational risk. While important, these risks are not unique to digital payments, so are not the focus of this report. We cover them at a high-level in the final section.

Three constituencies are impacted by risk, each in different ways:

- **Providers.** Providers can be impacted through direct losses, regulatory fines, costs to remediate issues, and forgone current or future revenue when users cannot or choose not to use a product or service.
- **Consumers.** Consumers should be able to understand the products and services they are offered, to use them as intended, and to get redress in case something does not work. Impact on consumers can include direct loss of money, the cost of getting redress (in terms of money and time), or the incremental cost of using a second-choice alternative, such as sending cash by bus from an urban to rural area.
- **The financial system at large.** Impact to the financial system at large can include macroeconomic effects when business is halted or harmed (e.g., if many businesses are unable to transact). It can also include consequences when the digital payment system is exploited to facilitate criminal activity (e.g., money laundering or moving funds to fund terrorist activities). We note that risk to the financial system at large is various and complex, and we offer this simplified schematic way to consider it.

Exhibit 1 provides a visual representation of this organizing framework.

EXHIBIT 1

Organizing framework for analyzing risk in digitally-enabled payments

Risk Type	Constituency impacted: Provider • *Direct losses & fines* • *Cost to remediate* • *Foregone revenue*	Consumer • *Direct losses* • *Cost to get redress* • *Cost of a second-choice alternative*	System at large • *Business halted or harmed* • *System used for criminal purposes*
I. Operational risk *Results from inadequate of failed internal processes, people, and systems or from external events*			
II. Solvency & liquidity risk *Occurs when a provider's ability to meet its financial obligations comes under threat due to insufficient capital or liquid funds*			
III. Other risks *Risks that particularly impact providers (e.g., strategic, reputational) and those arising from credit products linked to the system*			

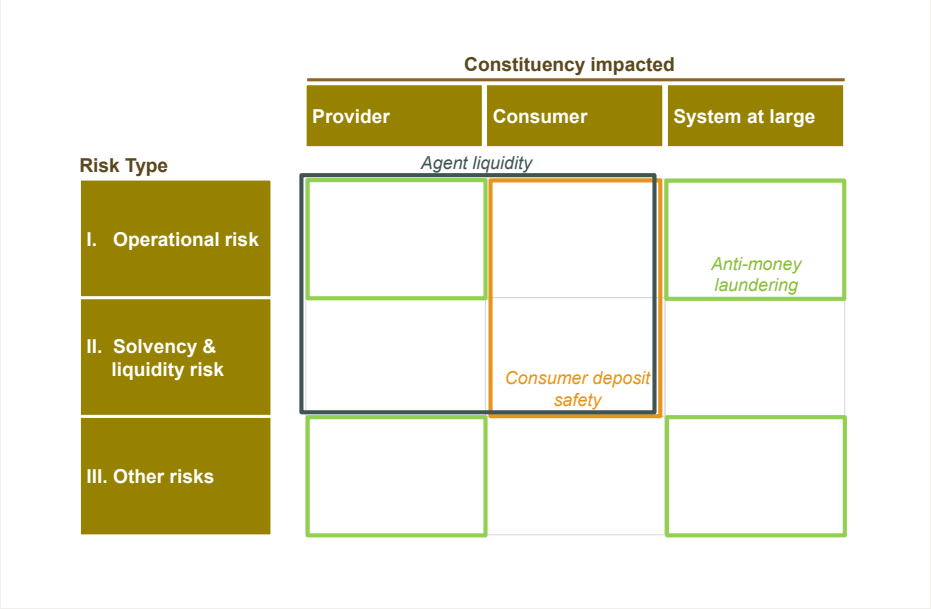
Use this grid to structure identification and analysis of risk in digitally-enabled payments and financial services

The framework may be particularly helpful to non-risk experts in understanding the role of regulators, who must consider the impact of all risk types on each of the three constituent groups in working towards their broad regulatory objectives. These objectives include protecting depositors, protecting consumers, and ensuring monetary and financial stability, all while fostering an efficient and competitive financial system. Protecting individuals' deposits and protecting consumers requires understanding risks to consumers. Ensuring stability requires understanding risks to the financial system at large. Fostering an efficient and competitive system requires understanding risks to, and the impact of, regulation on providers. Regulation plays a particularly important role in requiring or incentivizing providers to behave in a way consistent with consumer and system interests when this behavior is not otherwise in provider best interests. Throughout this report, we reference regulators' role in risk management as it pertains to each of the three constituencies.

We offer three examples of how to structure discussion about important issues of risk using this organizing framework (illustrated in Exhibit 2):

EXHIBIT 2

Examples of using the organizing framework to structure identification and analysis of risk



1. **The issue of consumer deposit safety often arises in discussion of risks in digital money or other payment instruments that allow users to store value.** Consumer deposit safety can be compromised either by operational risk or solvency and liquidity risk. Operational risk plays a role since inadequate or failed internal processes, people, or systems compromise consumer deposit safety. For example, a third-party hacker might draw down the bank account containing the money in many digital money customers' accounts, or an employee with system access might commit fraud, stealing money from accounts. Both solvency and liquidity risk play a role since either insufficient capital or liquidity at a provider in the value chain can compromise the safety of availability of customer funds. If the bank holding a pooled digital money account were

to fail, funds of digital money account holders could be endangered (subject to country-level details of deposit insurance and liability of the issuer of the digital money). When someone starts to speak about consumer deposit safety, one can stop and ask whether we are talking about a case of theft (operational risk) or solvency of a bank, telco, or other provider (solvency & liquidity risk).

2. **A second issue frequently discussed in the context of both digital money and agent banking is agent liquidity.** Agents may not have sufficient cash or "e-float"on hand to meet consumer needs for depositing or withdrawing cash. Using the framework demonstrates that this is really an operational risk issue. Agents may have a temporary shortage of cash or of e-money from a failure of internal processes, when they do not correctly predict when they will need to rebalance their supply of cash, do not have time to rebalance amid their other duties, or are unable to access the cash they need from a bank or other source[4]. In areas with one or few agents, when agents run out of cash, it can affect both consumers, who may be unable to withdraw their money when they need it, and providers, who may lose revenue from cash-out fees. When someone starts to speak about liquidity risk, one can stop and ask, are we talking about agent liquidity (operational risk) or a bank/telco shortage of liquid funds, which could impact operations on a large scale (solvency & liquidity risk).

3. **A third issue that gets significant attention in digital payments discussions is the presence of anti-money laundering (AML) rules and regulations.** The framework helps illustrate that fighting money laundering involves both operational and other risk issues. Operational risk plays a role since some combination of inadequate or failed internal processes or decisions made by people could leave the system vulnerable to money laundering. In principle, such a failure can affect the system at large, since money laundering can hurt country GDP and other macro factors. Other risks also play a role in discussions about money laundering since prominent or repeated breaches can harm the reputation of providers with regulators and shareholders (and sometimes consumers), and the reputation of countries with standard-setting bodies and the international community.

[4] Though this issue arises when an agent does not have sufficient, immediately available liquid funds, we do not also classify it as a liquidity risk for two reasons. First, in the case considered here, lack of liquidity occurs at the level of individual agents, who are not central to the value chain – if one individual agent encounters difficulties, the value chain will continue to function nearly unaltered. Second, agents typically do have access to liquidity within a matter of minutes to several hours.

I. Operational risk

Introduction

Just by turning on the lights, every company assumes some level of operational risk. The list of such risks is long and diverse, spanning events as varied as fraud, manual data entry errors, failure of information systems, shutdown of physical infrastructure, commercial disputes, and natural disasters. As a result, strong but prioritized operational risk management and regulation is critical.

We have found that a systematic approach to operational risk that identifies these risks where they arise in business processes is both actionable and flexible. Such an approach can be applied to a wide variety of payment systems across many different markets, to understand the system-specific risks to providers, consumers, and the financial system at large.

In this section, we describe such an approach to identify, quantify, and manage operational risks in digital payments. We have structured this section around the four parts of the approach. The parts describe how to:

A. Identify the most critical risks by tying them to business processes.

B. Quantify the severity of the identified risks, if they do occur.

C. Quantify the size of risks by weighing their severity against the likelihood that they will actually occur.

D. Shape a prioritized approach to operational risk management or regulation.

The work draws on approaches to operational risk management in banking, which we have tailored based on discussion with a wide range of experts and, as a test, applied to what we observed during our field visits to Kenya and India. The way that we quantify risks, in terms of severity and likelihood (B and C), has been standard practice in risk management for many years. However, identifying risks through a process-based view (A) reflects current developments in operational risk management at banks. This approach identifies process breakpoints, at which the likelihood of a breakdown leading to loss is highest, or where a breakdown would lead to a high loss. It helps front-line managers see and control the link between process operations and risk, and is more actionable and flexible than more traditional approaches built around categorizations of risk event types[5].

Before delving into the approach, it is important to note that applying it has presented us with several insights about operational risks in digital payments. We summarize them below, with more detailed analysis in the remainder of this section. Some of these insights will help stakeholders address how to approach operational risk management, while others provide preliminary conclusions about the size and nature of specific sorts of operational risk[6].

---

[5] We note that users of our risk management approach can employ existing categorizations of risk events, and specialized risk lists, as cross-checks alongside our approach. For example, many banks will use the Basel II classification of operational risks to classify operational risk losses into seven categories, each of which is further sub-divided. For example, the "internal fraud" category contains sub-categories including smuggling, bribes and insider trading. Each of these sub-categories describes a type of risk event, but does not help identify how or where these risks originated. In the mobile money space, the USAID Mobile Financial Services Risk Matrix, provides an example of an extensive list of risks that may also serve as a helpful completeness check. Other more specialized tools may help facilitate a deeper examination into niche areas.

[6] Calculations behind findings on the size of operational risks are available on request.

1. **The operational risks introduced by digital payments are similar to those associated with similar payments-related products in the financial system at large, but with a transfer of existing risks to new participants in the value chain.** Operational risks emerge as a result of process breakpoints. The nature of the risk is thus set by details of operational processes, and not by the type of provider who carries them out. A growing number of new participants will be subjected to operational risks that traditionally affected financial service providers only. These participants will need to monitor, measure, and report on these risks. Conversely, as financial institutions build out agent networks, they will be subjected to operational risks with which other types of providers have more experience – for example telcos, have used agents for years to sell scratch cards. Regulators can help ensure that market participants are equipped to manage risks new to them through explicit supervision, and by encouraging or requiring providers to articulate their operational risk appetite.

2. **Despite the emergence of new participants, products, services, and distribution channels, approaches to operational risk management used in traditional contexts remain useful.** As in traditional approaches, we quantify the size of risks by weighing their severity, if they do occur, and the likelihood that they will occur. Also in digital payments as in traditional contexts, systematic yet flexible tools can be applied across widely varying markets both today and as they evolve over time. In operational risk, an approach that identifies risks where they arise in business processes is both actionable and flexible. Such an approach can be applied to a wide variety of payment systems across many different markets to identify and assess the system-specific risks to providers, consumers, and the financial system at large.

3. **The size of operational risks to consumers and providers can be analyzed in terms of three types of process breakpoints – technology failure, human error and malfeasance.**

    A. **The greatest risk to consumers is human error (on the part of consumer, provider, or both), which is responsible for approximately 70 percent of the risk that they face, in financial terms.** The remainder is split between malfeasance and technology. The financial impact of human error is driven by the risk of consumer money being deposited into, or sent to, the wrong account.

    B. **The greatest operational risk to providers is malfeasance, which is responsible for approximately 80 percent of operational risk losses that they sustain.** The remainder is split between human error and technology. The risk of malfeasance is driven largely by the risk of a hack into a provider's back-end accounts that drains all user funds.

    C. **Technology failure is the smallest risk for both providers and consumers; however, its importance could increase over time with increased automation**, since the failure of centralized technology would pose increasing risks, and the risks of human error and small-scale fraud would decrease.

    D. **In total, financial losses to providers from operational risks are similar to those to consumers, or an estimated $1.00-to-$4.00 per year per consumer.** Since this figure is just an average, some consumers could suffer significantly more. This means that provider and consumer interests in managing risk are relatively well-aligned, particularly if providers account for likely foregone future revenue due to customer attrition arising when adverse events occur. This provides another good reason for regulators to support providers in articulating their operational risk appetite, accounting for expected future revenues.

A. Identifying operational risks by tying them to business processes

Operational risks are identified in two steps: first map business processes, then identify breakpoints in each process. Breakpoints are those points in a process at which the likelihood of a breakdown leading to loss is highest, or where a breakdown would lead to a high loss. Identifying breakpoints helps reveal sources of risk.

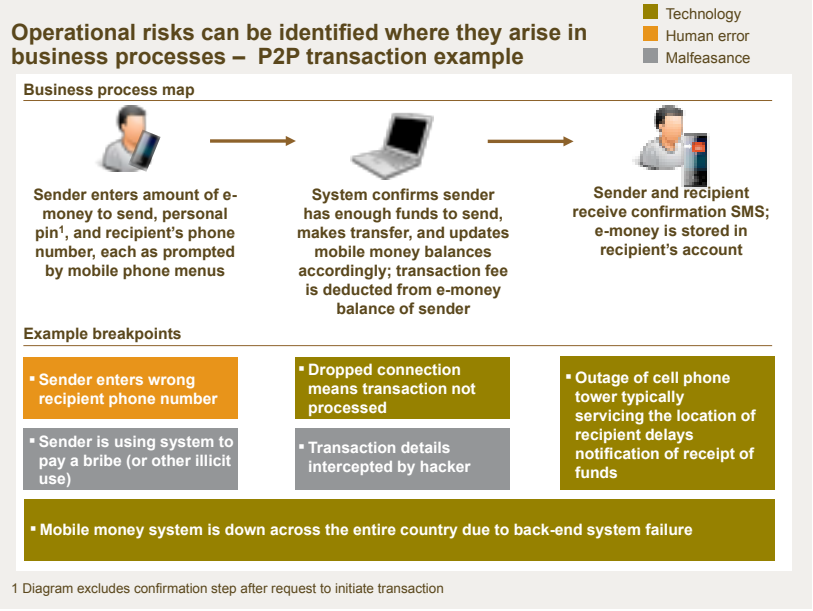
1. MAPPING BUSINESS PROCESSES

In this first step, we identify and classify all processes using the four core elements of the ACTA framework[7] – Account, Cash-in-cash-out, Transactions, and Adjacencies – and then create a more detailed map of each process. In this section, we focus on the first three elements – ACT – since activities related to Adjacencies typically involve processes that extend beyond the operational risks associated with payment systems themselves.

As an example, consider this step for a mobile money provider (e.g., M-PESA in Kenya or Tigo in Ghana). First, we categorize processes according to ACT. Examples of processes associated with Account include opening accounts, providing routine customer service at a call center, and generating text messages with account balances in response to consumer requests. CICO processes include both cash-in and cash-out at an agent, as well as the process by which an agent rebalances his account, to ensure he has enough cash or e-money to meet his customers' needs. Processes associated with Transactions include person-to-person remittance, point-of-sale consumer purchases at a business that accepts digital money, or automatic periodic wage payments from a business to an employee's digital money account.

Next, we create a more detailed map of each of these processes, focusing on the most critical processes first. Within the Transaction category, for example, the process behind person-to-person digital money remittances (P2P) potentially carries significant risk. While this process is highly automated, P2P transactions generate 30 percent-to-50 percent of total revenue, and a significant malfunction would affect large numbers of consumers, and seriously jeopardize the provider's credibility. Mapping this process in detail involves looking at each step, beginning with what happens when a consumer initiates a payment, when the provider receives and processes the payment, and when the recipient receives payment notification. The top of Exhibit 3 shows an overview of the P2P process in digital money; a truly detailed process map would show steps at a much more detailed level.

EXHIBIT 3



[7] See *Fighting poverty profitably: Transforming the economics of payments to build sustainable, inclusive financial systems* (Special Report, Financial Services for the Poor, 2013)

Integrated IT risk management

Banks and other providers in the digital financial services value chain are relying on increasingly complex IT (e.g., increased use of vendors, new digital channels and processes, ageing legacy systems) that needs to meet increasingly high standards (e.g., for prevention of fraud and anti-money laundering). This is introducing new risks and increasing the potential downside of existing risks.

