

**2<sup>nd</sup> GPI Conference on Standard-Setting Bodies and Financial Inclusion:  
Standard Setting in the Changing Landscape of Digital Financial Inclusion**

**30 and 31 October 2014**

**Issues Paper  
Digital Financial Inclusion and  
the Implications for Customers, Regulators, Supervisors  
and Standard-Setting Bodies**

**INTRODUCTION**

*“Universal access to financial services is within reach—thanks to new technologies, transformative business models and ambitious reforms .... As early as 2020, such instruments as e-money accounts, along with debit cards and low-cost regular bank accounts, can significantly increase financial access for those who are now excluded.”* —World Bank Group President Jim Yong Kim, 11 October 2013, in a dialogue with Her Majesty Queen Máxima of the Netherlands—the United Nations Secretary General’s Special Advocate for Inclusive Finance for Development and the Honorary Patron of the G20 Global Partnership for Financial Inclusion

World Bank President Jim Kim’s optimism about financial inclusion efforts and the pivotal role of digital financial services in achieving universal access is shared not only by Her Majesty Queen Máxima, but also by the G20 Leaders, who have explicitly recognized the role of the global standard-setting bodies (SSBs) in achieving this vision. G20 and SSB members are among the more than 50 countries committed to taking up the challenge both on the home front and globally. Many contribute to the Global Partnership for Financial Inclusion (GPI) workstream acting on the call of the G20 Leaders to engage on financial inclusion with the SSBs<sup>1</sup> and to explore “targeted actions to ... harness emerging mechanisms such as electronic payments and mobile technology that can significantly improve access.”<sup>2</sup>

With the prospect of reaching billions of new customers, banks and a widening array of non-banks have begun to offer digital financial services for financially excluded and underserved populations, building on the digital approaches that have been used for years to improve access channels for those already served by the formal financial sector. Digital financial services—including those involving the use of mobile phones—have now been launched in more than 80

---

<sup>1</sup> At their September 2013 summit, the G20 Leaders endorsed a call to the SSBs to “(i) continue their progress to integrate consideration of financial inclusion in their work, consistent with their respective mandates; (ii) to participate in relevant activities of the GPI and engage GPI representation in relevant activities of the SSBs; and (iii) to give attention to emerging issues in financial inclusion of relevance to multiple SSBs.”

<sup>2</sup> G20’s St. Petersburg Development Outlook at [https://www.g20.org/sites/default/files/g20\\_resources/library/Saint%20Petersburg%20Development%20Outlook\\_0.pdf](https://www.g20.org/sites/default/files/g20_resources/library/Saint%20Petersburg%20Development%20Outlook_0.pdf).

countries,<sup>3</sup> with some reaching significant scale. As a result, millions of formerly excluded and underserved poor customers are moving from exclusively cash-based transactions to formal financial services—payments, transfers, savings, credit, insurance, and even securities—using a mobile phone or other digital technology to access these services. And the picture is continuing to shift rapidly with the emergence of ever more new technologies.<sup>4</sup>

Alongside the benefits of digital financial services there are potential risks. While the years of experience with digital financial services for the banked population provide guideposts for those navigating the digital financial inclusion space—both in the design of new products and services and the means by which to regulate and supervise them—there are particular risks introduced by these new services. These resulting from, among other things, the introduction of non-financial firms deploying new technologies; new contractual relationships between financial institutions and third parties, including the use of agent networks and other outsourcing arrangements; the different regulatory treatment of deposit-like products (compared to deposits); unknown and as-yet unpredictable costs to inexperienced and vulnerable consumers; and the use of new kinds of data—and new uses of data—introducing both new privacy and data security issues.

The exploration of these topics—both the potential benefits to financially excluded and underserved populations flowing from digital financial inclusion and the potential risks—will be the work of the SSBs and other global bodies participating in the 2nd GPMI Conference on Standard-Setting Bodies and Financial Inclusion: Standard Setting in the Changing Landscape of Digital Financial Inclusion. The conference, hosted by the Financial Stability Institute, will include participants from six SSBs—the Basel Committee on Banking Supervision (BCBS), the Committee on Payments and Market Infrastructures (CPMI),<sup>5</sup> the Financial Action Task Force (FATF), the International Association of Deposit Insurers (IADI), the International Association of Insurance Supervisors (IAIS), and the International Organization of Securities Commissions (IOSCO)—as well as members and Implementing Partners of the GPMI. This Issues Paper, key points from

---

<sup>3</sup> This figure is based on the data on *mobile* financial services only as there is no central data source for countries with non-mobile digital financial services for the financially excluded and underserved. As of 2013, mobile money accounts had been launched in 84 countries (GSMA 2014). (A mobile money account as tracked by GSMA, which is distinct from a traditional bank account, enables a mobile phone customer to place funds, make payments and transfers, and withdraw funds.) The number of active mobile money accounts as of June 2013 exceeded 60 million. *Id.*

<sup>4</sup> In September 2014, for example, Apple launched Apple Pay, a contactless payment system that may have superior security to other similar systems (Google, eBay, Square) with its use of Apple’s fingerprint technology, a secure chip, and a system that requires a one-time security code (WSJ, 10 September 2014). Some have questioned the novelty of Apple Pay, citing that the Japanese company NTT Docomo pioneered “Osaifu-Keitai” or “mobile wallet” a decade ago (<http://blogs.wsj.com/japanrealtime/2014/09/11/long-before-apple-pay-japan-had-mobile-wallet/>). See also the Ripple protocol, a new “open-sourced payment protocol that enables free and instant payments with no chargebacks and in any currency,” including loyalty points (<https://www.ripplelabs.com/>). And see “Taking the Mobile out of Mobile Money” (20 August 2014, <http://mondato.com/blog/taking-the-mobile-out/>).

<sup>5</sup> Formerly the Committee on Payment and Settlement Systems, widely referred to by its acronym: CPSS.

which are summarized in Box 1, frames the subject matter to be discussed in the opening conference session and throughout the event.

### **Box 1: Digital Financial Inclusion—Summary of Key Points**

#### **What Is Meant by “Digital Financial Inclusion”? (Part I)**

“Digital financial inclusion” refers broadly to the use of digital financial services to advance financial inclusion. As specifically addressed in this Issues Paper, digital financial inclusion involves the deployment of digital means to reach financially excluded and underserved populations with a range of formal financial services suited to their needs, delivered responsibly at a cost affordable to the customer and sustainable for the providers. The essential components are as follows:

**Digital transactional platform.** A digital transactional platform enables a customer to make or receive payments and transfers and to store value electronically through the use of a device that transmits and receives transaction data and connects—directly or through the use of a digital communication channel—to a bank or non-bank permitted to store electronic value.

**Device.** The device used by the customer can be digital such as a mobile phone that is a means of transmitting data and information or an instrument such as a payment card that connects to a digital device such as a point-of-sale (POS) terminal.

**Retail agents.** Retail agents that have a digital device connected to communications infrastructure to transmit and receive transaction details enable customers to convert cash into electronically stored value (“cash-in”) and to transform stored value back into cash (“cash-out”).

**Additional financial services via the digital transactional platform.** A digital transactional platform may be leveraged by combinations of banks and non-banks to offer additional financial products and services to the financially excluded and underserved—credit, savings, insurance, and even securities—often relying on digital data to target customers and manage risk.

#### **How Digital Financial Inclusion Affects the Financially Excluded and Underserved (Part II)**

Digital transactional platforms offer the possibility of providing the financially excluded and underserved with access to formal financial services. The typically lower costs of digital transactional platforms—both to the provider and thereby the customer—allow customers to transact locally in irregular, tiny amounts, helping them to manage their characteristically uneven income and expenses. The payment, transfer, and value storage services embedded in the platform itself, and the data generated, enable additional financial services tailored to customers’ needs and financial circumstances.

