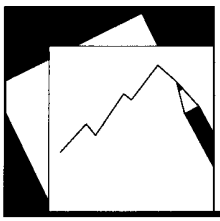
WP/14/123



IMF Working Paper

Oversight Issues in Mobile Payments

Tanai Khiaonarong

INTERNATIONAL MONETARY FUND

 WP/14/123

IMF Working Paper

Monetary and Capital Markets

Oversight Issues in Mobile Payments

Prepared by Tanai Khiaonarong[1]

Authorized for distribution by Ghiath Shabsigh

July 2014

Abstract

This paper examines oversight issues that underlie the potential growth and risks in mobile payments. International experience suggests that financial authorities can develop effective oversight frameworks for new payment methods to safeguard public confidence and financial stability by establishing: (i) a clear legal regime; (ii) proportionate AML/CFT measures to prevent financial integrity risks; (iii) fund safeguarding measures such as insurance, similar guarantee schemes, or "pass through" deposit insurance; (iv) contingency plans for operational disruptions; and (v) risk controls and access criteria in payment systems. Such measures are particularly important for low-income countries where diffusion is becoming more widespread.

JEL Classification Numbers: D18, E42, E58, G38, O33

Keywords: Oversight, risks, mobile payments, payment systems

Author's E-Mail Address: tkhiaonarong@imf.org

[1] Thanks are due to Suliman Aljabrin, Yasmin Almeida, Biaggion Bossone, Pierre-Laurent Chatain, Massimo Cirasino, Stijn Claessens, Dorothee Delort, Bjarne Hansen, Nadim Sami Kyriakos-Saad, Thomas Lammer, Harish Natarajan, David Parker, Kristel Poh, Gynedi Srinivas, Concha Verdugo-Yepes, David Walker, Froukelien Wendt, Mary Zephirin, and seminar participants at the IMF for helpful comments. Karen Lee provided research assistance.

Contents Page

GLOSSARY

ACH	Automated Clearing House
AFI	Alliance for Financial Inclusion
AML	Anti-Money Laundering
AMPI	African Mobile Phone Financial Services Policy Initiative
ATM	Automated Teller Machine
BCBS	Basel Committee on Banking Supervision
BIS	Bank for International Settlements
CFPB	Consumer Financial Protection Bureau
CFT	Countering the Financing of Terrorism
CPSS	Committee on Payment and Settlement Systems
DNS	Deferred Net Settlement
EC	European Commission
ECB	European Central Bank
EU	European Union
FAS	Financial Access Survey
FATF	Financial Action Task Force
FCA	Financial Conduct Authority
FDIC	Federal Deposit Insurance Corporation
FPS	Faster Payments Scheme
FSB	Financial Stability Board
GSMA	Groupe Speciale Mobile Association
HKMA	Hong Kong Monetary Authority
IADI	International Association of Deposit Insurers
IMF	International Monetary Fund
IOSCO	Technical Committee of the International Organization of Securities Commissions
KDIC	Kenya Deposit Insurance Corporation
LIC	Low Income Countries
LLSA	Liquidity and Loss Share Agreement
MNO	Mobile Network Operator
NFC	Near Field Communication
PFMI	Principles for Financial Market Infrastructures
PSD	Payment Services Directive
QR	Quick Response
RPS	Retail Payment Systems
RTGS	Real-Time Gross Settlement
SMS	Short Message Services
SVF	Stored-Value Facilities
TA	Technical Assistance
WAP	Wireless Application Protocol

I. INTRODUCTION

1. **Mobile payments have gained wider acceptance as an emerging payment method in both advanced and emerging economies.** Their rapid diffusion and growth potential have been largely shaped by many factors, including increased deployments worldwide, mobile phone penetration, financial inclusion, and market demand for convenient, faster, and more economical means of payments. The design of risk-proportionate regulation has also been viewed as enabling innovations to help broaden financial services to underserved populations, while also being flexible enough to be tightened if their expansion could compromise financial stability (Dittus and Klein, 2011).

2. **Financial authorities have been faced with oversight challenges in protecting consumers and the payment system.** Such innovations have exposed grey areas in existing laws and regulations, and have led to legal reforms and the need to strengthen risk controls in some jurisdictions (Hong Kong, Kenya). In some cases, central banks temporarily suspended the use of mobile payments due to financial and information security concerns (China), or revoked operating licenses owing to failure to sustain business operations (Zambia). Their widespread deployment and heightened activity in some jurisdictions have raised policy issues, particularly the protection of customer funds. Such risks have been well highlighted by financial authorities, industry, and other global forums (AFI, 2014a; AFI, 2014b; Flood et al., 2013; Castri, 2013; Braun et al., 2008). They also point to the need to assess and mitigate potential risks, particularly in jurisdictions where oversight arrangements are weak or supervisory capacity is limited.