To meet the challenges of these risks, IT risk management needs competencies across seven discplines:

1. **Information and cyber security,** to fight leakage of confidential customer and internal data, fraudulent transactions, blackmail, and hacktivism, identify and protect the most critical information assets, working backwards from desired business outcomes.
2. **Resilience and disaster recovery,** to minimize recurring on or prolonged interruptions of IT services that support critical processes; and, to define technology requirements, and closing gaps in technology, based on the prioritized business requirements for such processes.
3. **Vendor and third-party management,** to ensure that vendors and third parties deliver reliable and secure service, establish clear standards for security and continuity/disaster recovery, enforce in a risk-prioritized way, and involving critical partners in proactive enterprise risk management.
4. **Project and change management,** to keep IT projects on schedule, within budget, and of high quality, and apply a comprehensive set of value assurance levers, including an improved operating model, alignment of stakeholders, and monitoring and tracking.
5. **Architecture, development and testing,** to ensure quality system design that supports long-term affordable, reliable, and maintainable service, and to develop clear enterprise architectural standards and a review process.
6. **Data quality and governance,** to avoid regulatory issues or errors in transaction settlement stemming from inaccurate, inconsistent, or missing data, to establish consistent enterprise data architecture, data ownership and "golden sources" and controls to ensure data quality.
7. **IT compliance,** to maintain IT systems and process processes that are in compliance comply with regulations, to work with the compliance group to maintain awareness of mandates and track and enforce IT implications of regulations.

2. IDENTIFYING BREAKPOINTS FOR EACH PROCESS

In this next step we identify the breakpoints in each of the identified processes. To avoid missing any material breakpoints, while keeping the approach simple, we assess the presence of the three types of breakpoints within a given process – technology failure, human error, and malfeasance.

- **Technology failure.** This includes issues such as a transaction delay due to poor cell phone signal, back-end issues with the core technology, an agent's phone or terminal not working, failure of the system to send a text confirming a transaction, or lack of signal due to towers being down post-earthquake. Note that this does not include technology failures due to malfeasance. With increasing digitization of processes, the number of technology-linked breakpoints will grow. The sidebar provides a view of effective IT risk management across its components.

- **Human error.** This includes issues such as an agent or customer inputting the wrong account number or menu selection, or an agent or customer accidentally providing the wrong amount of cash. It also includes instances when agents do not carry out their intended role due to external factors (e.g., sickness, protest, or bankruptcy of their employer). Human error also can occur at the main provider offering the service (e.g., call center agent accidentally misinforming a customer, or transferring the wrong amount of money in a manual process or override). In addition, while some human error is arguably caused by poor process design, we assume that processes are designed well enough that they can be carried out without error (assuming no technology malfunction)[8].

- **Malfeasance.** This includes fraudulent and/or illicit activities, such as agents stealing from customers, customers stealing from agents, third-party actors stealing from customers, agents or providers, or individuals intentionally tampering with core infrastructure, such as cutting critical fiber optic cables[9].

As an example, we go back to the person-to-person (P2P), mobile-money remittance process we described earlier. During the initiation step, the system typically asks the money sender to enter the phone number of the recipient of the transfer, and then select "enter" on a mobile phone menu. Things that might go wrong here include breakpoints of all three types. For instance, the money sender could encounter trouble with the cellular network as the information is transmitted (technology malfunction). The payer could also mistype the recipient's phone number (human error), or could be trying to send money for illicit purposes such as terrorist financing, or part of an attempt to launder money (malfeasance). The bottom of Exhibit 3 (above) illustrates examples of breakpoints. Smart phones or other factors, can change the details of potential breakpoints.

Each breakpoint falls along a continuum, from affecting a single customer to affecting all customers. For example, in this P2P remittance process, a dropped connection that delays a transaction is a technology risk affecting a single customer. By contrast, failure of a digital money operator's entire back-end system affects all customers' ability to transact. Other breakpoints affect an intermediate number of customers. For example, in the case of a cell phone base station power outage, customers within that tower's radius of coverage are unable to transact until the tower is functioning again. Exhibit 4 shows examples of the three types of breakpoints in the P2P process and how they affect varying fractions of customers.

In general, we should examine breakpoints at a sufficiently detailed level to make them actionable without being cumbersome. Doing so improves our ability to estimate the likelihood that something will go wrong. It also aids us in integrating mitigating controls into the process design, and it helps us monitor performance at the most critical points in the process.

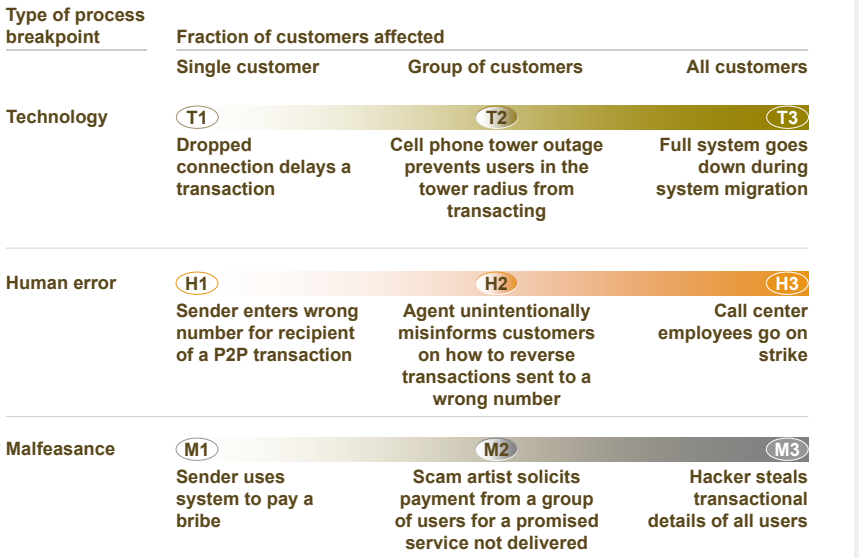
---

[8] In some categorizations, process risks and external risks are considered separate from human error and technology failure. In our categorization, however, external events are not considered separately because they could affect technology or human ability to perform their intended tasks. Similarly, a process risk that manifests due to technology is considered a part of the technology failure category, and a process risk that happens due to humans not utilizing the process as intended is considered human error.

[9] Note that some malfeasant acts require that multiple failure modes break sequentially in order to successfully break the system. In such a case, the set of failures that would have to occur should be understood as one break in the system. For example, for an agent to successfully skim money during a customer deposit, the customer would have to not notice the discrepancy both during transaction verification (typically done via text) and during the final account balance update.

EXHIBIT 4

Process breakpoints fall into three types and can affect different numbers of customers – P2P transaction example



B. Quantifying the severity of the identified operational risks

In the second step of our approach, we quantify the severity of identified operational risks for each constituency – providers, consumers, and the financial system at large. We note this is most difficult for the 'financial system at large', since it is the least concretely defined. The severity of a risk depends on the aggregated contribution from each of three categories of its potential impact: direct loss, cost to remediate, and foregone opportunity.

- **Direct loss** occurs when money in an account is misappropriated or a cash-in, cash-out, or transaction flow is misdirected (e.g., to the wrong account through error or fraud). Whether the provider, the consumer, or some combination of both bears direct losses depends upon the situation and payment system. For example, in the event that a money sender mistypes the recipient's phone number, he could send money to the wrong account. This would result in a direct loss to the consumer unless the provider had a protocol in place for reversing the transaction or reimbursing the consumer.

- **Cost to remediate** occurs when providers or consumers bear a cost to address an issue when a part of the system does not function, or there is a direct loss. For example, providers encounter costs when call center agents or technical support staff troubleshoot issues, or when employees check records manually, or reverse transactions. Consumers bear costs, particularly in time spent, if they must follow up with provider support staff to understand the issue, reverse transactions, find alternative ways to send money, or get some other form of redress.

- **Foregone opportunity** from compromised functionality occurs when a breakpoint blocks a process from being carried out, in part or in full. For example, when power goes out to a cell phone base station, this can block consumers within the range of the station from using the payments system via their mobile phones. If they give up on making a payment, or use an alternative payment channel, the payments provider would have to forego fee revenue. Compromised functionality can also hurt the financial system at large, if the payment system is central to the operation of the full economy. Currently in all countries, however, payment flows associated with digital money and agent banking are very small compared to overall flows[10].

To illustrate this step in our approach, we will continue with our example of the cell phone base station losing power for an hour, thereby compromising some number of P2P digital money transfers. Both *cost to remediate* and *foregone revenue* contribute to the severity of this risk for providers. (Sidebar on next page shows a template to structure estimates of risk severity).

Cost to remediate contributes because if the cell tower loses power mid-transaction, the money sender may follow-up with the provider to confirm whether his transaction went through. The provider will bear any associated costs from reversing the transaction or call center agent time. For example, if an average base station handles 15 P2P transactions per hour, once power has been regained, the call center may get as many as 15 calls asking about failed transactions. Suppose that only 1/15 of the transactions that were compromised by the power outages generated customer services calls, and that each such call costs the provider $0.50. That translates to just one call during a 1-hour power failure, and a resulting cost to remediate of $0.50[11]. Note that part of the cost to remediate would be borne by the users in cases where they must pay for the phone call to customer service.

Foregone opportunity contributes while the tower is down because the provider foregoes revenue from transactions money senders would otherwise have made. While some percentage of money senders will wait until they are able to access the service and then transact, others will decide not to send money, or will make the transaction through another mechanism (e.g. send money by bus) that does not generate revenue for the provider. In this case, we can estimate the foregone revenue from compromised functionality by looking at all these potential responses by money senders, and revenue lost from transactions that did not occur due to the power failure. As before, suppose that an average base station handles 15 P2P transactions per hour. If 85 percent of consumers wait until the system is working and then make their transaction, while 15 percent use a different method or decide not to send money (i.e., 2/15), then the provider will forego the revenue representing two P2P transactions. If a typical P2P transaction generates $0.30 in revenue to the provider, then an hour- long power failure at a base station would contribute roughly $0.60 in foregone opportunity to the provider.

---

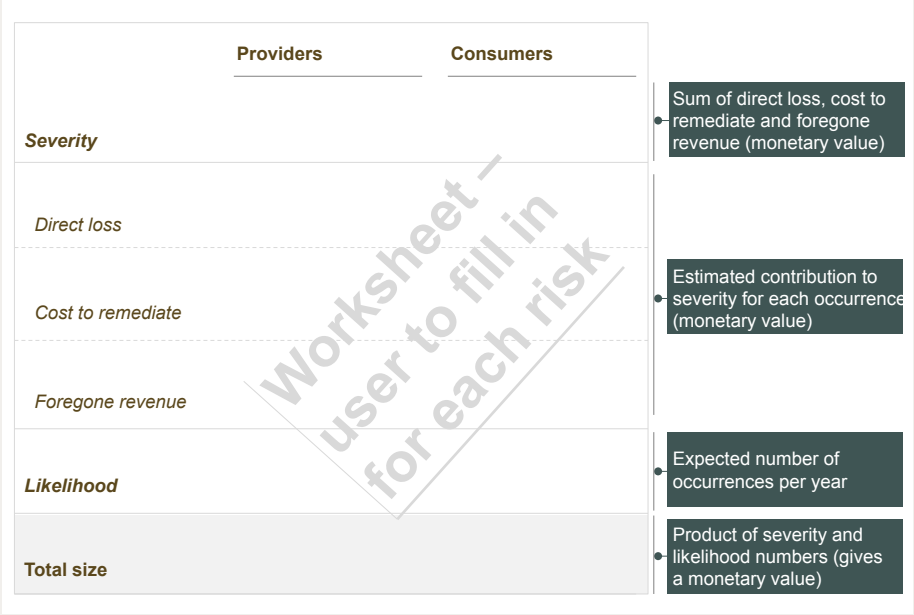
[10] Even in Kenya, where mobile money represents the largest payment flows as a fraction of overall GDP (49 percent in 2013), mobile money flows are only roughly 7 percent of total payment flows in the country (2013), based on Central Bank of Kenya and World Bank statistics.

[11] Note that in many countries, on-grid base stations have a diesel generator, which switches on when the grid power goes down. A portion of additional cost to run the generator (pro-rated, since the base station primarily serves call and other data transmission) is a cost to remediate. For simplicity, and because it is small, we do not include it here.

Estimating risk severity, likelihood and total size

To estimate risk severity, likelihood, and the resulting risk size, we can use a simple template for each potentially sizable risk, such as the one in the exhibit below. The rows under severity break out the three types of impact discussed in the section of this report on sizing severity of risks. In each row, we estimate the contribution of the specified type of impact to severity, in monetary value. Total severity is given by the sum of the contributions from each row. In the likelihood row, we estimate the number of occurrences of the given risk in a single year. We note that likelihood is the same for both providers and consumers. In the bottom row, the product of severity and likelihood gives the total monetary size of the risk for the year.

Sample worksheet for estimating size of each potentially important risk



Providers will complete the "provider" column, to understand their risks. Regulators will complete the "consumer" column, and potentially the "provider" column. Estimating numbers in the consumer column can help regulators ensure they focus on areas that matter most to consumer protection. Estimating numbers in the provider column helps regulators understand when provider and consumer interests are aligned – when a risk is similarly sized for both – and identify any potential areas where providers are underestimating the size of significant risks.

To get the data to support estimates, we can look first to past data on risk severity and likelihood at a given institution, in the industry, and across industries. There is typically a trade-off between getting more data and ensuring the data's relevance to the risk in question. Estimation is more difficult when the risk in question has occurred rarely or not at all. Techniques to confront the difficulty in estimating severity include looking at similar events as well as looking as using known quantities to make estimates. For example, if the average amount stored in each consumer account is up to $20, a risk that compromises the security of a group of accounts may lead to a loss of $20 per account (borne by either provider or consumer, depending upon the system rules). Techniques to confront the difficulty in estimating likelihood include comparing the risk likelihood to that of other known events, or determining the scenarios in which the event could occur, and then assessing the likelihood of such scenarios.

C. Quantifying operational risk size by weighting severity against likelihood

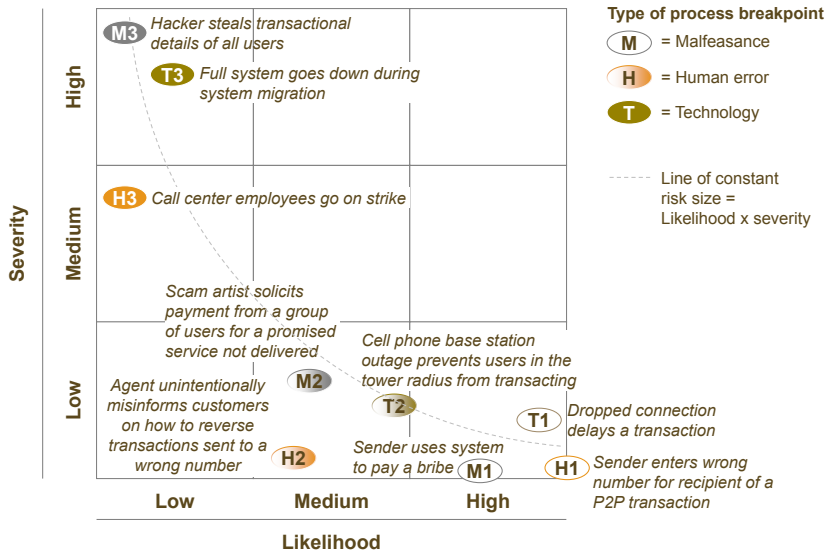
Now that we have estimated the severity of risks, we turn to estimating the likelihood those risks will actually occur, and then weighing these two against each other to quantify risk size. This gives an objective view of each risk's importance. In our example of a cell phone base station power outage, we can estimate likelihood using past data on frequency of base station power outages in the country or region. Even without exact numbers, we can approximate[12].

Having understood both the severity and the likelihood of a risk, we quantify its size as the product of both. (The adjacent sidebar provides a potential template for doing so systematically.) Graphing the severity and likelihood on a matrix can give us a sense of how different risks compare to one another. Exhibit 5 shows an illustrative plot of likelihood vs. severity for providers for a range of risks associated with P2P transactions. Risks appearing in the upper right of this matrix are largest, those along the diagonal line (from the upper left to lower right) are of intermediate size, and those in the bottom left are smallest.