Digital financial inclusion reduces the risks of loss, theft, and other financial crimes posed by cash-based transactions, as well as the costs associated with transacting in cash and using informal providers. It can also promote economic empowerment by enabling asset accumulation and, for women in particular, increasing their economic participation.

Digital financial inclusion also carries risks for the same vulnerable financially excluded and underserved customers that benefit from the opportunities. Agent-related risks figure among the most distinctive compared with the risks posed by conventional financial services.

### **Key Regulatory Issues in Digital Financial Inclusion (Part III)**

The key regulatory issues raised by digital financial inclusion relate to agents, anti-money laundering and countering financing of terrorism (AML/CFT) rules, regulation of e-money, consumer protection, payment system regulation, and competition. Many of these issues fall within multiple regulators' competencies, requiring effective communication and collaboration among them.

### **Models of Digital Financial Inclusion and Their Risk Implications (Part IV)**

The models of digital financial inclusion emerging in countries around the world introduce new market participants and allocate roles and risks (both new and well known) in different ways as compared with traditional approaches to retail financial service delivery. Some risks are common to most or all approaches to digital financial inclusion. The engagement of mobile network operators (MNOs), whether as e-money issuers or as a channel for a bank or similar provider, presents certain potential risks that differ from approaches without MNOs. Some risks are triggered by the model of the digital transactional platform in question. Finally, some risks relate to the provision of additional financial services beyond the payments, transfers, and value storage services offered by the digital transactional platform itself.

## **PART I: WHAT IS “DIGITAL FINANCIAL INCLUSION”?**

“Digital financial inclusion” refers broadly to the use of digital financial services to advance financial inclusion. The term “financial inclusion” refers to an ideal end state in which all households and businesses have access to *and use*<sup>6</sup> a range of financial services (see Box 2). As noted by the GPFI, financial inclusion can contribute to economic growth, efficiency, increased welfare, and help to reduce the risks posed by financial exclusion.<sup>7</sup> The GPFI has also noted that financial inclusion is changing the nature and sometimes also the level of risks to consumers, providers, and financial systems. These changes result from a variety of factors, including the characteristics of financially excluded and underserved customers and their lack of experience with formal financial services; the specifics of the products, services, and providers capable of

---

<sup>6</sup> Currently, less than 30% of mobile money customers are active users (GSMA 2013 State of the Industry Report on Mobile Financial Services for the Unbanked, [http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2014/02/SOTIR\\_2013.pdf](http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2014/02/SOTIR_2013.pdf)).

<sup>7</sup> GPFI White Paper “Global Standard-Setting Bodies and Financial Inclusion for the Poor—Toward Proportionate Standards and Guidance” (2011, GPFI White Paper) at <http://gpfi.org/publications/global-standard-setting-bodies-and-financial-inclusion-poor>. The risks posed by financial exclusion include threats to financial integrity and international security, social and political stability, and in some cases, financial stability. Id at 1–2.

reaching them; and the innovative approaches needed to accomplish significant increases in financial inclusion. All these factors are relevant to digital financial inclusion.

**Box 2: GPFi’s Definition of “Financial Inclusion”: An Ideal End State**

“Financial inclusion” is a state “in which all working age adults have effective access to the following financial services provided by formal institutions: credit, savings (defined broadly to include current accounts), payments, and insurance.”<sup>8</sup>

“Effective access” involves convenient and responsible service delivery, at a cost affordable to the customer and sustainable for the provider, with the result that financially excluded and underserved customers can access and use formal financial services.<sup>9</sup>

“Responsible delivery” involves both responsible market conduct by providers<sup>10</sup> and effective financial consumer protection oversight. The specific characteristics of excluded consumers have significant implications for effective consumer protection regulation and supervision, and therefore also SSB standards and guidance aimed at enabling financial inclusion.

*Source: GPFi White Paper (2011).*

For decades, banks and other financial institutions have been using digital means to serve their existing customers. Credit cards, debit cards, and automated teller machines (ATMs) have been widely used since the 1970s and 1980s, although debit cards and POS terminals became widely used only in the 1990s. The use of computers and landline phones to access bank accounts has increased significantly since 2000. More recently, bank customers and customers of some other non-bank deposit-taking institutions have been able to access their accounts via mobile phone. And most recently, digital technology and communication channels—including mobile phones, payment cards, and POS terminals—have been used by those who do not have a direct relationship with a bank but instead sign up with a non-bank provider. “Digital financial inclusion” involves the deployment of these and other new cost-saving digital means to reach currently financially excluded and underserved populations with a range of formal financial

---

<sup>8</sup> The GPFi White Paper did not address financial inclusion issues relevant to securities or the International Organization of Securities Commissions (IOSCO). The GPFi commenced collaboration with IOSCO in September 2013, as securities are being sold and traded in some markets to formerly excluded customers, including via digital transactional platforms.

<sup>9</sup> A “formal” financial service involves a financial service provider that has a recognized legal status. This category includes entities (and, in some countries, individuals) with widely varying regulatory attributes, subject to differing levels and types of external oversight.

<sup>10</sup> “Responsible market conduct by providers” includes reasonable steps to ensure transparency and fair treatment and to mitigate consumer risks.

services suited to their needs that are responsibly delivered at a cost affordable to customers and sustainable for providers.

*Components of digital financial inclusion.* The essential components of digital financial inclusion include the following:

- **Digital transactional platform.** A digital transactional platform enables a customer to make or receive payments and transfers and to store value electronically<sup>11</sup> through the use of a device that (i) is a means of transmitting and receiving data and (ii) connects—directly or through the use of a digital device—to a bank or non-bank that is permitted to store electronic value.<sup>12, 13</sup>
- **Device.** The device used by the customer can be (i) a digital device, such as mobile phone,<sup>14</sup> that is a means of transmitting data and information or (ii) an instrument, such as a payment card, that connects to a digital device, such as a POS terminal.<sup>15</sup>
- **Retail agents.** Retail agents have a digital device connected to communications infrastructure to transmit and receive transaction details and other data and information. Retail agents also have a cash drawer that enables the customer to convert cash into electronically stored value (“cash-in”) and to transform such stored value back into cash (“cash-out”).

---

<sup>11</sup> The stored value may or may not constitute a “deposit” under the law of the country in question. The broad definition of electronic money given by the CPSS (now CPMI) Working Group on Innovations in Retail Payments is: “monetary value represented by a claim on the issuers which is stored on an electronic device ... and issued upon receipt of funds in an amount not less in value than the monetary value received and accepted as a means of payment by undertakings other than the issuer.”

<sup>12</sup> The terms “digital wallet,” “mobile wallet,” “e-wallet,” and “electronic wallet” are sometimes used to refer to this ability to carry, access, and use value stored in or via a digital device. When issued or distributed by an MNO, this stored value is often referred to as “mobile money.”

<sup>13</sup> The bank or non-bank that holds the stored electronic value may be the customer’s provider or may hold funds deposited by the customer’s provider (whether in the provider’s own name or on behalf of the customer).

<sup>14</sup> The customer may own the phone or other digital device or may use a device of another person: agent, friend, family member.

<sup>15</sup> Today, mobile phone-based digital transactional platforms have the advantage of using the existing communications infrastructure and the device, which many financially excluded or underserved poor people already own or can otherwise access and use. According to the GSMA, an estimated 1.7 billion people around the world have access to a mobile phone but no bank account (*Mobile Money: Enabling regulatory Solutions* 2013, <http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/02/MMU-Enabling-Regulatory-Solutions-di-Castri-2013.pdf>). However, lack of adequate infrastructure (electricity, mobile network coverage, roads, and transport networks) continues to hinder the expansion of such services in rural areas (World Bank Development Research Group, the Better than Cash Alliance, and the Bill & Melinda Gates Foundation 2014).