EXHIBIT 5

Illustrative

Risk size depends on both likelihood and severity – P2P transaction example

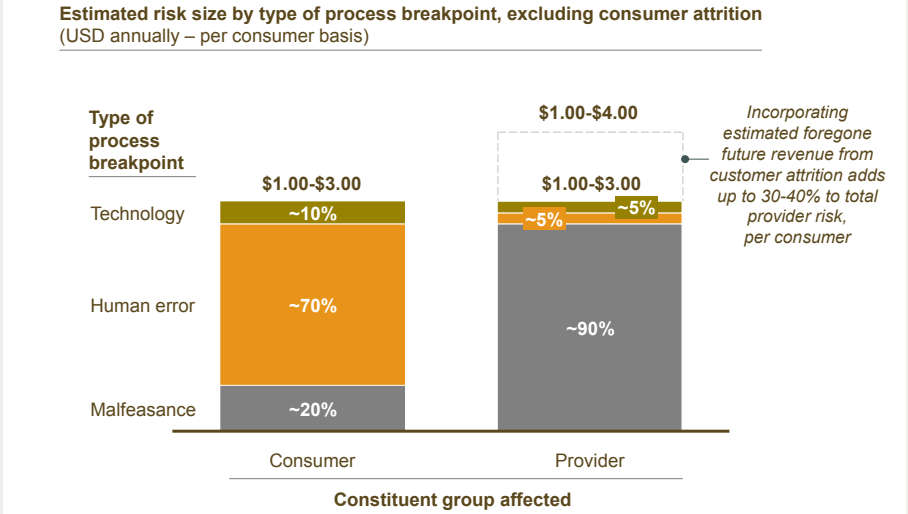


[12] For the example of power outages at base stations, a high-level approximation might look as follows: 97 percent of Kenya's 5,000 on-grid base stations have under six hours of power outage daily, 1.5 percent have from 6-to-12 hours of outage and 1.5 percent have over 12 hours of outage. Taking the mid-point of each of the given ranges and averaging – e.g., assuming 97 percent of base stations have no power for 3 hours a day since 3 is the midpoint between 0 and 6 – translates into roughly 3 hours of no power per base station. Assuming that, two-thirds of the time, power failures are backed up by diesel generators, suggests that base stations have no power for roughly 5,000 hours daily. See Powering Telecoms: East Africa Market Analysis (GSMA, 2012) for relevant statistics.

Quantifying operational risk in digital payments for providers and consumers

To illustrate the sort of insight our approach can provide, we estimate the size of operational risk in digital payments for both providers and consumers using a composite data set from our observations of and interviews with more than 10 providers in Kenya and India*. The exhibit below shows a summary of our results.

Risk sizes for providers and consumers vary significantly by type of process breakpoint



Since both the absolute and relative sizes of risks can vary significantly across markets, providers, and products, anyone making meaningful decisions based on the size of risks must undertake their own analysis. However, our analysis illustrates the typical relative aggregate size of the three types of process breakpoints – technology failure, human error, and malfeasance – and the sorts of questions users of our approach should ask themselves when quantifying risk size.

Our analysis suggests that, in general, operational risk for providers is similar to that for consumers, or an estimated $1.00-to-$3.00 per year per consumer. To put these numbers in context, for providers we estimate that this amount is roughly 10 to 30 percent of annual profit in the markets we studied. For consumers, the total estimated loss to a typical customer in the markets we studied is under 1 percent of the value that customer transacts annually using these these services. Since this figure is just an average, some consumers could suffer significantly more.

We also found that the relative contribution of the three types of process breakpoints differs significantly between consumers and providers. The greatest risk to consumers is human error – particularly from money being deposited into, or sent to, the wrong account. This is responsible for approximately 70 percent of the risk that they face. Malfeasance accounts for about 20 percent, and technology about 10 percent. Most of the contribution from malfeasance comes from small-scale fraud or scams (e.g., use of fake cash, impersonation) perpetrated on consumers, one or a small number at a time. Technology's contribution comes from the chronic issues present in many countries that affect individual or small numbers of transactions at a time, including cell phone base station power outages as well as transaction delays due to poor cell phone signals, or an agent's phone or terminal not working.

The greatest risk to providers is malfeasance, which is responsible for approximately 90 percent of the risk they face. The remaining 10 percent splits roughly evenly between human error and technology. About 80 percent of the contribution from malfeasance comes from the risk of a hack into the provider's back-end accounts that drains all consumers' funds. The remainder of the contribution from malfeasance comes from the risk of smaller-scale fraud borne by providers, largely agents, or by those providers who act as agent managers.

* Numbers used in calculations are based on averages across all of the providers from whom we gathered or observed related data, and supplemented by country-level data from public sources. As a result, the risk size at any given provider cannot be deduced from the results presented. Aggregate-level estimates on the size of operational risks are available on request.

In relatively mature markets, risks rarely fall in the upper right. Since such risks are both likely to occur, and severe if they do, providers have designed processes and systems to nearly eliminate them, and consumers do not adopt or continue to use a product that leads to regular material harm.

The largest actual risks tend to fall in either the upper left or lower right portion of the matrix. Those in the lower right occur frequently – potentially thousands or millions of times a year – but have relatively low severity. Their total risk size could be big, however, if the small consequence of many occurrences adds up to something meaningful. The case of base station power outages affecting P2P transactions provides an example (see T2 in Exhibit 5). By our estimation, in eastern African markets, a regular user may be affected by short base station power outages as many as several times a month, and we anticipate that numbers are similar in other emerging markets. The cost of each occurrence is typically minimal to both providers and consumers. If a consumer just delays her transaction, it costs providers nothing and consumers only potential inconvenience. Even if a small fraction of users contact call centers, costs to providers remain relatively small. Providers may lose more money if a significant fraction of consumers stop transacting or change providers. However, we anticipate that, as long as spotty cell phone reception remains the norm, it will not cause significant attrition for providers of digital payments.

Risks in the upper left have low likelihood, but high severity if they do occur. For many providers, these risks may never strike, but they could be crippling if they did. The case of a full system failure during a back-end migration affecting P2P transactions provides an example (see T3 in Exhibit 5). By our estimation, the likelihood of this occurring may be as small as once in 20-to-50 years, and will depend significantly on company- and project-specific factors. However, the severity of such a system failure, particularly one that lasts multiple days, could be enormous. Providers would bear significant costs (e.g., associated with fixing the system, pro-active customer communication, and fielding service calls from both customers and agents). Providers would also have to forego all revenues from P2P transactions that would otherwise have occurred, and would likely see significant customer attrition, thereby losing associated future revenues.

A number of small risks, with both low likelihood and low severity, will also fall in the bottom left portion of the matrix. Examples associated with P2P transfers may include call center employees going on strike, or agents misinforming customers about how to get refunds on misdirected transactions (H3 and H2, respectively, in Exhibit 5). Once we have determined that a risk falls in the bottom left of the matrix as so is small, we should not spend large amounts of time in estimating risk size exactly.

To show how this process for quantifying operational risk might play out across an entire market, we offer the adjacent sidebar, based on the markets we studied.

D. Develop a prioritized approach to risk management or regulation

After users of our approach to operational risk management determine the severity, likelihood, and resulting size of operational risks in their markets, they should prioritize risks for attention and subsequent action. Both the objectives of, and approach to, prioritization will vary by provider and regulator, but all will have implications for the level of financial inclusion in a particular market.

IMPLICATIONS FOR PROVIDERS

Providers must decide which operational risks to accept and which to mitigate or manage actively and, if so, how. Typically, each provider will care about the risks to itself. Providers should first identify and focus on the biggest risks, say all risks above a threshold size associated with that provider's appetite for risk (e.g., risk sizes larger than 1 percent of annual revenue). For each of these risks, the provider should systematically identify potential mitigation approaches and controls. For each proposed mitigant or control, a provider can assess both the residual risk size (size of the risk after mitigation) and the cost to implement, incorporating direct cost, forgone revenue, and any other intangible factors (e.g., feasibility given the institutional culture). A provider can use this analysis in selecting which risks to mitigate actively, which controls to put in place, and how to incorporate regulatory guidance.

After identifying the biggest risks, along with potential mitigation approaches and their implementation costs, providers may also consider ease vs. impact to address smaller risks. It may make sense to address small risks that are easy to mitigate.

As we said, the largest risk to providers is malfeasance, particularly a hack into the account storing customer funds. To manage this risk, providers can focus on minimizing the chance a hack will happen in the first place (depending on the costs involved), and/or ensure they have a contingency plan in place in the event a hack does occur.

In addition to helping providers understand where risks are large, our operational risk approach helps them understand the concerns of regulators. Through estimates of how processes could affect consumers and the financial system as a whole, our approach supports providers in proactively addressing areas in which regulators may intervene, and in actively shaping their dialogue with regulators. This is particularly relevant for providers that aim to address financial inclusion through innovative new products for which there is only a nascent regulatory framework. For example, the risk size of human error is roughly 14 times larger for consumers than for providers because consumers risk losing their entire transaction amount, while providers risk losing only the cost of reconciling the error and potential consumer attrition. By proactively working to shrink the human error risk that

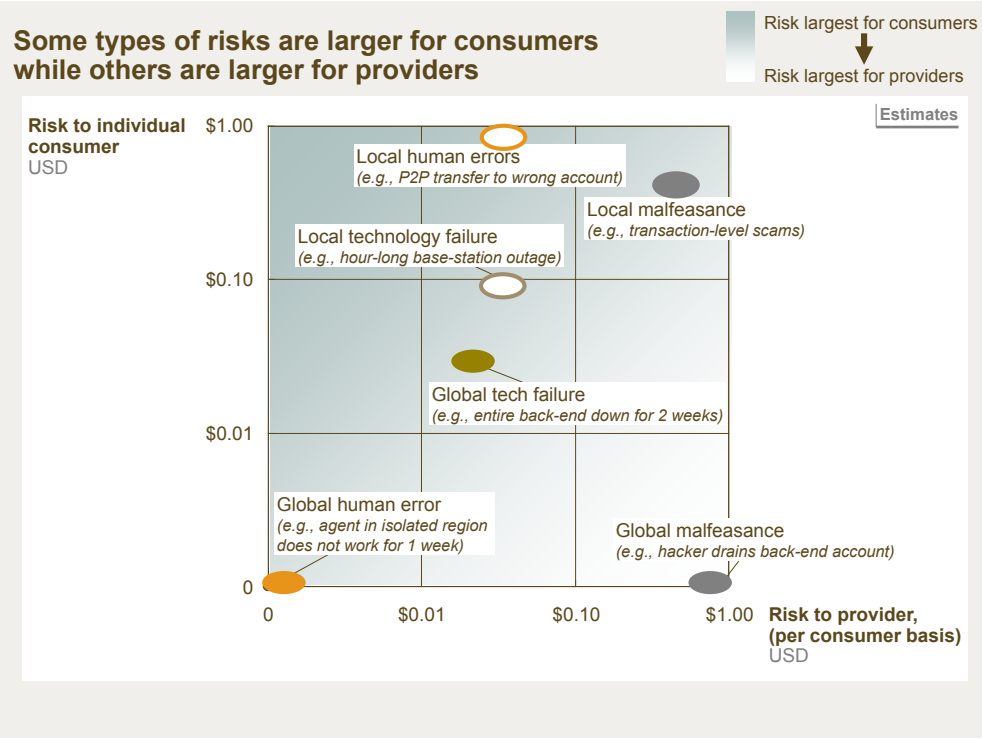
consumers face (through continued improvements to product design, for example), providers may be able to avoid situations where a regulator would step in, while simultaneously keeping their customer base satisfied.

IMPLICATIONS FOR REGULATORS

Regulators must decide where and when to allow market forces to address specific issues and where and how to intervene actively. In making their decisions, they must balance multiple goals such as protecting consumers, ensuring system stability and integrity, and promoting financial inclusion, which can include fostering an ecosystem of sustainably profitable providers. This means regulators will care about risks to consumers and the system at large, and ought also to consider how approaches to risk and regulation may affect provider costs and profitability. Regulators may focus particularly on risks that have a relatively large severity on consumers or the financial system at large, but no or limited direct economic cost to providers in the absence of specific regulation.

Regulators may find our proposed risk approach helpful as they focus on understanding where provider interests may be misaligned with those of consumers, the financial system at large, or regulator goals for financial inclusion. The discrepancy between risks to consumers and those to providers is particularly large for human error and malfeasance that affects one or a small number of consumers at a time. In such cases, without appropriate incentives, providers may not naturally prioritize managing the risk. Exhibit 6 shows a comparison between providers and consumers for sizes of risks that are local (affecting one or a small number of customers) and risks that are global (affecting most or all customers) for each of the three types of process breakpoints.

EXHIBIT 6



The fact that the effects of local human error and malfeasance are much larger on each individual consumer vs. the provider is particularly problematic for poor consumers in landscapes with minimal provider competition (where consumers have few options), or in landscapes with large illiterate populations who may not notice errors in a timely manner or understand options for recourse. The size of provider vs. consumer discrepancy, however, depends on the time window that the constituent is considering because it is in the long-term economic interest of providers to retain consumers. And, providers who suffer multiple cases of local malfeasance, for instance, may fail to retain adequate consumers over the long run. Individual consumers may stop using the service, and word of mouth may discourage even those not directly affected. Regulators may be able to play a role in encouraging providers to act in their own long-term best interest, which is also good for consumers – instead of making a short-term decision that may benefit them now, but would be detrimental in the long run. For example, by requiring providers to articulate a risk appetite that takes into account a view of future earnings, regulators can foster increased systematic thinking about the tie between short-term business decisions and business performance over time.

In concluding this section of our report, we hope that a common approach for both providers and regulators enables stakeholders to discuss and prioritize operational risk and will support meaningful conversations on how they can work together to promote financial inclusion for poor people through systematic operational risk management practices that factor in the economics to serve this population.

II. Solvency and liquidity risk

Introduction

Solvency and liquidity risk occur when a provider's ability to meet its financial obligations comes under threat, due to insufficient capital or liquid funds. In particular, solvency risk occurs when an institution cannot fully meet its obligations as they come due, even by selling all its assets, while liquidity risk occurs when an institution does not have sufficient liquid assets (e.g., cash) to meet its debts. These risks often intermingle so, for the purposes of this paper, we do not distinguish between them in detail, except when the nature of the outcome depends on the details.

The result of solvency or liquidity risk can range from manageable to serious. At the less serious end, the provider might need to curtail investment or cut back on day-to-day operations. More seriously, it might need to restructure debt, liquidate assets or default on its obligations to reimburse creditors. Such disruptions of normal business operations could potentially impact both the provider's customers and other providers with which it interacts, in ways either small or large.

A systematic approach to identifying solvency and liquidity risk, built around the payments value chain, gives structure to an otherwise complicated discussion. Providers and regulators can use such an approach to understand risks to providers, consumers, and the financial system at large, and to help stakeholders have meaningful, directed conversations.

In this section of our report, we introduce such an approach, to identify and help quantify and manage the solvency and liquidity risk associated with digital payments. To describe our approach, we have structured this section in the same basic four parts we used for operational risk. The parts describe how to:

A. Identify solvency and liquidity risks by tying them to the payments value chain.

B. Quantify the severity of the identified risks, if they do occur.

C. Quantify the size of risks by weighing their severity against the likelihood that they will actually occur.

D. Help providers and regulators develop a prioritized approach to managing and regulating solvency and liquidity risk.

We focus on how to apply the overall approach, and do not attempt to quantify severity and likelihood for specific risks at particular institutions. The details of solvency and liquidity risk depend strongly on specific features of the provider and the market, and estimating them requires in-depth knowledge of provider cash flows and balance sheets, and country laws and regulations. Precisely because complex and sometimes arcane details matter, we believe that a simple high-level approach is useful in structuring the conversation, focusing attention on the issues that matter most, and allowing non-experts to participate. This approach should be a useful tool for providers as they develop contingency plans in case they, or other providers they work with, have a capital or liquidity shortfall. It should also aid regulators as they develop requirements – including for capital, liquidity, and contingency planning – for different types of players.