- ***Additional financial services via the digital transactional platform.*** A digital transactional platform may be leveraged to provide additional financial products and services: credit, savings, insurance, and even securities. In some cases, a third party provides the service and the digital transactional platform enables the receipt of funds (such as the proceeds of a loan), depositing funds (such as into a savings account), paying for and/or administering the service (such as paying insurance premiums, disbursing insurance benefits, or purchasing a security), and the means for signing up for a product or service (such as credit, insurance, or a security).

*Agents and agent networks.* Currently, in most cases of digital financial services offered to financially excluded and underserved populations, the agent network is a critical component.<sup>16</sup> In addition to their essential cash-in and cash-out role,<sup>17</sup> agents may perform other functions. For example, in some cases, customers can sign up for an account or other service (such as submitting a loan application) via agents; in other cases, an account or a loan cannot be activated without the approval—in person or remotely—of the service provider. And in yet other cases, certain products can be signed up for directly via digital device, without an agent’s involvement.

Great diversity can be found among models for developing and managing agent networks. In the case of mobile phone-based digital transactional platforms, airtime distribution networks may serve as a basis for developing an agent network for financial services as well. There are many examples of using well-developed retail networks such as supermarket chains and petrol stations. Agent networks have also been built using independent, community-based microenterprises. Where agent networks have become well developed, digital transactional platform providers have used agent network managers to recruit, train, and oversee agents and, in many cases, to manage agent liquidity.<sup>18</sup>

In some countries, retail agents for cash-in and cash-out exist alongside what may be seen as “electronic agents”: ATMs and payment terminals. These are generally used for cash and payment functions.<sup>19</sup> Several factors—increased use of digital means for paying wages, salaries,

---

<sup>16</sup> See World Bank Development Research Group, the Better than Cash Alliance, and the Bill & Melinda Gates Foundation (2014): “Providing physical access to financial services or cash-in/out points and ensuring sufficient liquidity at access points, including in rural areas, remain the core challenges in moving toward digital payments.” *Id.* at 14.

<sup>17</sup> Today, some countries permit agents to provide cash-in but not cash-out services; other countries permit agents to provide the reverse. The utility of a digital transactional platform as a vehicle for financial inclusion is limited in obvious respects if agents are not permitted to provide both cash-in and cash-out services.

<sup>18</sup> Finding a profitable model that offers sufficient remuneration to agents is challenging, and providers are working with varying levels of success to develop agent fee structures that are sustainable for both agents and providers and affordable to the customer as well.

<sup>19</sup> As with human agents, in some countries these machines and terminals are used only for cash-out, and in some they are used only for cash-in.

government benefits, remittances, merchant payments, and bill payments; increased use of smart phones by currently financially excluded and underserved populations; and apps designed for their needs—could reduce the role of the agent network in the provision of digital financial services in the future. For the time being, however, agents are a key distinguishing feature of digital financial inclusion as compared with digital financial services offered to customers already served by the formal financial system.

*Digital transactional data.* Data from digital financial transactions (and mobile phone usage data in the case of MNOs) help providers better understand customer needs and patterns. Increasingly, the data are providing a basis for creating new products targeting previously financially excluded and underserved market segments and offering better tailored terms. For example, new approaches to credit scoring for this clientele using algorithms based on these data provide the basis for credit risk analysis for tiny consumer loans delivered via digital transactional platforms. The potential of Big Data to drive the provision of additional financial services delivered via a digital transactional platform is significant.<sup>20</sup>

## **PART II: HOW DIGITAL FINANCIAL INCLUSION AFFECTS THE FINANCIALLY EXCLUDED AND UNDERSERVED**

For the 2.5 billion adults who transact exclusively in cash due to lack of effective access to formal financial services,<sup>21</sup> having digital access to financial services may be transformational. First, the digital transactional platform permits them to transact locally in irregular, tiny amounts, helping them to manage their characteristically uneven income and expenses. Over-the-counter transactions<sup>22</sup> are generally the most commonly used digital financial services among the previously financially excluded and underserved in many countries, though migration to account-based services has also typically expanded over time as customers gain familiarity with—and trust in—a digital transactional platform. (See description of bKash in Box 3.) For recipients of government-to-person payments, such as conditional cash transfers, receipt into a digital stored-value account may be the recipient’s door into the financial system.<sup>23</sup> Second, this functionality also makes possible the offering of other financial products tailored to their needs.<sup>24</sup> (See description of M-Shwari and Tigo in Box 3.) Third, it reduces the risks of loss, theft,

---

<sup>20</sup> The term “Big Data” is often used in the digital financial inclusion context to refer to high-volume, high-velocity, and high-variety data of the types described. The potentially broader scope of the concept extends beyond that of this Issues Paper.

<sup>21</sup> See report by the World Bank Development Research Group, the Better than Cash Alliance, and the Bill & Melinda Gates Foundation (2014).

<sup>22</sup> An over-the-counter transaction does not involve customers using electronically stored value. Instead, customers go to an agent to send and receive funds instead of using their own accounts.

<sup>23</sup> See, eg, Zimmerman, Jamie M., Kristy Bohling, and Sarah Rotman Parker. 2014. “Electronic G2P Payments: Evidence from Four Lower-Income Countries.” Focus Note 93. Washington, D.C.: CGAP, April.

<sup>24</sup> The capacity for poor people to “pay as you go” afforded by a digital transactional platform is also enabling the offering of non-financial services, such as electricity and water, to customers too poor to



and other financial crimes posed by cash-based transactions, as well as the costs associated with transacting in cash and using informal providers (although there will typically be transaction fees charged to the customer). Digital financial services can also promote economic empowerment by enabling asset accumulation and, for women in particular, increasing their economic participation.<sup>25</sup>

### **Box 3: Three Examples of Digital Financial Inclusion**

#### ***bKash in Bangladesh—An example of a digital transactional platform***

bKash launched in 2011. A 51% subsidiary of BRAC Bank, bKash enables mobile phone customers to open an account, to make bill payments and money transfers via mobile phone, and to do cash-in/cash-out transactions at bKash agents. Today, a majority of the transactions are over-the-counter transactions between family members, although the number of account-to-account transactions is increasing.

While bKash manages the mobile financial service operations, BRAC Bank is responsible for regulatory compliance. bKash is required by law to deposit its customers' mobile account balances with a prudentially regulated bank.

As of December 2013, bKash (with more than 500 staff and 90,000 agents) conducted a monthly average of 13 million cash-in transactions and 12 million cash-out transactions, 5 million "account-to-account" transactions, and 300,000 other transactions. The average transaction size was \$27, and monthly transaction volume was \$680 million.<sup>26</sup>

#### ***M-Shwari in Kenya—An example of interest-bearing savings and consumer loans offered via a digital transactional platform***

M-Shwari—a joint venture of the Commercial Bank of Africa (CBA) and Safaricom, Kenya's largest MNO—launched in November 2012. Both an interest-bearing, no minimum balance, savings and a consumer credit product are available to customers of M-PESA, a digital transactional platform offered by Safaricom. M-Shwari accounts are bank accounts with the CBA that can be accessed only via the M-PESA platform.

---

afford post-paid utilities. This is sometimes referred to as "digital finance plus" and falls beyond the scope of this Issues Paper.

<sup>25</sup> Report by the World Bank, the Better than Cash Alliance, and the Bill & Melinda Gates Foundation (2014). "The Opportunities of Digitizing Payments," August. See also [http://www.huffingtonpost.com/lisa-kienzle/savings-groups-mobile-pho\\_b\\_5695573.html?utm\\_hp\\_ref=tw](http://www.huffingtonpost.com/lisa-kienzle/savings-groups-mobile-pho_b_5695573.html?utm_hp_ref=tw).

<sup>26</sup> Chen, Gregory, and Stephen Rasmussen. 2014. "bKash Bangladesh: A Fast Start for Mobile Financial Services." Brief. Washington, D.C.: CGAP, July. [http://www.cgap.org/sites/default/files/Brief\\_bKash\\_Bangladesh\\_July\\_2014.pdf](http://www.cgap.org/sites/default/files/Brief_bKash_Bangladesh_July_2014.pdf)

For the savings product, customers can transfer funds from M-PESA to M-Shwari, earning an interest rate of 2–5% per annum, and funds can be withdrawn through M-PESA’s network of agents. The M-Shwari loan is a consumer loan product that is available to M-PESA customers who have had an M-PESA account (with Safaricom) for at least six months. To determine the maximum borrowing limit, M-Shwari uses an algorithm based on factors including savings behaviour with the M-Shwari account, as well as prior behaviour as a Safaricom customer, including use of voice, data, and the M-PESA digital transactional platform. A fee of 7.5% is levied for each one-month loan.

Ten weeks after launch, Safaricom reported that M-Shwari had 1.6 million registered customers. (The aggregate outstanding M-Shwari loan balance as of end 2013 was US\$9.3million.) As of March 2014, there were 5 million registered M-Shwari customers and 2.4 million active customers with total deposits of US\$21million.

***Tigo Family Care Insurance in Ghana—An example of life insurance coverage offered via a digital transactional platform***

Tigo Family Care Insurance launched in 2010. The insurance product, which is underwritten by Vanguard Life Assurance, is provided by the MNO Tigo to its customers without charge as a loyalty product for Tigo’s prepaid airtime package. Tigo introduced the product to reduce the significant “churn” (i.e., movement of pre-paid mobile phone customers from one provider to another). Customers can double their coverage by paying a premium using Tigo airtime.<sup>27</sup>

Between the launch of this innovative product and December 2013, the total number of insurance policy holders in Ghana increased from 720,000 to 3.6 million, including 1.3 million customers insured through Tigo.

Digital financial inclusion also introduces risks for customers due to their lack of familiarity with the products, services, and providers and their resulting vulnerability to exploitation and abuse. The risks may be even higher if the new providers offering the services are not subject to the consumer protection provisions that apply to banks and other traditional financial institutions.

Customers with little or no literacy and limited numeracy may have difficulty with even a simple payment transaction using a mobile phone operating on a USSD channel.<sup>28</sup> Recent studies indicate that inexperienced customers are more likely to rely on someone else—perhaps even

---

<sup>27</sup> Tigo’s digital transactional platform is capable of having premiums paid with mobile money (as opposed to airtime), and this will likely be permitted in the future. Claims are paid out only to a Tigo wallet.

<sup>28</sup> USSD (unstructured supplementary service data) is a menu-driven communication channel that can be used by GSM mobile phones and that can be used for large-scale mobile financial services. However, it cannot be used in all alphabets.

the agent with whom they most frequently transact—to supply and remember personal identity numbers (PINs).<sup>29</sup>

Perhaps the greatest source of customer vulnerability with digital financial inclusion results from the central role played by agents as the principal customer interface. When there is little if any face-to-face communication with the provider, there is likely less clarity and transparency with respect to the risks that the customer is assuming as well as the means of recourse in the event of a loss or transgression by either the provider or the agent. Moreover, it is difficult for even the most scrupulous provider to monitor and combat agent fraud, which could range from smaller wrong doing such as imposing and pocketing fees not sanctioned by the provider to much more serious offenses, such as mass appropriation of PINs given to an agent in trust by unsuspecting customers and the emptying of the stored-value accounts in question.

Customer uptake of digital financial services in many markets suggests on balance these risks may not be perceived to outweigh the benefits of being financially included. Nonetheless, the case is strong for appropriate regulation and supervision, as discussed in Part IV, and there are calls for suitability standards and principles in digital financial inclusion from a number of observers.

### **PART III: KEY REGULATORY ISSUES IN DIGITAL FINANCIAL INCLUSION**

The key regulatory issues raised by digital financial inclusion relate to agents, AML/CFT rules, e-money regulation, consumer protection, payment system regulation, and competition.<sup>30</sup> Many of these issues fall within multiple regulators' competencies, requiring effective communication and collaboration among public bodies, at least some of which may not be accustomed to working together.

*Agents.* Regulatory permission to transact through agents is becoming commonplace across all regions, at least with respect to some categories of providers and with respect to certain activities (although the permitted activities vary significantly across countries). Many countries are now confronting new agent-related issues, including whether to apply the same rules to bank- and non-bank agents where both exist in a given market; whether agents should be permitted to work with multiple financial service providers; whether providers may require agents to be exclusive; what activities agents should be permitted to engage in; and how agents should be supervised.

---

<sup>29</sup> See CGAP and MicroSave presentation “Consumer Protection and Emerging Risks in Digital Financial Services: Perspective from Bangladesh, Uganda, Colombia, and the Philippines” at Responsible Finance Forum, Perth, Australia, 28 August 2014.

<sup>30</sup> All are reflected with various levels of specificity in the G20's Principles for Innovative Financial Inclusion. See <http://www.gpfi.org/publications/principles-and-report-innovative-financial-inclusion>. See, also, Lyman, Timothy, Mark Pickens, and David Porteous. 2008. “Regulating Transformational Branchless Banking: Mobile Phones and Other Technology to Increase Access to Finance” Focus Note 43. Washington, D.C.: CGAP.

*AML/CFT.* Development of risk-based AML/CFT rules adapted to the realities of remote transactions conducted through agents remains a significant challenge to progress on financial inclusion generally in many countries. This has particular significance regarding customer due diligence, given the lack of a fixed address and other information often required for customer identification and verification under applicable country-level regulation. On the other hand, data derived from the use of digital transactional platforms and from the customer’s digital device (i.e., non-financial data from a mobile phone, such as geolocation data and calling patterns) offer both providers and law enforcement new means of discerning suspicious transactions and financial crimes.<sup>31</sup>

*Regulation of e-Money and Other Stored-Value Instruments.* Appropriate regulation of the issuance of e-money and other stored-value instruments<sup>32</sup> by parties other than prudentially supervised banks is often important both for providers (i.e., e-money issuers) and supervisors. For e-money issuers, regulation helps guard against arbitrary regulatory and supervisory actions; for supervisors, regulation provides guideposts for the level and type of oversight appropriate.

*Consumer Protection.* With digital financial inclusion, the use of agents as the primary interface with the customer introduces new consumer protection challenges, especially when the customer is located far from the provider of financial services (and from recourse mechanisms). Long distances can make oversight of agent actions difficult, introducing increased risk of fraud and theft, abusive treatment, and failure to handle customer data confidentially. Use of retail agents and agent network managers expands the possibility of factual and legal disagreements about who is responsible to the customer in the case of fraud or other alleged misdeeds. Disagreements may also arise from the use of data analytics that develop and support credit scoring models and other means of targeting new customers.

Transparency with respect to risks, liability, recourse, and other issues of relevance to the consumer poses a greater challenge when there is little if any face-to-face communication with the provider. Transparency (and comprehensibility) of pricing becomes more difficult with arguably separate, yet embedded transactions. In the design of new products and services, it is important to ensure that such products meet suitability standards and principles.<sup>33</sup>

New risks with respect to data privacy and security are introduced by the storage and transmittal of data that provide the new AML/CFT tools noted above. These risks are magnified due to the large number of agents handling customers’ transactional and other data, the increased capacity to analyse those data, and the increasing risk of data breaches.