Before we delve into our approach, we note that applying it has presented us with several insights about solvency and liquidity risks in digital payments. We summarize these below. Some of them will help stakeholders address how to approach managing risk, while others will provide preliminary conclusions about the severity and nature of specific sorts of solvency and liquidity risk:

1. **While digital payments do not introduce major new solvency and liquidity risks beyond those that exist in traditional payments and in the financial system at large, we see a transfer of existing risks to new participants in the value chain, who must quickly learn how to understand and effectively manage these risks.** These institutions will need to monitor, measure, and report new metrics (e.g., liquidity ratios). To do so, they can look to hire people from the banking industry with relevant experience, for example in balance sheet management. Regulators can help, through explicit supervision in these new areas, and by encouraging or requiring providers to articulate their appetite for solvency and liquidity risk.

2. **Despite the emergence of new participants, products, services, and distribution channels, approaches to managing solvency and liquidity risk used in traditional contexts remain useful.** As in traditional approaches, we quantify the size of risks by weighing their severity, if they do occur, and the likelihood that they will occur. Also in digital payments as in traditional contexts, systematic yet flexible tools can be applied across widely varying markets today, and as they evolve over time. For solvency and liquidity risk, an approach built around the payments value chain provides structure to an otherwise potentially complicated discussion. Providers and regulators can use such an approach to understand risks to providers, consumers, and the financial system at large, and to help stakeholders have meaningful, directed conversations.

3. **The largest risk associated with solvency and liquidity is to the ability of consumers to access their funds in case of a "run on the bank,"** rather than the actual safety of those deposits. This is especially true because a run on the bank with new value chains in digital payments could potentially include a "run on the telco" or "run on an agent network."

A. Identifying solvency and liquidity risks by tying them to the value chain

A capital or liquidity shortfall at a provider can prevent or hamper it from executing the business operations for which it is responsible, thus compromising processes, and potentially, the digital payments value chain as a whole. By contrast with operational risk, which depends only on the process and not on the player executing that process, the nature and magnitude of solvency and liquidity risks can vary dramatically with the details of the value chain. Solvency and liquidity risks are identified in two steps: first map the roles in the value chain and second link capital and liquidity shortfalls at the providers playing these roles to process breakpoints. As we described in the section on operational risk, breakpoints are those points in the process at which the likelihood of a breakdown leading to loss is highest, or where a breakdown would lead to a high loss. Our approach to operational risk provides a way to investigate the consequences of the breakpoint failures arising from solvency or liquidity risk at a provider.

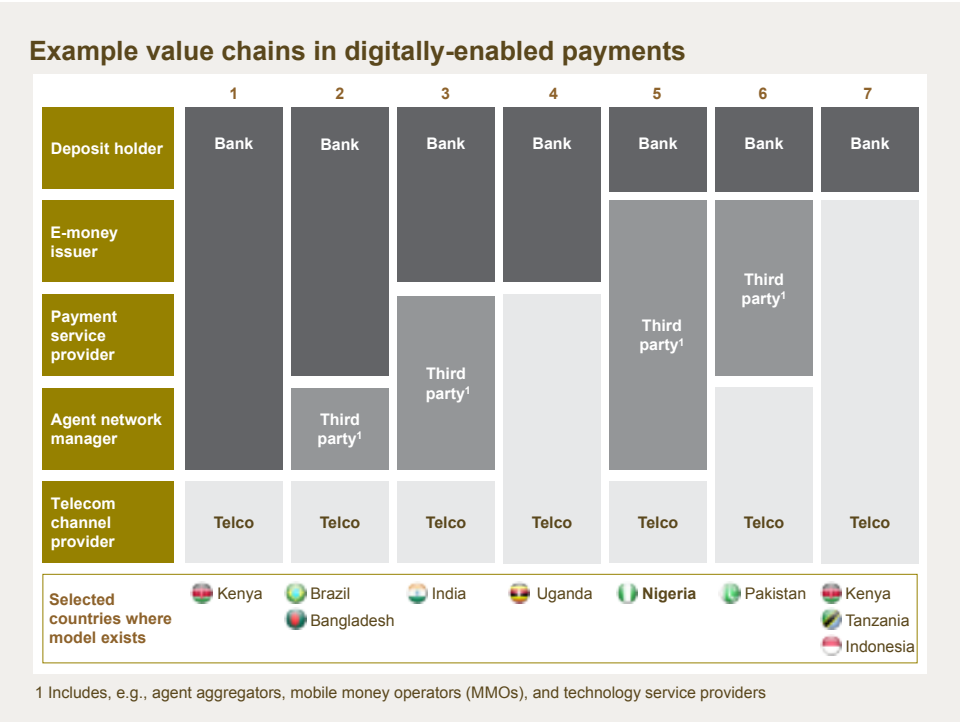
1. MAP ROLES IN THE VALUE CHAIN

This step involves laying out the roles in the value chain, understanding how these map against business processes, and identifying the type of provider playing each role – bank, mobile network operator, or other third-party provider. We can examine either an existing value chain or a new one.
While details of the value chain can differ by country, there are typically five main roles (See sidebar for further details):

- Deposit holder
- E-money issuer (EMI)
- Payment service provider[13]
- Agent network manager
- Telecommunications channel provider

Which entity – bank, telco, or other third party provider – plays each of the five main roles varies by country, and sometimes even within a single country. In all value chains of which we are aware, a bank or other depository institution plays the role of deposit holder, and a telco plays the role of telecom provider. Banks, telcos or third-party providers can play each of the remaining three roles. Exhibit 7 shows a selection of models that exist across the world today. We note that variation can exist even within a given model, for example in relative rights and authorities of the various parties.

EXHIBIT 7



1 Includes, e.g., agent aggregators, mobile money operators (MMOs), and technology service providers

[13] Many value chains contain technology service providers (TSPs) and/or Aggregators. Sometimes, but not always, the same company plays the role of TSP and/or Aggregator. We do not include all potential roles for simplicity. The analysis would proceed in the same way, were they included.

India and Kenya provide two typical models. Kenya supports value chains for two types of digital payments: mobile money and digitally-enabled agent banking. In the mobile money value chain, several different banks are deposit holders, while telcos play all remaining roles (these can include money issuer, payment service provider, agent network manager, and telecommunications channel provider, with some variation across markets). For digitally-enabled agent banking, banks typically play all roles except for that of the telecommunications channel provider (i.e., deposit holder, money issuer, payment service provider, and agent network manager)[14].

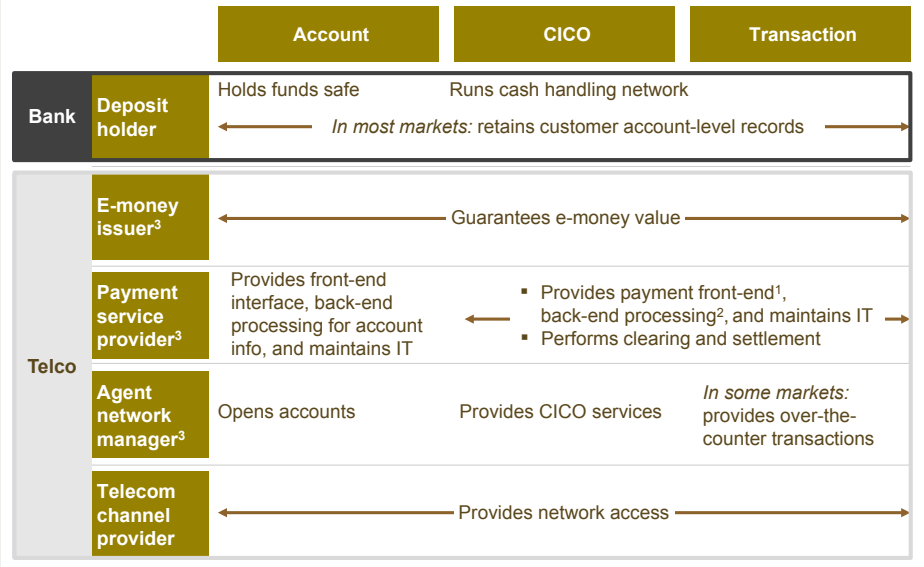
India has an agent banking model, in which consumers hold accounts directly with banks, which play the role of deposit holder and e-money issuer[15]. Third-party providers offer both payment services and agent network management as part of the so-called business correspondent model. In some cases, the same third party plays both roles (e.g., A Little World, Eko, FINO, and Integra Micro Systems) . In others, the two roles are split between two providers (e.g., Eko acts as the PSP for Cashpor, working with ICICI bank).

In coordination, the providers in the five main roles carry out the business processes in the value chain. Users of our approach can map roles, first against elements of the ACTA framework and then, in a more detailed way, against the most important business processes.

Exhibit 8 shows an example of the mobile money value chain in countries such as Kenya, Tanzania, and Indonesia (value chain type 7 in Exhibit 7). The process mapping is based on how each of the five main roles typically contributes to processes associated with each of Account, CICO, and Transactions. Note that, as in the operational risk section, we focus just on ACT, since Adjacencies activities typically involve processes that extend beyond systems themselves.

EXHIBIT 8

Example value chain mapping including providers, roles and processes associated with Account, CICO, and Transactions



1 For example, phone interface for agents and customers, agent biometrics devices, customer enrolment tools such as web camera
2 Can include exceptions processing and fraud, invoicing and reporting, and the technical aspects of capture and authorization
3 One or more of e-money issuer, technology service provider, or agent network manager provides call center customer service

[14] Note that some banks have now become mobile virtual network operators (MVNOs), e.g., Equity Bank in Kenya. In so doing, they gain some but not all aspects of telecom infrastructure (not base stations and back-haul links that connect networks). The details of associated risk profiles is not the mission of this paper.

[15] Recent payments bank legislation in India could potentially lead to changes in models.

2. LINK CAPITAL OR LIQUIDITY SHORTFALLS AT PROVIDERS TO BREAK-POINTS IN THE PAYMENTS VALUE CHAIN.

When a capital or liquidity shortfall triggers a breakpoint failure, this generally has one of three degrees of impact on a provider's ability to play its roles in the payments value chain:

- **Curtailed operations.** The provider shrinks its range of operations, for example, by closing outlets, reducing available services, or limiting its hours of operation. This may force the provider to stop or alter some processes in the payments value chain. This may, in turn, trigger other providers to stop or alter some of their processes in the value chain, if those processes are contingent on the troubled provider.

- **Temporarily ceased operations.** The provider ceases all operations for a period of time, so temporarily does not carry out the processes for which it is responsible.

- **Permanently ceased operations.** The provider ceases all operations permanently. Thus, processes in which the provider plays an essential role are likely to cease, unless there is a contingency plan. Processes in which the provider plays a non-essential role can continue, potentially only partially or imperfectly. The case of the deposit holder ceasing operations has some unique features so we say a few general words about this particular case, acknowledging that the reality is complex and situation-specific.

  When a deposit holder ceases operations, it can no longer hold customer deposits. It can deal with this in four ways. (1) immediately disburse all customer deposits in full; (2) delay before disbursing consumer deposits in full (e.g., while assets are liquidated or debt is restructured); (3) disburse some, but not all, money to depositors; (4) do not return any money to depositors[16].

[16] Partial deposit disbursement corresponds to a partial bank default - the bank respects some of its debts, including some of those to deposit holders. No deposit disbursement corresponds to a complete bank default – the bank is unable to respect its debts to depositors.

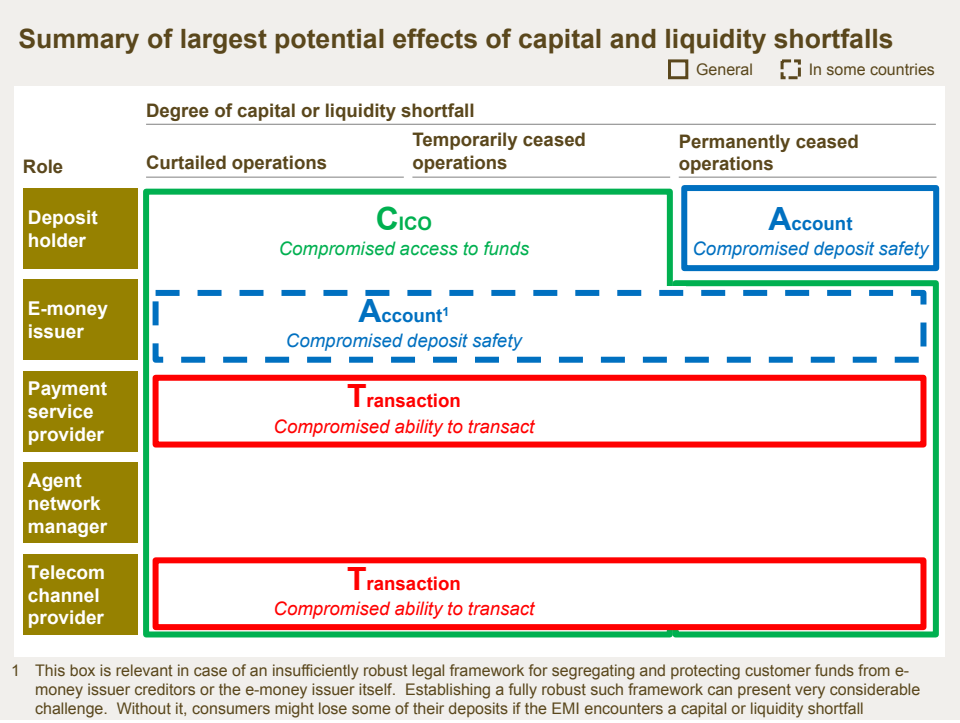
B. Quantifying the severity of the identified solvency and liquidity risks

After we identify the solvency and liquidity risks in a digital payments system, the second step in our risk management approach uses tools to quantify the severity of those risks. For each constituency – providers, consumers, and the financial system at large − the severity of a risk depends on its collective impact on all the processes for which providers are responsible.

For example, in the value chain shown in Exhibit 8 (above), we would first look at the effect of a capital or liquidity shortfall on processes that the deposit-holding bank undertakes. These include holding funds safe, running the cash-handling network, and retaining customer account-level records (in most markets). Next, we would look at the effect of a capital or liquidity shortfall on the processes that a telco undertakes, in each of its roles, e.g., money issuer, payment service provider, agent network manager, and telecommunications channel provider. These processes include providing the front-end interface, back-end processing, and IT maintenance for processes associated with Accounts, CICO, and Transactions. e.g., opening accounts, providing cash-in and cash-out services, and providing access to the telecommunications network.

Characterizing a capital and liquidity shortfall at a given provider in terms of its effect on ACT can be a helpful way to structure quantification of the overall severity of that shortfall. Here, we highlight the most important categories of impact, which are also summarized in Exhibit 9.

EXHIBIT 9



1 This box is relevant in case of an insufficiently robust legal framework for segregating and protecting customer funds from e-money issuer creditors or the e-money issuer itself. Establishing a fully robust such framework can present very considerable challenge. Without it, consumers might lose some of their deposits if the EMI encounters a capital or liquidity shortfall

- **Compromised safety of customer funds – associated with Account.** Consumers might lose some or all of the money they have deposited in the system if the deposit holder (always a bank) undergoes a partial or complete default. We also note that in the case of an insufficiently robust legal framework for segregating and protecting customer funds from e-money issuer creditors or from the e-money issuer itself (e.g., to cover emergency operational expenses), consumers might also lose some of their funds if the e-money issuer encounters a capital or liquidity shortfall[17].

- **Compromised access to funds – associated with CICO.** Any form of capital or liquidity shortfall affecting the payment service provider, agent network manager, or telecom provider may seriously compromise the ability of customers to cash-out their money easily or when they want it.

- **Compromised ability to transact – associated with Transaction.** Consumers may lose the ability to pay and be paid in the way in which they typically do if a payment service provider or telecom channel provider ceases operations temporarily or permanently.

Next, we examine in greater detail the contribution to risk severity of each of these categories of impact.