---

<sup>31</sup> See Chatain (2011) for a discussion and guidance on addressing the AML/CFT risks of mobile financial services.

<sup>32</sup> Some electronically stored-value products may not be defined as “e-money” although they likely have the elements of e-money as defined in the 2012 Report of the CPSS (now CPMI) Working Group on Innovations in Retail Payments and quoted in footnote 11.

<sup>33</sup> See, eg, FinCoNet’s “Report on responsible lending—Review of supervisory tools for suitable consumer lending practices,” July 2014, <http://www.finconet.org/FinCoNet-Responsible-Lending-2014.pdf>.

*Payment system regulation.* Inclusive payment system regulation that enables participation, direct or indirect, by banks and non-banks and effective payment system oversight take on increasing importance as digital transactional platforms reach scale. Regulation and policies that promote interoperability and interconnectivity will be critical to the success of digital financial inclusion.<sup>34</sup> The participation of non-banks in payments schemes and the emergence of schemes that do not follow the traditional card-based model raise new issues for regulators and payment system overseers, including non-banks' access to clearing and settlement systems used by the banking system and banks' access to USSD channels.

*Competition.* Competition between banks and non-banks for new customers—including the financially excluded and underserved—is present in many markets and is evidenced by lowering of fees, efforts on the part of banks to reduce their operational costs, and the introduction of new products and services. Policies that balance incentives to launch new products and platforms with the risk of protecting a dominant player in the market will also be critical to the success of digital financial inclusion.<sup>35</sup> For example, when non-banks are excluded from a real-time gross settlement system (RTGSS), in the absence of a competition policy that enables new entrants and innovations, banks may impose high costs and deliver low-quality payment processing services. In one jurisdiction, in response to such actions by banks, the regulator issued new regulations specifically to promote mobile payments (due to their ability to reach the excluded and underserved) and their interoperability. The new regulations require mobile payment clearing houses to participate in the RTGSS (CPMI 2014).<sup>36</sup>

#### **PART IV: MODELS OF DIGITAL FINANCIAL INCLUSION AND THEIR RISK IMPLICATIONS**

In countries around the world, both banks and non-banks are developing the means of reaching financially excluded and underserved people and businesses via digital transactional platforms. In an increasing number of countries, this is enabling the offering and delivery of additional financial services beyond payments, transfers, and value storage to the same market segment. These new platforms involve emerging models that bring in new market participants and allocate roles and risks (both known and new) in different ways when compared with traditional approaches to retail financial service delivery.

---

<sup>34</sup> The CPMI recently noted that the limited impact of payment services on access to and use of other financial services “can be attributed, in part, to the lack of interconnectivity of predominantly proprietary innovative systems with other retail payment systems, both ‘traditional’ and innovative, and the broader financial system” (CPMI 2014).

<sup>35</sup> With respect to government-to-person payments, such as salaries, pensions, and other benefits, governments will often start with a pilot with one provider. Governments should consider in advance the competition issues raised by providing one provider with the first-mover advantage.

<sup>36</sup> The new regulations also require all participants to process interbank mobile payments in less than 15 seconds (from initiation to funds posting), faster than the requirement for other RTGSS transfers, and cut the originating fee for mobile payments to less than US\$0.01 from US\$0.04 (CPMI 2014).

The diversity of models, differing market structure, and varying legal and regulatory frameworks make it impossible to predict every risk. For similar reasons, it is not possible to address meaningfully at a global level the many challenges to effective communication and coordination among the various regulatory and supervisory bodies that might be involved, including the prudential banking authority, the payment systems overseer, the telecommunications authority, the financial intelligence unit responsible for AML/CTF rules, and the relevant consumer protection agency or agencies.<sup>37</sup>

However, it is possible to identify and explore some of the main risks of interest to both country-level policy makers and the SSBs. The main risks of interest to BCBS, CPMI, and FATF discussed below include credit risk, operational risk (such as technology failure or unreliability), clearing and settlement risk, and the risk of financial crimes, including agent fraud<sup>38</sup> as well as money laundering and terrorist financing risk. In addition, consumer risks of interest to the SSBs generally are considered, including the risk of customer confusion as to whether customers' balances are insured, which is of specific interest to IADI.

Some risks are common to most or all approaches to digital financial inclusion; these risks are tied primarily to the use of agents, the technology, and the legal status and treatment of electronically stored value. The engagement of MNOs, whether as issuers of e-money or as a channel for a bank or similar provider, presents some specific risks. Other risks are triggered by the model of the digital transactional platform in question. And yet other risks are triggered by the offering via the digital transaction platform of additional financial services that may be provided by third parties. Each of these topics is covered separately below.

### ***Three Drivers of Risk Common to Most or All Digital Financial Inclusion Models***

As noted, three broad drivers of risk distinguish most or all digital financial inclusion models from digital financial services offered as a channel to customers already served by traditional channels:<sup>39</sup>

1. The use of agents as the principal customer interface.
2. The digital technology used, which may present certain risks in its own right, as well as additional risks due to the involvement of agents and the profile of the previously financially excluded and underserved customers themselves.
3. The likelihood that multiple bank and non-bank parties will be involved in the storage and management of account data and the holding of customers' funds, adding complexity to protecting customers against risk of loss upon the failure of one or more

---

<sup>37</sup> Other public bodies that might be involved include, among others, the competition authority and the social protection ministry (in countries using digital means for making social payments).

<sup>38</sup> Agent fraud in digital financial inclusion is an operational risk; it is also a financial crime. In this Issues Paper it is discussed as both.

<sup>39</sup> These are obviously only some of the drivers of risk common to all models of digital financial inclusion, although they tend to figure among the most material.

of them, depending on the division of labour among the parties and their regulatory treatment.

*Agent-related risks.* Agents introduce new operational, financial crime, and consumer risks. Many of the operational and consumer risks are the result of the physical distance that may separate agents and the provider or the agent network manager, which makes oversight and ongoing training challenging. Furthermore, use of agents and agent network managers expands the possibility of factual and legal disagreements about who is responsible to the customer in the case of fraud or other alleged misdeeds. Physical distance can also introduce oversight challenges with respect to AML/CFT compliance.

Agents introduce operational risks including fraud (also a financial crime and consumer risk), agent error, poor cash management by the agent, and poor data handling. In addition to the financial crime risks of fraud and theft (including data theft), agents may fail to comply with AML/CFT rules regarding customer due diligence, handling records, and reporting suspicious transactions.<sup>40</sup> Agents may also engage in abusive treatment, take actions that reduce transparency (for example, on pricing, terms, and recourse), and fail to handle customer data confidentially.

*Digital technology-related risks.* The quality of the digital technology and its reliability informs the operational and consumer risks of disrupted service and lost data, including payment instructions (for example, due to dropped messages), as well as the risk of a privacy or security breach resulting from digital transmittal and storage of data.<sup>41</sup> (As there may be more than one provider involved in storing and transmitting data, the security against a breach in the system as a whole is only as great as the weakest link.) These privacy and security risks are magnified due to the large number of agents that handle customers' transactional and other data and the profile of previously excluded and underserved customers, as noted above.

*Account data storage and management, custodial arrangements, and customers' risk of loss.* Digital financial inclusion models typically involve at least one bank and one non-bank in both the electronic storage and management of data as well as the holding of customers' funds. (See "Risks Varying by Notional Model of Digital Transactional Platform," below.) Protecting

---

<sup>40</sup> In all three cases, the financial service provider's overall responsibility for AML/CFT compliance does not change with the addition of agents to the picture. This said, digital transactional platforms introduce sometimes complex divisions of labor in practice among the provider, the agent, and potentially third parties. See Box 6, Using Agents in AML/CFT Compliance: Illustrative Examples from Three e-Money Issuers, in Lyman and Noor (2014).

<sup>41</sup> The licensing, regulation, and supervision of the technology provider may be handled by a non-financial regulator—for example, the telecommunications regulator in the case of an MNO—and may introduce additional challenges to identifying, managing, and mitigating data privacy and security risks presented by the technology in question in the context of financial services. Such challenges are not unique to the financial inclusion context.

customers' funds in the event of the failure of the party holding the funds<sup>42</sup> will depend on many factors, including whether the holder participates in a deposit insurance system and whether the specific type of account in which the funds are held is insured;<sup>43</sup> and if the account pools multiple customers' funds, whether coverage limits apply to the account as a whole or to customers' individual balances. Even if the customers' funds are insured, if they are pooled and a third party (such as an MNO) is responsible for storing and managing records of customers' account balances, then there are risks related to real-time accuracy and reconcilability of the records of the failing holder of funds with the records of the entity managing the accounts.<sup>44</sup>

### ***Risks Presented by Models Involving MNOs***

Models in which an MNO has a central role—as a channel, a distributor, or as an issuer of e-money—raise operational, financial crime, and consumer risks tied to the use of an agent network and the nature of the MNO's technology.

*MNOs and agents.* An MNO's use of agents may introduce increased operational risks (as compared with those faced by banks and similar providers) if the MNO lacks necessary experience to manage and oversee an agent network engaged in financial transactions (as distinguished from the agent activities with which MNOs are familiar, such as opening mobile accounts and air-time top-up).<sup>45</sup> Similarly, some MNOs may be less experienced, at least initially, with managing AML/CFT compliance. When the MNO is a channel for a provider, that provider (for example, a bank) is responsible for compliance with AML/CFT rules and will need to ensure itself of the MNO's effective oversight of its agent network and the network's compliance with such rules.

*MNOs and technology.* Consumer risks tied to the MNO's technology include privacy risks that are presented by the particular situation in which an MNO handles information about its

---

<sup>42</sup> Regulation typically requires that e-money be held by a bank or other prudentially regulated and supervised institution.

<sup>43</sup> In some jurisdictions, a bank can be specifically licensed to issue e-money, which is treated differently from other money held by the bank for its customers: customers' balances will not be treated as deposits but rather as accounts payable on the books of the bank and, therefore, are unlikely to be covered by deposit insurance and are likely to fall below deposits on the prioritization of claims in the event of a bank failure.

<sup>44</sup> The failure of a third party storing and managing account data poses additional risks of loss for customers: Even if their funds are held in a financially sound institution, electronic records documenting each customer's claim may be lost. If the failing party managing account data is also the issuer of e-money that customers have purchased, the fact that their funds are held in a pooled account with a financially sound institution may not prevent loss, if the account in question is not a trust or similar custodial arrangement for customers' benefit, but rather is subject to claims of the failing e-money issuers' creditors. Varying treatment of banks and non-banks under a country's bankruptcy and resolution regimes adds complexity beyond the scope of this Issues Paper.

<sup>45</sup> Over time, MNOs that work with agents to provide financial services should become familiar with the management tasks and responsibilities, reducing or eliminating any difference in capability between MNOs and traditional financial institutions.



customers' financial transactions. The role of the MNO enables the sharing of information between merchants and payment service providers in a way that typically doesn't occur with the other payment instruments (for example, credit and debit cards). Information transmitted in a payment transaction using a mobile phone is collected by providers. This information can be analyzed to create an aggregate picture that was never intended to be disclosed by the customer and may not even be known to the customer. While such practices may enable providers to profile and target individual customers (whether or not they want their data used in this manner), the potential to increase financial inclusion, as evidenced by the rapid uptake of M-Shwari (see Box 3), warrants attention.

### ***Risks Varying by Notional Model of Digital Transactional Platform***

The specifics of the digital transactional platform—the parties involved, roles played, the regulation to which they may be subject—will be key determinants of risks and their mitigation. The various arrangements that have emerged can be grouped into four notional models based on the party holding the contractual relationship with the customer: (i) full-service banks providing access to a “basic” or “simplified” transactional account for payments, transfers, and value storage via mobile device or POS terminal; (ii) limited-service niche banks providing access to an account via mobile device or POS terminal; (iii) MNO e-money issuers; and (iv) non-bank non-MNO e-money issuers.<sup>46</sup> Within these four notional models, there are numerous variations, some of which materially affect important risks and their mitigation. Nonetheless, the four notional models provide a framework for highlighting the main risks presented by a particular model as well as the main holder or holders of those risks. In some cases, the potential risks and risk-holders are similar across two or more notional models. Some risks may be relevant to all models, but with different parties holding the risk.

*Banks with Small Transaction Accounts Accessed via POS Terminal or Mobile:* Some banks offering small-balance transaction accounts (often defined in regulation as “simplified” or “basic” accounts, and sometimes treated as bank-issued e-money) host their account operations on an external platform managed (entirely or in part) by a third party.<sup>47</sup> This third party could be a licensed or unlicensed payment service provider (PSP), an MNO, or even a mobile virtual network operator (MVNO) that contracts with existing MNOs to use their unused network capacity. The third party may drive the business, selecting the bank, marketing the product and signing up new customers, managing the accounts, and handling all aspects of the agent business. In some cases, the arrangement is between two parties unrelated except by contract;

---

<sup>46</sup> For purposes of this discussion, the term “e-money issuer” also covers issuers of other similar digital stored-value products.

<sup>47</sup> Having such accounts managed on an external system can be extremely cost effective and may be a driving factor in the profitability of the model. The accounts are highly transactional and require large bandwidth and throughput of the core banking system, which is typically very expensive. In addition, it is difficult and costly to implement new products in legacy core banking systems. Finally, accounts hosted in core banking systems are subject to accounting rules and reporting requirements that are typically more expensive to comply with than the requirements applied to a simplified account or e-money account.

in others, the parties are a parent and subsidiary.<sup>48</sup> In all cases, customers' funds are held by the bank and may, in some cases, be considered bank deposits.<sup>49</sup>

The specific outsourcing arrangements between the bank and the third party—in particular, the allocation of responsibility for various aspects of the digital transactional platform—will determine which entity is managing the various operational risks outlined above. This outsourcing poses an additional operational risk, which may be difficult for the bank to manage if the outsourced business grows to represent a significant portion of the bank's assets.<sup>50</sup> Some supervisors may do onsite supervision of such outsourcing or eventually require a transfer of the business to a larger bank. Some banks are experimenting with new core processing systems specifically designed (by external providers) for simplified accounts and e-money accounts.

Several countries that allow for this notional model of digital transactional platform have adopted regulation defining “tiered accounts” for purposes of AML/CFT compliance. The term refers to a progression of types of account, ranging from a basic, low-value product with limited functionality to a conventional transaction account with greater functionality and higher value limits. Account “tiers” directly link the level of customer due diligence to the extent and range of financial services offered to a customer.

*Niche Banks Accessed via POS Terminal or Mobile:* Niche banks are limited-service banks that generally provide payment, transfer, and electronic storage-of-value services. In some countries, they are permitted to engage in microlending, although more commonly they are required to hold exclusively specified safe and liquid assets. They generally require fewer back-end capabilities than commercial banks and, therefore, have lower technology and labour costs. They may also use less expensive core processing systems. As with the model described above, a third party may drive the business, selecting the bank, marketing the product and signing up new customers, managing the accounts, and handling all aspects of the agent business.