COMPROMISED SAFETY OF CUSTOMER FUNDS

As we noted above, there are two ways that safety of customer funds might be threatened. First, the deposit-holding institution can fail. Second, an e-money issuer can fail in the case of a legal framework that does not sufficiently isolate the customer funds held by that EMI from its operational expenditures or creditors.

Here we focus on compromised safety of customer funds coming from a deposit holding-institution permanently ceasing operations, since this is a risk in all countries. We also focus on banks, which typically play the deposit holder role in digital payment value chains.

The answers to two questions determine whether consumers lose money if the deposit holding institution permanently ceases operations:

1. Will the deposit holder eventually be able to pay back consumers' funds? Two factors shape the answer: a) creditor hierarchy, and b) the degree of segregation of funds.

2. If the deposit holder cannot pay back consumers, is there anything else in place to help them get their money back? Two additional factors shape this answer c) the existence of deposit insurance, and d) the obligation of e-money issuers to reimburse consumer funds.

[17] This is a complex subject, about which few generalizations are possible. That said, we note existence of various regulatory frameworks for segregating depositor funds from EMI creditors and operational uses. Terminology varies and includes, trust account, escrow account (e.g., see Mobile Money Guidelines 2013 – Uganda), settlement account (e.g., see Regulatory Framework for Mobile Payment Services in Nigeria). The soundness of customer funds protection depends on robust and properly implemented trusts legislation and consistent application of bankruptcy law and other relevant legislation. For example, establishing that mobile money users are the beneficiaries of the pooled account may not be sufficient to protect them against possible losses.

Answering Question 1: Will the deposit holder be able to pay?

A. Creditor hierarchy. When a bank cannot reimburse all of its creditors fully, they are typically reimbursed in a specified order that can vary by country. Along with deposit holders, other claimants will include the tax revenue authority, employees, the central bank, bond holders, and other general unsecured creditors. The higher consumer deposits or other funds fall in the hierarchy, the more likely the bank will be able to pay them back.

B. Segregation of funds. At a conventional bank, consumer deposits sit on the balance sheet, and can be used to issue loans, or buy other assets. The bank will then hold some fraction of deposits in cash, to ensure it has enough cash on hand when depositors wish to make a withdrawal. Beyond this, there are rarely specific restrictions on how a bank can use particular consumer deposits. Instead, there are overall restrictions on liquid assets that a bank must hold in reserve in case consumers withdraw their deposits. In some countries, however, non-bank e-money issuers put some or all of their customers' funds in isolated investments. There are two typical ways that this happens. First, e-money issuers are sometimes required to deposit funds into bank-held accounts that are isolated from the rest of the bank's balance sheet, and themselves may be invested only in specified safe asset types. For example, multiple countries require that the bank hold the deposits in highly liquid and safe securities such as sovereign bonds. When this happens, safety of depositors' money hinges on the specifics of the investments made. Second, some countries allow EMIs to directly invest a portion of consumer deposits in safe investments, and keep the residual with a depository institution[18]. In both of these cases, the safer the isolated investments, the more likely the bank will be able to pay back consumer deposits.

Answering Question 2:
If the deposit holder cannot pay, is there anything else to help consumers get their money?

C. Deposit insurance. Deposit insurance is protection, usually government provided, to depositors against losing money when their bank (or other depository institution) fails[19]. Typically, this insurance pays up to a fixed maximum amount per deposit account. The higher the deposit insurance cap, the more money people can recover even if the deposit holder is unable to pay them back directly. Of course, deposit insurance only helps consumers get their money if it is both binding and implemented, both of which can pose challenges.

D. E-money issuer obligation to reimburse consumer funds. In the markets we examined, we have not found explicit language about (or a case history on) the legal obligation of e-money issuers to repay customers if the deposit-holding bank fails and cannot repay. In general however, depositors will get more money if EMIs have a strong obligation to make them whole (e.g., from regulators), or a strong willingness to do so (e.g., to retain them as customers).

In examining how these factors weigh on the risks of digitally enabled accounts, it is helpful to compare how they weigh on traditional bank accounts in the same countries. In some cases, the risks are quite different (see sidebar below).

---

[18] Examples of this approach include the Philippines (see *Circular 649*), the West African Economic Monetary Union (see *Instruction No. 1 of 2006, Article 18*), and the European Union (see *Article 7 of the 2009 EU E-Money Directive* and Article 9(1) and 9(2) of the *2007 EU Payment Services Directive*).

[19] Typically, deposit insurance is funded through regular assessments on the insured depository institutions.

Comparing the risk of compromised deposit safety in digital payments accounts to that of traditional bank accounts

The severity of solvency and liquidity risks in the traditional retail banking sector provides a useful comparison point for these same risks in digital payments accounts. We consider a very general comparison in terms of the four factors that influence the severity of compromised deposit safety.

- **Creditor hierarchy.** In principle, e-money issuer accounts could have either higher or lower priority than traditional retail banking deposit accounts in the creditor hierarchy. In some markets – including Kenya, Indonesia, and Uganda – accounts held by e-money issuers (pooled accounts made up of individual customers' mobile money accounts) have the same priority as traditional accounts. The situation may differ, however, in markets that treat accounts held by e-money issuers as "accounts payable."
- **Segregation of funds.** As explained earlier in this report, e-money issuer accounts may be isolated in investments, rather than as a standard deposit account. Typically they are tied either to a country's currency (e.g., if money is kept in a cash settlement account) or to sovereign bonds. The level of safety relative to a retail banking account hinges on whether in-country banks are a better or worse credit risk than the country itself. If banks are safer, the traditional account is safer. If banks are less safe, than the e-money account is safer.
- **Deposit insurance.** Depending on country and business model, the effective deposit insurance for digital payments consumers is either the same or smaller than that for traditional banking accounts. It is the same in the case of pass-through deposit insurance, which currently exists for mobile money customers in the U.S. only. The Kenyan Deposit Insurance Act of 2012 includes a provision for similar insurance, but this has not yet been implemented. Deposit insurance for digital payments accounts can be smaller in two ways. In the first, the maximum insured amount for an individual digital payments account can be smaller than that for a traditional bank account. In Nigeria, for instance, the Nigerian Deposit Insurance Corporation (NDIC) has considered adopting a lower level of deposit insurance for small value accounts, which would include mobile money accounts. In the second, deposit insurance is on a pooled account of individual mobile money accounts, held by an e-money issuer at a bank. In this case, the insurance is substantially diluted, so the effective insurance on any individual account can be negligible.
- **E-money issuer obligation to reimburse account holders.** In the case of traditional deposit accounts, no additional party such as an EMI exists to make depositors whole if the bank cannot meet its obligations and deposit insurance is insufficient (or doesn't exist). Therefore, because of the existence of the EMI, in some instances e-money accounts could actually be safer than traditional bank accounts, if the EMI is obligated to reimburse consumers.

When a country lays out its regulatory position on how these four factors will impact the digital account system, it implicitly decides how risks associated with safety of funds will be different from traditional bank accounts. It is useful to consider several examples.

First, in India, agent bank accounts are configured the same as traditional bank accounts. Therefore, the likelihood that funds are threatened, and the size of loss to consumers in case of default, are the same as a traditional account.

In Kenya, the situation is more complicated. Mobile money deposits are kept in major local Kenyan banks and occupy the same position on the depositor hierarchy as other deposit accounts. Therefore, the likelihood that funds are threatened is the same as traditional bank accounts. However, if a bank does fail in Kenya, mobile money deposits are currently insured only as a single pooled trust account, so deposit insurance is effectively zero for individual accounts and mobile money account holders risk losing nearly all of their money (unless the mobile money providers provide reimbursement). By contrast, deposit insurance for traditional bank accounts in Kenya covers up to approximately $1,150 USD per account, which is roughly the same as the average consumer account in Kenya.

Nigeria also presents a complicated picture. Currently Nigeria offers no deposit insurance for mobile money accounts, potentially putting 100% of funds at risk if a bank default does occur. By contrast, traditional bank accounts in Nigeria have deposit insurance up to roughly $3,100 per account in universal banks (and $1,200 per account in micro-finance banks). The average consumer demand-deposit account in Nigeria holds roughly $1,100, or less than the deposit insurance amount.

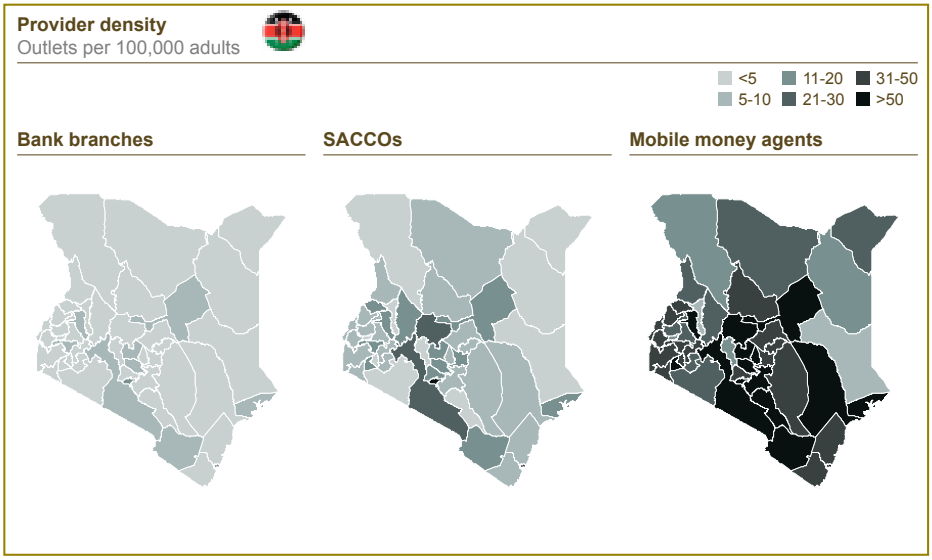
COMPROMISED ACCESS TO FUNDS

When a provider has a capital or liquidity shortfall, consumers might not be able to cash out their money easily or when they want it. Failure of a bank that holds traditional deposit accounts provides a useful starting point for comparison. When such a bank fails – or when its customers are afraid that it might fail – customers may rush to bank branches or ATMs to withdraw their money. If a branch or ATM does not have enough cash on hand, the customer may be turned away empty handed. If the bank does not have enough cash or ready liquid assets, customers may need to wait some time until the bank can generate cash and then move it to branches for distribution[20].

Since digital payments and banking rely on agents to perform cash-out, however, the severity of the impact from the inability to do so may be significantly higher than it is for traditional retail accounts. For a consumer to get cash, an agent must first get that cash[21] and then be available and willing to distribute it, often in remote areas where no bank branches exist. (As an example, Exhibit 10 shows the distribution of bank branches, savings and credit cooperative societies (SACCOs), and mobile money agents in Kenya).

EXHIBIT 10

Reach of mobile money agents in Kenya is much wider than that of the formal banking sector



SOURCE: CBK – *Bank Supervision Annual Report (2011);* themix.org

[20] If deposit-holding bank defaults, deposit holders may need to wait to cash out any money the bank pays out. Cash disbursement may look somewhat different from the case described above.

[21] The model for getting cash to agents varies across the world. In some markets, such as for mobile money in East Africa, agents are responsible for "rebalancing"' their own accounts, going to a bank branch or a "super-agent" to stock-up on cash. In other markets, such as in India, the agent manager (in the banking correspondent model), or another third party carries cash to the agent.

We highlight two particular challenges in ensuring that agents get the cash they need, and are willing to distribute it:

- **Agent ability to collect cash (i.e., rebalance).** Several issues may stand in the way: How do bank branches distribute cash and in what order of priority? Where do agents fall in this order of priority? Particularly given that many agents live and work away from bank branches – closer to their actual customers – how well prepared will they be to pick up money from bank branches?

- **Agent willingness to distribute cash they manage to collect.** In most models, agents trade their own money for e-money or other form of credit. For example, when an agent provides a consumer with a $100 withdrawal, he gets $100 worth of e-money in return. That $100 is the agent's own. When the system is functioning well, the agent knows that he can redeem the $100 worth of e-money for cash from the bank or e-money issuer. However, if the bank is failing – or if its customers are afraid that it might fail – the agent may not be willing to disburse cash to users, fearing he will not get it back from the bank.

COMPROMISED ABILITY TO TRANSACT

If transaction flow through a digital payments system is sufficiently large, an interruption in system functioning would not only hurt individual consumers, it could actually harm the economy. However, even in Kenya, where mobile money represents the largest segment of payment flows as a percentage of GDP (49% in 2013), mobile money flows are only roughly 7% of total payment flows in the country, based on Central Bank of Kenya and World Bank statistics.

HOW DIFFICULTIES AT ONE PLAYER CAN HARM OTHERS IN THE VALUE CHAIN

When one player in the value chain ceases, temporarily halts, or curtails operations, others may be harmed as well. As an examples, we describe two ways in which this might happen. First, when a third-party payment service provider or agent network manager works with several e-money issuers or banks, a capital event at one bank, or e-money issuer, could contribute to the collapse of the third party. This in turn could harm the business of the other EMIs or banks working with that third party. For example, in India, failure of a significant bank could contribute to the collapse of a business correspondent (playing the role of agent network manager). In turn, this would harm the agent banking business of other banks relying on that collapsed business correspondent. Since agent banking currently represents a small percentage of revenues and customer base for all banks, this would not compromise the overall integrity of the surviving banks. However, it might temporarily hamper their ability to operate in mobile money or agent banking.

Second, when various companies rely on one dominant provider, if something happens to that provider, the companies would immediately be hurt. We see this risk in Kenya. Numerous companies have developed a product that is dependent or sits atop one e-money issuer.

C. Quantifying the size of solvency and liquidity risks by weighing severity against likelihood

Having presented a systematic way to assess severity of solvency and liquidity risks, we now discuss estimating the likelihood those risks will actually occur, and then weighing these two against each other to quantify the size of the risks. Doing so can give an objective view of the relative importance of various solvency and liquidity risks, compared to one another and compared to operational risk.

In principle, determining risk likelihoods involves estimating the probability that various providers in the value chain will encounter shortages of capital or liquidity. In this report, however, we will not attempt to estimate the absolute likelihood of such shortfalls at any particular types of providers. In general, such likelihoods depend strongly on specific features of the provider and of the country in question, and estimating them requires in-depth knowledge of provider cash flows and balance sheets[22]. For instance, to limit the probability of failure, depository institutions typically are required to hold capital and liquid funding according to specific rules, typically guided by the Basel accords but with country-specific variation[23]. So, the probability of an issue at a bank is determined by the stringency of capital and funding requirements in a country[24]. Capital and funding requirements at non-bank financial institutions can vary significantly across the world, depending on jurisdiction and on the exact range of activities undertaken by the company.

In the sidebar, we offer an indicative template for systematically examining the severity, likelihood, and the resulting size of solvency and liquidity risks for providers in a particular value chain.

[22] Note that when a country has specific quantitative regulatory requirements, they can provide a rough tool for assessing likelihood of failure, since many are constructed to guard against issues to a very high and sometimes explicit level of probability.

[23] The Basel Accords (Basel I, Basel II, and Basel III) are recommendations on banking laws and regulations issued by the Basel Committee on Banking Supervision. Basel III, the most recent, provides a global, voluntary regulatory standard on bank capital adequacy, stress testing and market liquidity risk. It was finalized in 2010–11, with a plan for phased implementation through 2019. Today, countries are at various stages of implementation.

[24] Apart from specific capital and liquidity rules (e.g., Tier 1 common capital ratio, common equity ratio, net stable funding ratio), additional country-specific factors may contribute, including GDP growth, interest rates, and changes in the level of formal sector employment.

Estimating solvency and liquidity risk severity, likelihood and total size

The exhibit below illustrates the template for sizing solvency and liquidity risk in a given value chain. In the gray box at the top, we describe each risk by type of provider and the degree of shortfall it experiences. As an example, we could use the mobile money value chain in Tanzania in which a bank plays the role of deposit holder, and a telco plays all other roles. In this value chain, one risk to examine would be that of the bank permanently ceasing operations.

To determine total risk severity, we first break out the severity of the risk in Accounts, CICO, and Transactions, in monetary value. In each of these rows, we estimate the collective severity from a breakdown of the associated processes for which the provider in question is responsible, taking advantage of our approach to operational risk to make these estimates. We get total severity by adding up the contributions from each row. Next, in the likelihood row, we estimate the number of occurrences of the given risk in a single year, noting that likelihood is the same for both providers and consumers. Since solvency and liquidity risks are typically infrequent but severe, numbers in the likelihood row will typically be much less than one, but severities will have large monetary values. In the bottom row, the product of severity and likelihood gives the total monetary size of the risk for the year.

Sample worksheet for estimating size of each potentially important risk

Type of provider (bank, telco, other): _____

Degree of shortfall (curtailment, temporary cessation, permanent cessation): _____

	Other providers in value chain				
	Provider 1	**Provider 2**	▪▪▪	**Consumers**	
Severity					Sum of contribution across processes in and across each of ACT
Account					Estimated contribution to severity from processes associated with each of ACT
CICO					
Transaction					Estimated contribution to severity from processes cutting across multiple of ACT
Cross cutting (across ACT)					
Likelihood					Expected number of occurrences per year
Total risk size					Expected number of occurrences per year

Worksheet – user to fill in for each risk

Each provider in the value chain (other than the one undergoing the capital and liquidity event) can complete the columns for “Provider 1”, “Provider 2”, etc. to quantify their risks. For the Tanzanian example mentioned above, a telco would complete a provider column, assessing the severity of the impact on it from a bank permanently ceasing operations. Regulators would complete the “consumer” column, and potentially all or some of the “provider” columns. Estimating numbers in the consumer column can help regulators ensure they focus on areas that matter most to consumer protection. Estimating numbers in the provider column helps regulators understand when provider and consumer interests are aligned – when a risk is similarly sized for both – and identify any potential areas where providers are underestimating the size of significant risks.

D. Helping providers and regulators shape a prioritized approach to solvency and liquidity risk management and regulation

After users of our approach to solvency and liquidity risk determine the severity, likelihood, and resulting size of such risks in their markets, they should prioritize risks for attention and subsequent action. While both the objectives of, and approach to, prioritization will vary by provider and regulator, all may have implications for the level of financial inclusion in a particular market.

IMPLICATIONS FOR PROVIDERS

For most substantial providers today, merely offering digital payments does not meaningfully increase solvency or liquidity risk. For the vast majority of banks and telcos, digital payments represent only a small part of their business. In the face of a capital or liquidity shortage, most will focus on their larger businesses, which may be in danger. Furthermore, we note that in many cases, such a shortage will arise from causes unrelated to digital payments, and will impact all of a provider's businesses and activities. For example, a bank might fail because of defaults in commercial loans, or a telco might have a capital shortage following a capital investment that does not produce projected revenues.

However, providers must decide when to accept and when to mitigate or manage such risks that emerge from others in their digital payments value chain. For example, in the value chain shown in Exhibit 8 if the deposit-holding bank permanently ceases operation and is unable to reimburse consumer deposits, the telco in that value chain will face severe issues. It may be liable for reimbursing its customers itself, depending upon the nature of its legal obligation as e-money issuer. Even if it is not legally liable, the telco must decide whether it is willing to allow its customers to lose money through the bank default, thus running the risk of severe customer attrition and resulting foregone revenue.

A given provider should identify each provider (if any) in its value chain at which a capital or liquidity shortfall of given degree poses meaningful risk. Providers should identify and focus on the biggest such risks above a threshold associated with their appetite for risk (e.g., risk sizes larger than 1 percent of annual revenue). In practice, this means that providers should focus on those solvency and liquidity risks that are as large as the operational or other risks on which they also focus.

Next, the provider should systematically identify and assess potential mitigation approaches or controls against meaningful risks. For each proposed mitigant or control, a provider should assess both the residual risk size (size of the risk after mitigation) and cost to implement, incorporating direct cost, potential forgone revenue, and any other intangible factors. A provider can use this analysis to select which risks to actively mitigate, which controls to put in place, and how to incorporate regulatory guidance.

To give an example, we return to the case of the defaulting deposit-holding bank in Exhibit 8. We offer four examples of risk mitigants or controls that a telco might adopt, singly or in combination.

First, a telco could adopt stringent and transparent standards for the deposit-holding banks it uses. It might use only banks with credit ratings above a given threshold, or banks that maintain capital ratios well above regulatory minimums, or that are in or near Basel III compliance. Such banks generally will have a lower probability of default. Imposing such standards, however, may mean that a telco will need to compromise on commercial terms or the level of service it receives from its banks.

Second, a telco could also distribute its deposits across multiple banks. This would decrease the risk to the telco from a single bank default. However, it also means the telco may need to compromise on commercial terms with the bank, and operational efficiencies coming from economies of scale and using a single back-end interface.

Another mitigant might be holding insurance against failure of the deposit-holding bank. This would need to be arranged on a customized basis and would cost the telco money every year. As a result, the telco would have to weigh a certain annual cost against its willingness to bear the larger cost if its deposit-holding bank fails.

Fourth, a telco might negotiate a pre-existing line of credit with another bank, or potentially with the central bank in the country in question, if legally feasible. This would carry a cost, both to maintain access to the undrawn line and/or actually using the line .

In addition to helping providers understand where risks are large, our approach to solvency and liquidity risk helps them understand the concerns of regulators, and actively shape dialogue with them. This is particularly relevant for providers that aim to address financial inclusion by participating in innovative and new value chains, splitting responsibilities between providers in ways not seen in traditional banking.

For example, in the traditional banking value chain, banks run their own branches. By contrast, in digital payments systems in many countries, banks rely on third-party agent network managers for digital payments, through a wide variety of different arrangements. Solvency or liquidity risk at a third-party agent network manager could severely compromise the ability of an e-money issuer to serve its customers. By proactively and transparently working to mitigate this risk, providers may be able to protect customers while avoiding regulation that hinders continued innovation around which sort of companies can act as agent network managers.

IMPLICATIONS FOR REGULATORS

As with operational and other types of risk, regulators must decide where to leave the market to function without additional constraints, and where and how to regulate actively. In making their decisions, they must balance multiple goals such as protecting consumers, ensuring system stability, and promoting financial inclusion. They may also include fostering an ecosystem of sustainably profitable providers, and promoting consumer awareness and a positive perception of formal financial systems. This means regulators should care about risks to consumers and the system at large, and may also consider how approaches to risk and regulation may affect provider costs and profitability.

Regulators may focus particularly on risks that have a relatively high severity for consumers or the financial system at large, but would not be severe for providers in the absence of specific regulation. For example, in the absence of regulation, mobile money operators (MMOs) might not focus on developing careful contingency plans in case they fail to disburse funds to digital payments customers. Having and executing such a plan may provide no direct benefit to the MMO, since it might have already failed, but it would benefit consumers.

Each market will settle on different mechanisms and levels of regulation, but we caution regulators from imposing regulation meant to control solvency and liquidity risks in the new digital payments space without first attempting to specify and quantify those risks. Regulation disproportionate to actual risk may ultimately harm prospective poor customers, by discouraging provider entry and curbing profits from serving low income users. Our analysis suggests that in the general case, traditional banking legislation offers a guide that could cover providers beyond banks, to prevent failures and other high-impact events, while at the same time encouraging or requiring providers to develop clearly thought out risk appetites and contingency plans in case of their own failure, or that of others within their digital payments value chains. Over time, countries will gain more experience with digital payments and may adjust regulation accordingly.

In concluding this section of our report, we hope that our systematic approach to structuring discussion about solvency and liquidity risk will help support meaningful conversations among regulators, providers, and other stakeholders. This should help relevant stakeholders work together to promote financial inclusion, while providing sufficient protection to consumers, and accounting for providers' economics.

III. Other risks

In order for providers to operate profitably while serving poor people, they will need to add adjacent revenue-generating activities to the basic payment system. These "adjacencies" include financial services such as long-term savings, lending, and insurance products. Adjacencies increase the scope of operational risk, and alter the nature of solvency and liquidity risk. Moreover, they introduce additional risk types including credit risk, counter-party credit risk, and interest rate risk, which affect providers, consumers, and the financial system at large.

Beyond these risks, providers encounter risks to profitability, strategic risk, and reputational risk – all of which influence their ability to earn positive returns with reasonable certainty. In this section, we outline these other risk types associated with digital financial services beyond payments. The discussion is at a higher level than we offered for operational risk and solvency and liquidity risk alone.

Risk types involving adjacencies

The impact of risks introduced by adjacencies depends on the providers' business model and nature of their partnerships. Here, we offer some ways to understand these risks broadly. (Exhibit 11 has an overview of these adjacency risks, compared with those for digital payments alone.)

EXHIBIT 11

Risk types associated with digital payments and credit-linked activities

Focus of this paper
Focus of this section

Risk Type	Digital payments	Credit-linked activities
I. Operational risk *Results from inadequate of failed internal processes, people, and systems or from external events*	✓	✓
II. Solvency & liquidity risk *Occurs when a provider's ability to meet its financial obligations comes under threat due to insufficient capital or liquid funds*	✓	✓
III. Other risks		
Credit risk *Occurs when a borrower defaults on a debt*		✓
Counterparty credit risk *Occurs when the counterparty to a transaction defaults before final settlement*		✓
Interest rate risk *Arises from interest rates changes affecting net interest income or investment value*		✓

INCREASING THE SCOPE OF OPERATIONAL RISK

Engaging in adjacent revenue-generating activities requires additional processes, roles and responsibilities for people, along with new systems capabilities. All of these increase the scope of operational risk. Our process-based approach to operational risk, discussed in Section I, extends to this broader range of activities, providing a way to identify, size, and manage risks associated with Adjacencies (see sidebar for discussion of our ACTA framework – Account, Cash-in-cash-out, Transactions, and Adjacencies).

ALTERING THE NATURE OF SOLVENCY AND LIQUIDITY RISK

Providers who offer credit, long-term lending, or insurance products have a more complicated solvency and liquidity risk profile than those who are only providing payment services. Products with a credit component introduce additional threats to capital – in case borrowers default or insurance claims are larger than foreseen – necessitating more complicated calculations of how much capital providers should hold, to buffer against solvency risk. Offering both credit products and other lending products also makes managing liquidity risk more complex, since institutions must balance a more complicated set of cash inflows (e.g., from loan payments and insurance premiums) against outflows (e.g., from occasional large withdrawals of money from savings accounts). Furthermore, a capital or liquidity shortfall at a provider would impact its ability to provide financial services beyond payments. Our value-chain-based approach to solvency and liquidity risk, discussed in Section II, extends to this broader range of activities, providing a way to identify, size, and manage associated risk.

INTRODUCING OTHER RISKS

Financial services adjacencies linked to credit introduce three main types of additional risk -- credit risk, counterparty credit risk, and interest rate risk[25]. Today, these risks apply primarily to financial institutions, and other entities to a lesser extent (i.e. telcos offering post-pay). In the future, we could envision new participants providing services linked to credit, and thus being exposed to these three risk types. Therefore, we add these risk types to our simple framework when considering risks in digital financial services beyond digital payments (refer back to Exhibits 1, and 2). The resulting overall view of risk can help stakeholders categorize and discuss it in a way that welcomes others to join the conversation, without misunderstanding.

- **Credit risk** is the risk that a borrower will default on a debt by failing to make required payment. From a provider perspective, impact can include lost principal and interest, disruption to cash flows, and increased collection costs. From a consumer perspective, impact includes the potential consequences of receiving a loan for an amount, or on terms, that are inappropriate. For example, consumers may get caught in a cycle of paying large fees, or have collateral repossessed, resulting in a net financial loss. In countries where credit scores and credit bureaus are in place, their credit history may be irrevocably harmed. From the perspective of the system at large, correlated or excessively risky lending across a country can contribute to financial instability, typically as a cause of capital or liquidity shortages. Conversely, excessively tight credit standards -- in general or for a particular type of borrower or industry -- can hamper financial growth. As long as lending to very poor populations represents a small fraction of overall lending in most countries, then the associated credit risk will have a limited impact on the financial system at large[26].

[25] Credit-linked financial service adjacencies may also introduce price risk (or market risk), and risk of changes in the value of traded instruments. A bank that holds a variety of different types of loans (assets) and deposits (liabilities) on its balance sheet likely will purchase instruments to help manage liquidity risk and interest rate risk, and thus will be affected by changes in instrument value.

[26] Though indebtedness of low-income consumers can contribute to systemic credit risk (e.g., it played a role in the recent sub-prime crises in the U.S. and U.K.), country-level systemic risk from lending to the very poor likely will remain limited in the foreseeable future, even as the credit market for those at the bottom of the pyramid grows. For example, in Kenya, the aggregate income of all people with average earnings of under $1.25 per day is equivalent to roughly 10% of total banking assets (based on 2005 World Bank numbers). Currently less than 15% of this population has a formal bank account. Even if all these people had loan outstandings equivalent to their annual income, these loans would represent only 1% of total Kenyan banking assets.

- **Interest rate risk** is the risk that change in interest rates will cause a change in an investment's value or in net interest income – due to relative change in interest rates on liabilities (e.g., deposits held) and assets (e.g., loans made). From a provider perspective, impact includes decreased net interest income, or decreased investment value[27]. From a consumer perspective, changes in interest rates may change the payment due on a loan or alter the interest received on a savings account (relative to inflation). From the perspective of the system at large, understanding how interest rate changes will affect bank lending provides an important input to ensuring monetary stability. Non-bank providers of digital payments and associated adjacencies will increasingly need to manage interest rate risk. We note that the contribution to interest rate risk from products and services used by very poor populations likely will be minimal; credit extended to the very poor will be small as a fraction of total country banking assets, and will mainly be in the form of short duration, fixed-rate (or fee-based) loans.

Counterparty credit risk

Counterparty credit risk is the risk that the counterparty to a transaction defaults before the final settlement of the transaction's cash flows. Counterparty credit risk can arise when one provider in the value chain advances credit to another to facilitate smooth interactions with customers. This can occur both in a slightly enhanced form of digital payments or in issuing loans. (Counterparty credit risk also arises through the purchase and sale of securities, but such activities are not relevant to this paper).

In digital payments, a provider might extend credit to agents or to merchants. To help an agent providing cash-in-cash-out services in a time of high consumer demand, a provider might extend that agent short-term credit, in the form of either cash or e-money. A provider might immediately credit the account of a merchant accepting payment via e-money, before final settlement, thereby accepting the risk that the payment would not settle.

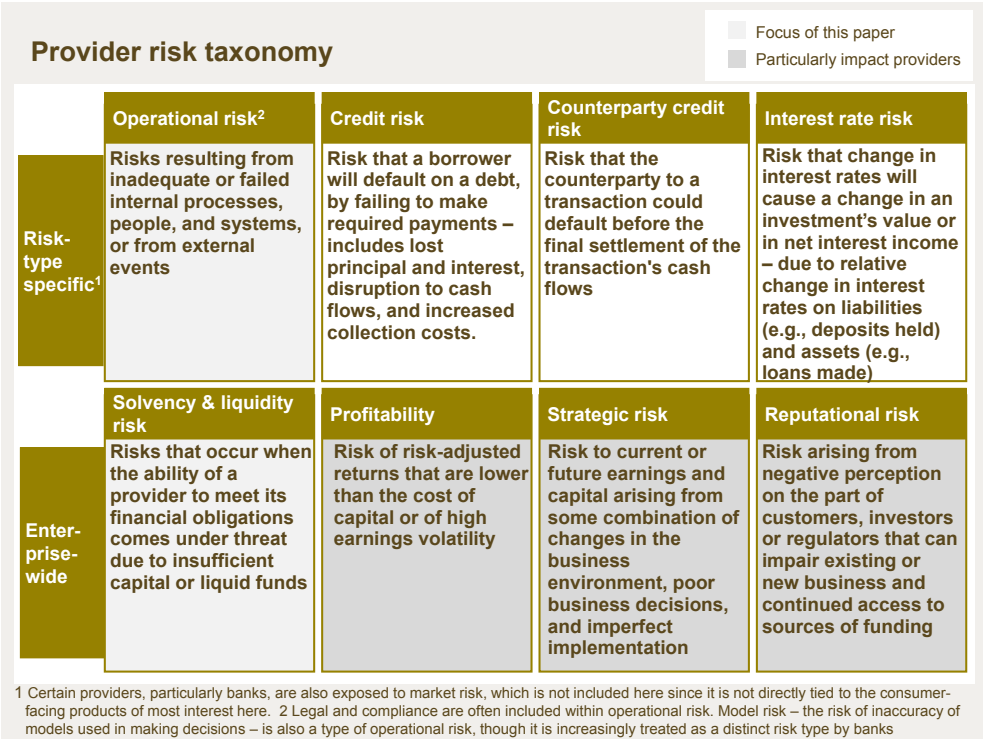
Lending provides another example, not directly related to digital payments. In issuing loans, counterparty credit risk can arise when one provider in the value chain issues loans directly to consumers, on behalf of a second provider – often a bank – who has agreed to buy the loan. For example, to facilitate smooth interactions with consumers, a bank might fund a loan issued by an agent before the final closing loan documents exist, are checked, and transferred to the bank. The bank thus runs the risk that the agent does not transfer the documents, or that the documents are incorrect and that the agent is unable to pay for any difference.