As niche banks present less complex and fewer risks due to the limited offering of services and products (and typically little or no credit risk if they do not engage in retail lending), they are subject to less onerous prudential rules than those applicable to commercial banks.<sup>51</sup>

Settlement risk for niche banks will depend on whether they have access to direct settlement through the central bank and, if so, whether they are regulated and subject to the same oversight as full-service banks taking part in central bank settlement.

---

<sup>48</sup> In some countries where MNOs are not legally permitted to issue e-money, an MNO wishing to offer a digital transactional platform has purchased a bank to issue e-money that is distributed via the MNO. In other countries, a bank has set up a separate subsidiary to issue the e-money.

<sup>49</sup> In at least one country, the funds are treated as accounts payable on the books of the bank rather than deposits, with one consequence being that the funds are not insured.

<sup>50</sup> This could also trigger concentration risk for the bank.

<sup>51</sup> For example, initial minimum capital requirements are often significantly less than requirements for full-service banks.

As in the case of the previously described notional model of a digital transactional platform, countries providing for niche banks in their regulatory frameworks have typically also adopted regulation defining “tiered accounts” for purposes of AML/CFT compliance. The lowest “tier” is designed to be of low (or at least lower) money-laundering and terrorist financial risk and justifies simplified approaches to customer due diligence.

*MNO e-Money Issuer:*<sup>52</sup> MNO e-money issuers are non-banks that provide a digital transactional platform via a customer’s mobile phone.<sup>53</sup> The flows in and out of these accounts, which are frequently subject to transaction limits, are managed and accounted for by the MNO, although the customers’ funds are typically required to be held in an account with a prudentially supervised bank (or are subject to similar safeguarding restrictions).<sup>54</sup> In the absence of e-money regulation, MNO e-money issuers may not be explicitly subject to prudential oversight, although in some countries the banking supervisor exercises limited oversight, such as through a non-objection letter in lieu of licensing or other special arrangement. Even if subject to e-money regulation, MNO e-money issuers may not be subject to oversight by the prudential banking authority (for example, if their permitted activities are limited to payments, transfers, and value storage), especially if they are subject to safeguarding restrictions regarding customers’ funds.

This notional model could pose additional operational and consumer risks beyond those applicable to all models of digital financial inclusion outlined above, as well as additional clearing and settlement risks. (All of the MNO-specific risks discussed above are also potentially relevant.)

Operational risks will turn on the quality of the MNO’s management in handling financial operations, not simply the management of accounts but bearing primary responsibility for the operations of a finance business and compliance with all applicable rules. On the consumer protection front, in the event of the MNO’s failure, customers’ funds may also be subject to claims of the MNO’s creditors, depending on the nature of the account in which the funds are held. Clearing and settlement risk will vary depending on the extent to which payments are interoperable and how such interoperable payments (for example, inter-MNO payments) fit into the existing interbank retail payments infrastructure. The MNO will typically not be allowed access to direct central bank settlement. As for clearing, inter-MNO clearing may happen through ad hoc, one-to-one agreements, which may create multiple and uneven conditions for

---

<sup>52</sup> Some MNOs have set up a wholly owned subsidiary to act as e-money issuer, often in response to a regulatory requirement. Such entities are treated as MNO e-money issuers for purposes of this discussion. It is also theoretically possible that an MVNO could be an e-money issuer, though the research for this Issues Paper uncovered no examples.

<sup>53</sup> Some MNO e-money issuers are also issuing payment cards to enable customers to leverage existing infrastructure.

<sup>54</sup> Often, regulation or supervisory practices require that the account be a trust account established for the benefit of e-money customers. In some countries, customers’ funds are required to be held in multiple banks to reduce the risk of loss in the event of bank failure.

handling retail payments in the market.<sup>55</sup> Ideally, the payments law will govern all payments schemes, including retail payments.

*Non-Bank, Non-MNO e-Money Issuer:* Non-bank, non-MNO e-money issuers are non-banks that provide stored-value accounts on a digital transactional platform, most commonly accessed by customers via a reloadable pre-paid card. Although the issuer is not an MNO, the model may allow the account to be accessed via a mobile device. The risks are essentially the same as those of the MNO e-money issuer notional model, except that the consumer risks and other operational risks relating to the use of a mobile device and to the reliability of mobile technology will not apply, unless the use of a mobile phone is involved.

### ***Additional Financial Products and Services and Shifting Risks and Responsibilities***

As noted, in some countries, additional financial products and services are already being offered at significant scale to previously excluded and underserved customers served via digital transactional platforms. Given the many variables involved and the significant variation across the different possible models, the discussion below highlights a few of the possible areas of concern that are raised by introducing additional products and services via the MNO e-money issuer notional model discussed above.<sup>56</sup> For purposes of this discussion, it is assumed the MNO is not itself licensed to be the legal provider in the case of interest-bearing savings or credit or to be the underwriter in the case of insurance, but offers the products on behalf of a licensed provider.

In the case of an MNO e-money issuer offering its customers access to an interest-bearing savings product, the bank partner faces operational risk and the customers face risk as well due to the dependence of the bank/customer relationship on a digital channel offered by a third party. If the channel fails or the MNO terminates the partnership, the bank's depositors would not have easy access to their deposits, especially if the bank has a limited branch network. The risk is greater if the arrangement is exclusive and the bank does not have an alternate provider with similar coverage.

In the case of an MNO e-money issuer offering its customers access to bank credit, the primary additional risks are credit risk and consumer protection. The credit may be inadequately underwritten by the bank if it uses the results of the MNO's scoring algorithm as a basis for making credit decisions (as opposed to having such information supplement the other information used by the bank for its credit decisions). To manage the credit risk, the bank will need to adapt the parameters of the scoring algorithm over time based on the loan portfolio.

---

<sup>55</sup> There are a few countries in which MNOs have prefunded accounts on each other's platforms to facilitate inter-MNO payments although such arrangements present their own risks both to the MNOs and their e-money customers.

<sup>56</sup> In the case of banks and certain niche banks, additional products and services may be offered to customers generally, although this may require customers to undergo additional customer due diligence for purposes of AML/CFT compliance.

In the case of both credit and savings, the size and nature of the bank will need to be sufficient so that the additional products do not make up too large a proportion of the bank's assets and liabilities. If the partnership is exclusive (as it is likely to be for commercial reasons), its scale relative to the bank's other business will warrant careful monitoring with respect to concentration risk.

In the case of insurance products offered via mobile phone (whether there is no identified premium or there is a premium that is paid for with airtime or a digital transactional platform), there are reputational risks and consumer risks. The MNO is offering its product in tandem with the insurance and will need to be able to evaluate the strength of the insurance company underwriting the coverage in question.<sup>57</sup> Models in which insurance is offered as a loyalty product without additional charge (for example, for signing up for or maintaining a prepaid voice plan) make it impossible for customers to understand the pricing, which is embedded in the cost of the airtime.<sup>58</sup> Additionally, when coverage is extended in this way, some customers may not understand the terms and conditions under which they are insured or the procedure for making claims.<sup>59</sup>

Additional consumer protection challenges are triggered by the offering of credit, insurance, and investment products via digital transactional platforms. These include significant risks of reckless lending and mis-selling: i.e., intentional, reckless, or negligent sale of products not suited to the customer's profile. While these risks may exist outside the digital context, the provider of the platform (whether an MNO or otherwise) may lack either the motivation or the capacity to monitor such risks effectively.

## References

Chen, Gregory, and Stephen Rasmussen. 2014. "bKash Bangladesh: A Fast Start for Mobile Financial Services." Brief. Washington, D.C.: CGAP, July.