[27] Decreased investment value can lead to losses in two ways. First, the provider must carry a loss on its books if its accounting standards require it to value its assets according to current market values (i.e., the price at which the provider could sell the investment). Second, the provider realizes a loss if it is forced to sell the investment, for example to obtain liquid cash.

Risk types impacting providers

Three additional types of risk particularly impact providers, both those only involved in digital payments, as well as those who also offer credit-linked products. These are risks to profitability, strategic risks, and reputational risk. Exhibit 12 provides a taxonomy of risk types particularly applicable to providers, including those we have previously discussed in this report.

EXHIBIT 12



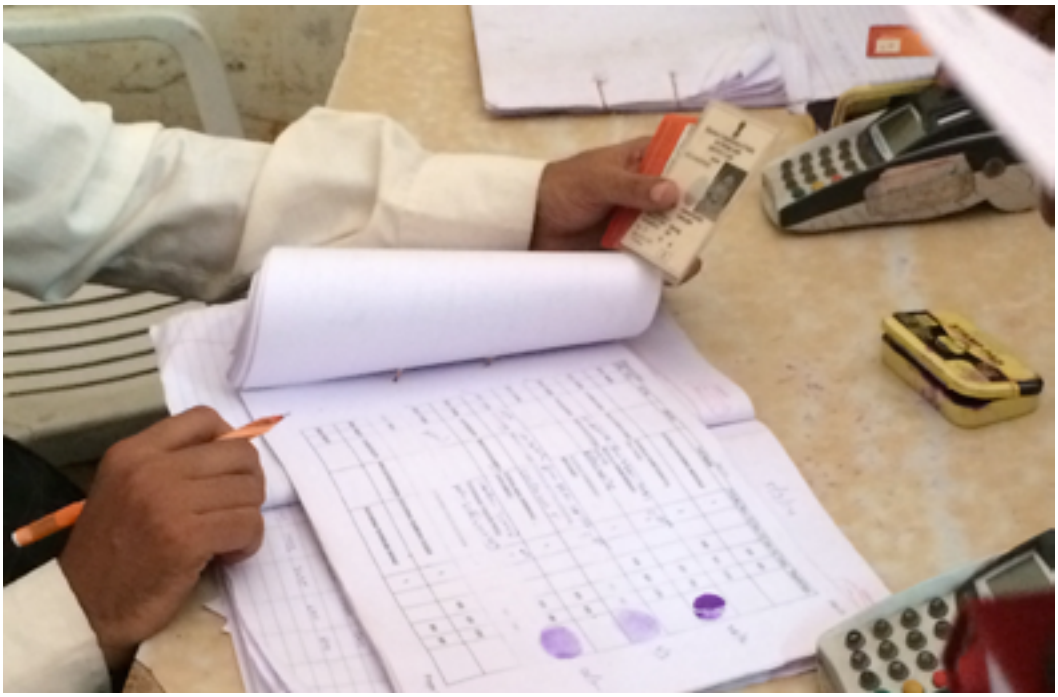
1 Certain providers, particularly banks, are also exposed to market risk, which is not included here since it is not directly tied to the consumer-facing products of most interest here. 2 Legal and compliance are often included within operational risk. Model risk – the risk of inaccuracy of models used in making decisions – is also a type of operational risk, though it is increasingly treated as a distinct risk type by banks

Since profitability, strategic, and reputational risk are not a primary focus of this report, we do not discuss in detail an approach for risk monitoring, measurement, and management. However, we do explain each, and provide some high-level metrics that a provider might use to assess the level of these risks.

- **Risks to profitability** include situations where risk-adjusted returns are lower than the cost of capital and the risk of high earnings volatility. One of the main challenges of providing affordable payment services to the poor is represented by the very thin margins provided by low-value transactions. Providers are particularly exposed to earnings volatility that can result from rapid changes in consumer demand, increased competition, heavier compliance costs, or taxation, particularly of digital money transactions. Even small variations may make a business unprofitable. Associated metrics a provider might monitor include risk-adjusted return on capital, net interest margin, losses or capital ratio under a hypothetical stress scenario, earnings at risk, or volatility of net income.

- **Strategic risk** is the risk to current or future earnings and capital arising from some combination of changes in the business environment, poor business decisions, and imperfect implementation. In providing financial services to the poor, providers may need to accept losses in the short term, for the promise of future profits. As a result, strategic decisions, and the associated risk, will be particularly important since they may determine if the business is viable. For instance, poor strategic decisions may result in insufficient investments in marketing activities, leaving consumer awareness and product uptake low in a particular country. Associated metrics a provider might monitor include capital allocated to non-core business, exposure to non-core relationships, or market share by business.

- **Reputational risk** is the risk that negative perceptions by customers, investors or regulators impair business and continued access to sources of funding. Reputational risk can arise from operational issues or other events. For instance, in digital payments, agent misbehavior, poor customer care, or unreliable technology can all compromise customers' confidence in the service provider, and put their loyalty at risk. Associated metrics a provider might monitor include traditional press coverage, customer satisfaction scores, customer complaints, and reputation ratings from third-party providers.



Implications for financial inclusion

Digital financial services beyond payments are exposed to multiple risk types beyond operational, solvency, and liquidity risks. All of these require serious attention from both regulators and providers, particularly if they are to succeed in increasing financial inclusion. Regulators will need to develop a broad understanding of the risk profile of all providers in the digital payments value chain. They will have to ensure that rules and regulations support development of sustainable and scalable business operations, provide legal certainty, and stimulate investment and innovation. They must work to ensure that profitability is within reach, with low volatility, in order to attract providers who will develop long-term strategies.

Providers of digital payments services, particularly non-banks, will need to realize that today's increasing competition and fast innovations leave them no space for complacency. They must ensure that they understand the needs and situations faced by the unbanked, if they are to develop a value proposition customized to these new customers that can become profitable over time.

Newcomers to payments such as mobile network operators will need to realize that storing and transferring money bears little resemblance to their core business of selling airtime. The new strategic and reputational risks they are assuming are different from those to which they are accustomed.

Conclusion

There is widespread agreement by regulators and consumer advocates about the need to provide stability, integrity, and protection in a new environment of digital payments particularly involving services for the poor. All stakeholders must also acknowledge the need for providers to earn adequate returns, and to have reasonable certainty of those returns in an evolving market.

To support these goals, this analysis has provided an organizing framework and tools to identify, discuss, and manage risk:

- The organizing framework, including three main categories of risk – Operational, Solvency and Liquidity, and Other – as measured across three constituencies – providers, consumers, and the financial system at large
- An approach to operational risk management based on identifying key process breakpoints, using these breakpoints to quantify the size of operational risks, then setting priorities for managing these risks
- An approach to managing solvency and liquidity risk based on a value chain analysis to identify institutional roles

Our analysis also makes an effort to identify the most important risks in this emerging ecosystem – risks that will require the most attention from regulators and providers.

Because the profit margins to provide payment services to the 2.5 billion unbanked will be razor thin, providers must make sure their systems and risk management are right-sized. A risk-based approach to business is therefore required, as it is in regulation.

Moreover, if financial inclusion at a country level means more people are included than excluded, there will be a lot more "noise in the system" about stability, integrity, and protection than there is today. Regulators will need to have sensitivity to and capacity for this noise.

The good news from this work is that digital payments and agent banking do not add much real solvency and liquidity risk to the overall system. Operational risk will simply need to be managed across a wider set of providers.

This report also provides some comfort to all constituents that the risks in an emerging digital payments environment are quite similar to those risks we already understand and manage in more traditional banking, albeit across new players and with new consumer segments and distribution channels. That said, there are important best practices in risk management that should be employed in this new arena. They include:

- Both regulators and providers should ensure there is a comprehensive risk framework in place across the digital payments value chain.
- Each provider in digital payments should think through and understand its own risk appetite, and use that guidance in entering new and different businesses.
- Providers will need to develop contingency plans and business continuity procedures to manage risk efficiently, and to allow customer access to funds.
- Providers also need to establish minimum capital and liquidity reserves that match their business needs. They need to reassess these regularly, as those needs change.
- Regulators and providers will need to assess what kind of deposit insurance is needed to make digital stored-value accounts as safe as regular deposits.
- Regulators must be clear about non-bank obligations involving consumers' deposits if a solvency or liquidity event occurs.

We hope that the insights and tools provided in this report will help all players chart a viable, strong, and sustainable path forward to increase financial inclusion – and help millions of poor people see significant improvement in their lives.

Acknowledgments

In writing this report we have capitalized on the significant and important work relevant to risk in digital payments and banking. First, we have drawn on the significant body of work on risk in traditional banking (see for instance the Basel Committee for Banking Supervision analysis and guidelines on operational risk). We also have examined specialized publications, focused on risk in digital payments that particularly target poor users. Examples from a list of many include the comprehensive *"Mobile Financial Services Risk Matrix"* developed by USAID, Booz Allen Hamilton and the Kenyan School of Monetary Studies and the University of New South Wales' knowledge product, *"Trusts Law Protections for E-money Customers"*.

The analysis and conclusions in this report also benefited from the generous contributions of colleagues and friends too numerous to fully acknowledge. Without these contributions, we could not have completed this work. There are, how¬ever, three groups of people we would like to acknowledge with special gratitude.

First, our external reviewers comprised executives, regulators, and thought leaders from a range of institutions and background. We are grateful for their special counsel and valued perspectives. They challenged our thinking and gave us insights that will help stakeholders take action.

Secondly, we want to thank the many people we visited in India and Kenya as well as the others we interviewed. In these countries, we received invaluable insight and support from central bankers, banking executives, telecommunications leaders, start-up entrepreneurs, leading academics, and many more. We are grateful for all of their time and contributions. Lastly, we want to acknowledge McKinsey & Company for providing a team of dedicated analysts and experts from their offices around the world. They partnered with the Gates Foundation to synthesize all of the information we gathered, to structure the findings, and formulate our assessment.

Glossary

Term	Definition
Account	An arrangement by which an organization accepts a customer's financial assets and holds them on behalf of the customer at his or her discretion.
ACTA	A framework including the four core elements of all payments systems: Account, Cash-in-cash-out, Transactions, and Adjacencies.
Adjacencies	Revenue-earning opportunities that are tied to the basic payment system but not explicitly core to any payment activity (includes financial adjacencies and non-financial adjacencies).
Agent	An authorized person or entity that handles financial account opening and/or transactions on behalf of another entity. The other entity may be a bank or, in some countries, a non-bank provider of digital money services. Cash-in-cash-out is a common service provided by agents.
Agent banking	Agent banking is the provision of financial services to customers by a third party (agent) on behalf of a licensed deposit taking financial institution and/or digital money operator (principal).
Agent network manager	Banks and other financial service providers sometimes use agent networks instead of traditional branches to reach more customers at a lower cost. Agent networks may comprise an established distribution network, such as post offices or retail chains, or be built from independent, small-scale traders and other retailers.
Aggregator	A person or business that is responsible for recruiting new mobile money agents.
Anti-money laundering (AML)	Legal controls that require financial institutions to prevent, track and report suspicious transactions as related to money laundering.
ATM, payment transaction channel	A payment channel referring to payments initiated at an ATM; only applicable to credit transfers. Note that ATMs are also a significant channel for CICO.
Bank	A financial intermediary that both accepts deposits and engages in lending activities, in so doing linking customers with capital deficits to those with capital surpluses. The exact definition of a bank varies from country to country.

Basel Committee for Banking Supervision	Committee of banking supervisory authorities established by the central bank governors of the Group of Ten countries in 1974. It is the primary global standard-setter for the prudential regulation of banks and provides a forum for cooperation on banking supervisory matters. Its mandate is to strengthen the regulation, supervision and practices of banks worldwide with the purpose of enhancing financial stability
Basel Accords (Basel I, II and III)	Recommendations on banking laws and regulations issued by the Basel Committee on Banking Supervision. Basel III, the most recent, provides a global, voluntary regulatory standard on bank capital adequacy, stress testing and market liquidity risk.
Branch, channel	A bank's main physical retail location, where customers can interact directly with bank employees to open an account, make transactions, withdraw and deposit cash, resolve inquiries and contract other financial services.
Breakpoint	Points in a process at which the likelihood of a breakdown leading to loss is highest, or where a breakdown would lead to a high loss.
Business correspondent (BC)	Individuals or firms designated by a provider to accept and distribute cash on their behalf, operating on a commission. Individual BCs either pick a base from which they provide service on a pre-set schedule, or they can be 'roaming', in which case they traverse a pre-determined route and schedule.
Call center, channel	A payment channel referring to payments initiated via a phone call (e.g., paying for a bill or purchase by dictating card information to a call center agent, who will enter it into a payment gateway).
Cash recycling	Using cash received from one customer to distribute cash to another.
Cash-in-cash-out (CICO)	Providing access points at which consumers can deposit and withdraw cash to and from their accounts.
Channel	The interface through which a transaction or CICO is initiated; includes POS, digital, mail, call center, branch, ATM.
Clearing & Settlement	Activities related to adjusting account balances resulting from a payment transaction, including authorizing payment across counterparties and transferring funds between payer's & payee's financial institutions.

Consumer deposits	A sum of money placed or kept in a bank account, usually to gain interest.
Cost to remediate	Occurs when providers or consumers bear a cost to address an issue when a part of the system does not function, or there is a direct loss.
Counterparty credit risk	Risk that the counterparty to a transaction defaults before the final settlement of the transaction's cash flows.
Credit card	A payment instrument initiated by a card linked to a credit account, where the capture of card and transaction information initiates a 'pull' transaction from the payer's credit account to the payee's account. The user pays the balance on the credit account on a regular basis, most often through a different payment instrument (e.g., direct debit). Commonly used for POS consumer purchases.
Credit risk	Risk that a borrower will default on a debt, by failing to make required payment.
Credit transfer	A payment instrument where a payer 'pushes' a transaction to a payee by entering the payee's account information (usually two numbers, one identifying the bank and another identifying the account) and transaction information. Commonly used for salary payments and consumer-to-consumer payments.
Current account	An account that allows users to store money, make payments, receive payments and, in some cases, earn interest on stored balances.
Deposit holder	Intuition that takes customer deposits into safe keeping
Depository institution	A financial institution (such as a savings bank, commercial bank, savings and loan associations, or credit unions) that is legally allowed to accept monetary deposits from consumers.
Digital payment system	A way of paying for a goods or services electronically, instead of using cash or a check, in person or by mail.
Digital transaction platform	A computer system that connects the financial service providers (banks, digital money providers), in-country payment market infrastructures (real time gross settlement systems, automated clearinghouses) and merchants to the users. The platform implements inter-operability between the players, so that - from the user perspective - all transactions can be carried out between bank accounts and digital money wallets.

Digital, channel	A payment channel referring to transactions initiated digitally; includes transactions initiated by mobile phone, online (e.g., online shopping) and batch transactions initiated through a file upload (e.g., some salary payments).
Direct debit	A payment instrument where a payer pre-authorizes access to his or her account and the payee 'pulls' the transaction from the payer's account. Direct debits are a relatively sophisticated instrument often used for repeating bill payments, requiring strict control, and not commonly used in emerging markets.
Direct loss	When money in an account is misappropriated or a cash-in, cash-out, or transaction flow is misdirected (e.g., to the wrong account through error or fraud).
E-money	Short for "electronic money," this is stored value held in the accounts of users, agents, and the provider of the mobile money service.
E-money issuer	An entity that distributes 'Electronic money' (a monetary value stored on an electronic carrier or remotely in a central accounting system).
Financial adjacencies	Revenue captured from offering financial services linked to a current account (e.g., credit card, life insurance, overdraft line).
Interest rate risk	Risk that change in interest rates will cause a change in an investment's value or in net interest income – due to relative change in interest rates on liabilities (e.g., deposits held) and assets (e.g., loans made).
Issuer	Financial entity that issues a payment instrument (i.e., the payer's bank).
Liquidity risk	Occurs when an institution does not have sufficient liquid assets (e.g., cash) cash to meet its debts.
Mobile money	The definition of mobile money varies across the industry. Most generally, it is a service in which a mobile phone is used to access financial services.
Non-financial adjacencies	Indirect profit pools that a stakeholder may be able to capture through a digital payment system. These include reducing churn on another product/ service, cross-selling and capturing value from the transaction information collected, among others.
Operational risk	Risk resulting from inadequate or failed internal processes, people, and systems, or from external events.

Payments service provider (PSP)	Third party that helps process payments. Most commonly PSPs help merchants accept or facilitate payments, often offering services in addition to processes transactions, which can include fraud protection.
Payment system	A system consisting of instruments, banking procedures, and, typically, interbank funds transfer systems that ensure the circulation of money.
Point-of-sale (POS)	The location where a retail transaction is completed and payment is made.
Point-of-sale (POS) terminal	An electronic device that reads a payee's payment information (e.g., debit card) and transmits the transaction and payment information to a payments provider over a network. POS terminals are most commonly at a merchant's checkout counter, but can be mobile as well.
Point-of-sale (POS), channel	A payment channel referring to payments initiated at a merchant POS (e.g., paying with a debit card at a card terminal).
Processing	A series of actions performed to complete payment transactions, typically involving high volumes of requests for authorization, clearing, settlement, and reporting.
Providers	Individuals who provide specialized service, including but not restricted to lawyers, accountants and management consultants
Reputational risk	The risk that negative perception on the part of customers, investors or regulators impair existing or new business and continued access to sources of funding.
Risk likelihood	The probability value of a specific risk occurring in a given time period (e.g., one year).
Risk severity	The estimated impact of a risk's occurrence.
Risk size	The product of risk severity and risk likelihood, indicating the average losses from that risk over a given time period (e.g., one year)
Risks to profitability	Situations where risk-adjusted returns are lower than the cost of capital and the risk of high earnings volatility.
Solvency risk	Occurs when an institution cannot fully meet its debts as they come due, even by selling all its assets.

Standard-setting bodies (SSBs)	Any organization whose primary activities are developing, coordinating, promulgating, revising, amending, reissuing, interpreting, or otherwise producing technical standards that are intended to address the needs of some relatively wide base of affected adopters.
Strategic risks	Risk to current or future earnings and capital arising from some combination of changes in the business environment, poor business decisions, and imperfect implementation.
Technology failure	Includes issues such as a transaction delay due to poor cell phone signal, back-end issues with the core technology, an agent's phone or terminal not working, failure of the system to send a text confirming a transaction, or lack of signal due to towers being down post-earthquake.
Technology service provider (TSP)	In the context of digital payments, TSPs help provide the technology used in processing payments. Depending on market and specific circumstance, the TSP and PSP may be either the same or a different entity.
Telecom channel provider	An organization that provides either a physical transmission medium such as a wire, or to a logical connection over a multiplexed medium such as a radio channel.
Transaction	Direct transfers of funds between accounts (e.g., debit and credit card payments, credit transfers, direct debits, and mobile money payments).

Reading list

Key reads

NON-TECHNICAL BOOKS ILLUSTRATING THE NEED BY POOR PEOPLE FOR FINANCIAL SERVICES

Portfolios of the Poor, Collins, Morduch, Rutherford, and Ruthven (2009). Based on the financial diaries project data, this book describes and quantifies the financial lives of poor families in South Africa, India, and Bangladesh.

The Poor and Their Money, Rutherford (2001). This is an essay, written by Stuart Rutherford, and based on his long experience working with the poor. It is a foundational piece describing different reasons poor people need financial services, and how they get by using informal arrangements.

A SELECTION FROM THE IMPACT LITERATURE

Mobile Money: The Economics of M-PESA, Jack and Suri (2011). This is a paper published by the National Bureau of Economic Research, with key data on the diffusion and usage patterns of M-PESA in Kenya. It is based on a study funded by FSP through our grantee the Consortium on Financial Systems and Poverty (at the University of Chicago). The paper contains a preliminary version of the impact results that Jack and Suri have found using this data. They plan to release a more formal working paper soon.

A Penny Saved: How Do Savings Accounts Help the Poor?, Kendall (2010). This paper reviews the experimental evidence (from both randomized controlled trials and natural experiments) regarding the impact of improved access to savings. It finds a limited but growing body of research that supports the claim that savings accounts improve welfare.

ACADEMIC PIECES THAT EXPLORE FINANCE FOR THE POOR

How Gambians Save, Shipton (1990). This is a good explication of the different ways in which poor people save through the informal mechanism available to them.

Saving in Developing Countries, Deaton (1989), a discussion and model of factors that make poor people's financial needs differ from those of rich people (and thus why our intuition might fail us in thinking about the poor).

Income and Consumption Smoothing, Morduch (1995). In this piece, Jonathan Morduch argues that because people lack financial tools to smooth consumption, they then make choices that smooth their income, which can reduce their productivity.

Income Risk and Coping, Dercon (2002). This looks at various indigenous methods for smoothing consumption in the face of emergencies, disasters, etc. without using formal finance.

Explorations of specific topics

ACCESS TO FINANCIAL TOOLS

Household Financial Behavior, Oliver Wyman (2008) consultant report with lots of relevant data.

Household Saving in Developing Countries, Morduch (2008). Written at FSP's request, this framing note provides a list of academic and non-academic papers on the demand for, and impact of, savings mechanisms in developing countries.

Financial Access 2009 and 2010. CGAP provide data and mapping of the high-level financial inclusion picture around the world.

Access to Finance: Chapter 2, Handbook of Development Economics, Karlan and Morduch (2009). An academic review of recent innovations that are improving the quantity and quality of financial access.

A Digital Pathway to Financial Inclusion, Radcliffe and Voorhies (2012) This paper discusses the cash-digital divide that creates inequities in the financial lives of the poor and presents evidence that connecting poor people to an integrated digital financial system may generate sizeable welfare benefits.

Savings as Forward Payments, Mayer and Mas (2012) This paper presents a new framework that allows people to manage their needs for diverse payment, cash flow management, and commitment savings simply and intuitively, from a single account.

PAYMENT SYSTEMS AND DEVELOPMENT

Fighting poverty profitably: Transforming the economics of payments to build sustainable, inclusive financial systems, Bill and Melinda Gates Foundation (2013). This work provides an extensive analysis of the economics of payment systems around the world and concludes that the costs of these systems could be significantly reduced, and they could be made more efficient, sustainable and accessible to poorer consumers, while at the same time boosting provider revenues.

Innovations in retail payments, Committee on Payment and Settlement Systems, BIS, (2012). This report, first provides an overview of innovative retail payment activities over the past decade across the world.

Payment Systems Worldwide: a Snapshot. Outcomes of the Global Payment Systems Survey 2010, World Bank, (2010). This work presents the results of the second survey of national central banks that collecting information on the status of national payment and securities settlement systems worldwide.

Measuring Payment System Development, World Bank, Financial Infrastructure Series, Cirasino and Garcia (2009). This work aims to provide central banks in developing countries with a tool to monitor developments in their payment systems and to compare them with those in other countries

Retail Payment Systems to Support Financial Access: Infrastructure and Policy, Cirasino, Garcia, Tresoldi, Vangelisti, and Zaccagino (2007). This World Bank publication presents lessons from the European experience and from the analysis of current trends in emerging economies with the aim of proposing an agenda for reform in the retail payment sector of developing countries.

A glossary of terms used in payment and settlement systems, Committee on Payment and Settlement Systems, BIS, (2001). A reference document for the standard terms used in connection with payment and settlement systems. It combines various glossaries appended to earlier reports by the CPSS and the European Central Bank (ECB).

REGULATION

Non-Bank E-Money Issuers: Regulatory Approaches to Protecting Customer Funds, Tarazi and Breloff (CGAP) (2010). The success of Kenya's M-PESA has raised the question of how most effectively to regulate nonbanks—most notably mobile network operators (MNOs)—who contract directly with customers to issue electronic value against receipt of equal funds ("e-money").

Regulating New Banking Models that Can Bring Financial Services to All, Alexandre, Mas, and Radcliffe (2010). This work highlights five areas where sharpened regulatory analysis could help strike a better balance between maximizing the opportunities of these models and containing risks.

On Harnessing the Potential of Financial Inclusion, Bank for International Settlements (BIS) Working Paper, Dittus and Klein (2011). The paper describes one commercially viable initiative in more detail, M-PESA in Kenya, and analyses in detail the transactions involved.

Financial Inclusion and Law Enforcement: United by a Common Enemy, Alexandre and Mas (2011). Discusses the conflict between the goals of financial inclusion and those of law enforcement.

Enabling mobile money transfer: The Central Bank of Kenya's treatment of M-PESA, Alliance for Financial Inclusion (2010). This case study examines the process that the Central Bank of Kenya (CBK) used to assess risk of the mobile banking service, M-PESA.

ADDITIONAL INFORMATION, AND BLOGS

Financial Services for the Poor Strategy, Gates Foundation. Financial Services for the Poor program aims to play a catalytic role in broadening the reach of digital payment systems, particularly in poor and rural areas, and expanding the range of services available on these platforms.

> http://www.gatesfoundation.org/What-We-Do/Global-Development/Financial-Services-for-the-Poor

FSP external site and Global Savings Forum page. Global Savings forum is part of the Financial Services for the Poor initiative of The Bill & Melinda Gates Foundation.

Findex Global Database This is a project funded by the Bill & Melinda Gates Foundation to measure how people in 148 countries - including the poor, women, and rural residents - save, borrow, make payments and manage risk.

> http://econ.worldbank.org/wbsite/external/extdec/extresearch/extprograms/extfinres/extglobalfin/0,,contentmdk:23147627~pagepk:64168176~pipk:64168140~thesitepk:8519639,00.html

Mobile Money for the Unbanked. This blog was created by GSMA in 2008 to accelerate the availability of mobile money services to the unbanked and those living on less than US$2 per day. It works with mobile operators and the financial services industry to deliver affordable, safe, and convenient financial services to millions of previously unbanked customers.

> http://www.gsma.com/mobilefordevelopment/programmes/mobile-money-for-the-unbanked/mmu-blog

The CGAP Technology Blog. CGAP develops innovative solutions for financial inclusion through practical research and active engagement with financial service providers, policy makers, and funders. This blog has many pieces on branchless banking and mobile money.

http://www.cgap.org/blog

The NextBillion Blog. NextBillion.net is a Web site and blog bringing together the community of business leaders, social entrepreneurs, NGOs, policy makers and academics who want to explore the connection between development and enterprise.

http://www.nextbillion.net/blogfeed.aspx

Mobile Money Deployment Tracker. This site monitors the number of live and planned mobile money services for the unbanked.

http://www.gsma.com/mobilefordevelopment/programmes/mobile-money-for-the-unbanked/tracker

Safaricom: M-PESA statistics and presentations.

http://www.safaricom.co.ke/personal/m-pesa/m-pesa-resource-centre

Sources

DATABASES

CIA World Fact Book

Findex Global Database

International Telecommunication Union - World Telecommunication/ICT Development database

Kenya Statistical Bureau

McKinsey Global Payments Map, 2013 edition

Nigeria National Bureau of Statistics

The Economist Intelligence Unit: Country Data - Annual Time Series and Market Indicators

World Bank (World Development Indicators database, Data Bank)

PRINT & ONLINE

AFI *(Trust Law Protections for E-Money Customers,* other publications, website)

Bangladesh Bank

Bank Indonesia

Bank for International Settlements (Committee on Payments & Settlement Services; Basel Committee on Banking Supervision)

Bank of Uganda

Bankable Frontier Associates - "Research on the scope of cash versus non-cash payment methods in Kenya"

Bill & Melinda Gates Foundation – *Fighting poverty profitably: transforming the economics of payments to build sustainable, inclusive financial systems*

Bridges to Cash: The Retail End of M-PESA

Central Bank of Kenya (annual reports, statistical bulletins, payments data and website)

Central Bank of Nigeria (annual reports, statistical bulletins, payments data, and website)

CGAP (blog, publications, website)

European Central Bank

European Commission (including Directive on Payment Services, E-Money Directive)

EFInA *(Scoping Study on Payment Systems in Nigeria, Access to Financial Services in Nigeria 2010,* among others)

European Financial Inclusion Network

Federal Reserve

FATF website

FDIC

Finalta

Financial Services 360

Gartner

Global Association of Risk Professionals – “Operational Risk Management”

Grameen

GSMA (Mobile Money for the Unbanked website and associated publications)

Hindu Business Line

IFC

IMF

InterMedia – Financial Inclusion Tracker Surveys Project report

International Telecommunication Union - World Telecommunication/
ICT Development Report

Kenyan Bankers Association

Lafferty World Cards Nigeria 2009

National Council for Law Reporting, Kenya

National Payments Corporation of India

Navigant

New Cash Policy (Cashless Lagos Stakeholder Implementation Session Oct 2011,
Stakeholder Engagement Presentation Oct 2011)

Nigeria Inter-Bank Settlement System Plc

Nigeria National Bureau of Statistics

Norges BankPopulation Reference Bureau (Kenya)

OCC (Comptrolers Handbook)

Reserve Bank of India (Payment System Vision Document – 2012-15, payments data,
website)

Safaricom (Annual Reports and website)

South African Reserve Bank

The Little Data Book on Financial Inclusion 2012

Unique Identification Authority of India

UNSW (research gateway website)

USAID (Mobile Financial Services Risk Matrixwith Booz Allen Hamilton and the Kenyan
School of Monetary Studies)

Washington Journal of Law

WDI

World Bank (World Development Indicators report and others)

WMM: Global Insights

OTHER

Bank and company websites

Authors

Jason Lamb
Deputy Director, Financial Services for the Poor
Bill & Melinda Gates Foundation

Jason Lamb is the Deputy Director, Global Partnerships on the Financial Services for the Poor initiative at the Bill & Melinda Gates Foundation.

Jason brings over 20 years of financial services and development experience to his role, spending several years at Washington Mutual in Seattle; McKinsey & Company in Central and Eastern Europe, Africa and North America; and the US Department of Agriculture Economic Research Service in Washington, DC. He was a founding member of the McKinsey Budapest office. Jason holds a BA in Economics and History from the University of California, Davis and an MBA from the Ross School of Business at the University of Michigan.

Sacha Polverini
Senior Program Officer, Financial Services for the Poor
Bill & Melinda Gates Foundation

Sacha Polverini joined the Bill & Melinda Gates Foundation's Financial Services for the Poor (FSP) team in December 2012 as Senior Program Officer - Regulation and Policy. In this capacity, Sacha represents FSP and the foundation on policy & regulatory related aspects with a variety of stakeholders including governments, SSBs, global agencies, grantee organizations and donors.

Sacha joined the foundation from Brussels where he lived and worked for almost 20 years representing the interests of the financial services industry before both EU and national policy and decision makers. Sacha worked – inter alia - at Barclays Bank PLC as Group Director for EU Public Policy and at Genworth Financial Mortgage Insurance (formerly GE Mortgage Insurance) as Managing Director of Government and Regulatory Affairs Europe. A graduate of University L.U.I.S.S Guido Carli in Rome, Sacha holds a Master's degree in European Political Studies from the Universite' Libre de Bruxelles. In addition he has completed the post-graduate management program at Solvay Business School, Ecole de Commerce de Solvay, Brussels.