[http://www.cgap.org/sites/default/files/Brief\\_bKash\\_Bangladesh\\_July\\_2014.pdf](http://www.cgap.org/sites/default/files/Brief_bKash_Bangladesh_July_2014.pdf)

CGAP and MicroSave. 2014. "Consumer Protection and Emerging Risks in Digital Financial Services: Perspective from Bangladesh, Uganda, Colombia, and the Philippines," presentation at

---

<sup>57</sup> If the mobile phone is used merely as a means of bill payment without any further contractual relationship between the MNO and the insurance company, then this is not a specific concern of the MNO.

<sup>58</sup> This issue is emblematic of a larger consumer protection challenge that attends financial services offered via mobile generally. In all such cases, a kind of product bundling is inherent (as the voice service must be purchased in order to gain access to the financial services). Traditional concerns over bundling in the insurance context—that customers are forced or lured into purchasing unneeded or unsuitable coverage because it is bundled with a service they want or need—merits rethinking or at least closer scrutiny in the digital financial inclusion context given the likelihood that the provider would not offer the financial services that customers value and need absent the economies that come with bundling.

<sup>59</sup> In some cases, a meaningful proportion of customers have opted to pay for additional coverage, suggesting that they may understand and value the coverage.

Responsible Finance Forum, Perth, Australia, 28 August.

<http://responsiblefinanceforum.org/publications/consumer-protection-emerging-risks-digital-financial-services/>

Chatain, Pierre-Laurent, Andrew Zerzan, Wameek Noor, Najah Dannoui, and Louis de Koker. 2011. *Protecting Mobile Money against Financial Crimes—Global Policy Challenges and Solutions*. Washington, D.C.: The International Bank for Reconstruction and Development/The World Bank. <http://elibrary.worldbank.org/doi/abs/10.1596/978-0-8213-8669-9>

Committee on Payments and Market Infrastructures. 2014. “Non-banks in retail payments.” September. <http://www.bis.org/cpmi/publ/d118.pdf>

Committee on Payment and Settlement Systems (now Committee on Payment Market Infrastructure) Working Group on Innovations in Retail Payments. 2012. “Innovations in Retail Payments.” May. <http://www.bis.org/cpmi/publ/d102.pdf>

Di Castri, Simone. 2013. *Mobile Money: Enabling Regulatory Solutions*. <http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/02/MMU-Enabling-Regulatory-Solutions-di-Castri-2013.pdf>

Faz, Xavier. 2014. “5 Sources of Untapped Innovation in Digital Finance.” CGAP blog, 24 September. <http://www.cgap.org/blog/5-sources-untapped-innovation-digital-finance>

Financial Inclusion Insights. <http://finclusion.org>

FinCoNet. 2014. “Report on responsible lending—Review of supervisory tools for suitable consumer lending practices.” July. <http://www.finconet.org/FinCoNet-Responsible-Lending-2014.pdf>

G20’s St. Petersburg Development Outlook. [https://www.g20.org/sites/default/files/g20\\_resources/library/Saint%20Petersburg%20Development%20Outlook\\_0.pdf](https://www.g20.org/sites/default/files/g20_resources/library/Saint%20Petersburg%20Development%20Outlook_0.pdf)

GPFI (Global Partnership for Financial Inclusion). 2010. “Principles and Report on Innovative Financial Inclusion.” 25 May. <http://www.gpfi.org/publications/principles-and-report-innovative-financial-inclusion>

GPFI White Paper. 2011. “Global Standard-Setting Bodies and Financial Inclusion for the Poor—Toward Proportionate Standards and Guidance.” <http://gpfi.org/publications/global-standard-setting-bodies-and-financial-inclusion-poor>

GSMA. 2014. “2013 State of the Industry Report on Mobile Financial Services for the Unbanked.” [http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2014/02/SOTIR\\_2013.pdf](http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2014/02/SOTIR_2013.pdf)

Kaffenberger, Michelle. 2014. "M-Shwari in Kenya: How Is It Really Being Used?" CGAP blog, 10 April. <http://www.cgap.org/blog/m-shwari-kenya-how-it-really-being-used>

Leach, Jeremy, and Sandisiwe Ncube. 2014. "Regulating m-insurance in Zimbabwe: Managing risk while facilitating innovation." Working draft. Finmark Trust, March. [http://cenfri.org/documents/microinsurance/2014/Rep\\_M\\_insurance\\_Zimbabwe\\_2014.pdf](http://cenfri.org/documents/microinsurance/2014/Rep_M_insurance_Zimbabwe_2014.pdf)

Lyman, Timothy, Mark Pickens, and David Porteous. 2008. "Regulating Transformational Branchless Banking: Mobile Phones and Other Technology to Increase Access to Finance" Focus Note 43. Washington, D.C.: CGAP, January. <http://www.cgap.org/sites/default/files/CGAP-Focus-Note-Regulating-Transformational-Branchless-Banking-Mobile-Phones-and-Other-Technology-to-Increase-Access-to-Finance-Jan-2008.pdf>

Lyman, Timothy, and Wameek Noor. 2014. "AML/CFT and Financial Inclusion: New Opportunities Emerge from Recent FATF Action." Focus Note 98. Washington, D.C.: CGAP, August. <http://www.cgap.org/sites/default/files/Focus-Note-AMLCFT-and-Financial-Inclusion-Sept-2014.pdf>

MicroSave. 2014. "Consumer Protection and Emerging Risks in Digital Financial Services— Perspectives from four countries," presented at the Responsible Finance Forum, 28 August. [http://responsiblefinanceforum.org/wp-content/uploads/140826\\_Draft-CGAP-Presentation-v2-2.pdf](http://responsiblefinanceforum.org/wp-content/uploads/140826_Draft-CGAP-Presentation-v2-2.pdf)

Mondato. 2014. "Taking the Mobile out of Mobile Money." Blog, 20 August. <http://mondato.com/blog/taking-the-mobile-out/>

Negishi, Mayumi. 2014. "Long before Apple Pay, Japan Had 'Mobile Wallet'." Blog. Wall Street Journal, 11 September. <http://blogs.wsj.com/japanrealtime/2014/09/11/long-before-apple-pay-japan-had-mobile-wallet/>

Porteous, David. 2013. "Mobile Financial Services in Africa: The Next Generation." In Thorsten Beck and Samuel Munzele Maimbo, eds. *Financial Sector Development in Africa—Opportunities and Challenges*. Washington, D.C.: World Bank. <https://openknowledge.worldbank.org/bitstream/handle/10986/11881/9780821396285.pdf?sequence=2>

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

Reserve Bank of India's January 2014 Report of the Committee on Comprehensive Financial Services for Small Business and Low Income Households. <http://rbi.org.in/scripts/PublicationReportDetails.aspx?UrlPage=&ID=727>.

Tellez, Camillo. 2013. "Emerging Practices in Mobile Microinsurance."

[http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/07/MMU\\_m-insurance- Paper Interactive-Final.pdf](http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/07/MMU_m-insurance- Paper Interactive-Final.pdf)

World Bank Development Research Group, the Better than Cash Alliance, and the Bill & Melinda Gates Foundation. 2014. “The Opportunities of Digitizing Payments—How digitization of payments, transfers, and remittances contributes to the G20 goals of broad-based economic growth, financial inclusion, and women’s economic empowerment.” August.

<http://betterthancash.org/news-releases/world-bank-report-digital-payments-vital-to-economic-growth/>

World Bank. 2011. Financial Infrastructure Series: Payment Systems Policy and Research: *Payment Systems Worldwide—A Snapshot: Outcomes of the Global Payment Systems Survey 2010*. Washington, D.C.: World Bank. <http://betterthancash.org/wp-content/uploads/2012/09/World-Bank-Presents-Outcomes-of-the-Global-Payment-Systems-Survey-2010.pdf>

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