3. **Many central banks have made mobile payment regulations more explicit.** Recent regulatory developments, which is not exhaustive, has included the Central Bank of Brazil Law 12865 of 2013, which provides guidance on mobile payments, the Bank of Uganda Mobile Money Guidelines of 2013, the Central Bank of Sri Lanka Mobile Payments Guidelines for bank-led and custodian account based mobile payment services of 2011, the Da Afghanistan Bank Money Service Providers Regulation of 2008, the Reserve Bank of India Operative Guidelines for Bank Mobile Payments, and the Central Bank of Egypt Regulations Governing Provision of Payment Orders through Mobile Phones. Other central banks in Africa, Asia-Pacific, and Latin America have introduced similar rules.

4. **Development of effective oversight frameworks can help maintain public confidence and payment systems stability, particularly in low income countries (LICs) where mobile payments are seen as a major tool of financial inclusion.** This appears to have stimulated real economic activity in some countries (Kenya). However, the appreciation of such benefits should not allow risks to go unchecked, which should be addressed as part of the broader framework for regulating retail payment systems (RPSs) and instruments by the central bank or other relevant authorities such as the banking regulator. This may also involve cooperative oversight with other regulatory agencies such as the telecommunications regulator, competition authority, or consumer protection bodies. Many LICs are in the process of strengthening their oversight frameworks as part of wider efforts to modernize national payment systems and have received IMF technical assistance (TA). Such regulatory developments help ensure the safety and integrity of mobile payment deployments that have increased in some regions (Africa), and enhances financial sector surveillance (IMF, 2012).

5. **This paper examines oversight issues that underlie the potential growth and risks in mobile payments.** It builds on the General Principles for International Remittance Services, which was developed by an international task force (including the IMF) that has also served as a guidance for mobile phone remittance services regulation (CPSS and World Bank, 2007). It further supports ongoing international initiatives led by the CPSS and World Bank in this area, including efforts to examine the payment aspects of financial inclusion and the role of nonbanks in retail payments (CPSS, 2012; World Bank, 2012). The paper is organized as follows. Section II describes the concept of mobile payments, and reviews market potential and data initiatives. Section III discusses five major risks and oversight issues, including legal regime, financial integrity, fund safeguarding, operational resiliency, and payment systems. Section IV concludes with policy implications.

II. WHAT ARE MOBILE PAYMENTS?

A. Definitions

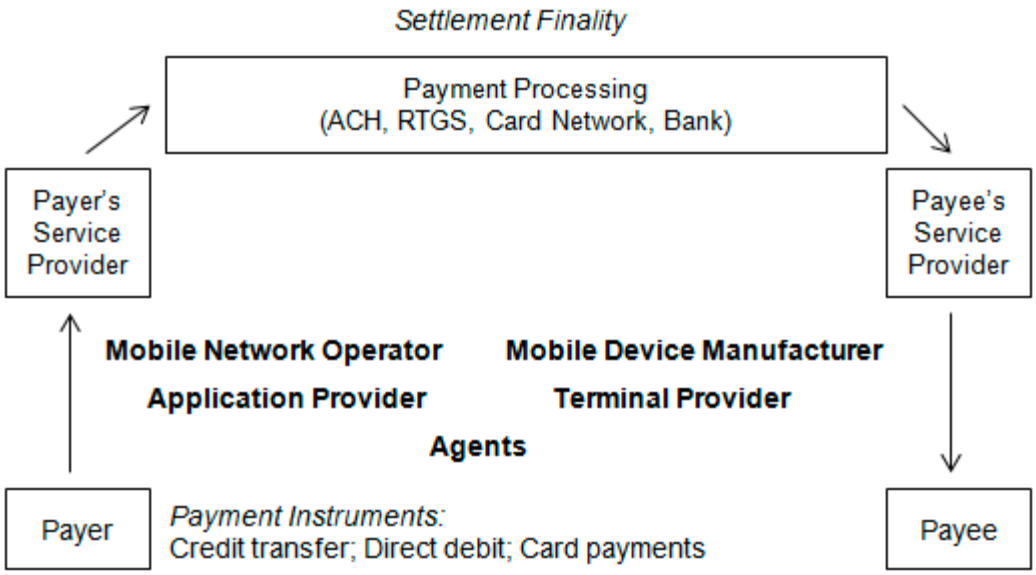
6. **Mobile payments may be defined as payments initiated and transmitted by access devices that are connected to mobile communication networks (CPSS, 2012).** Transaction values are small in amount and serve the purpose of purchasing goods or services at the point of sale, or remitting funds. Money originates from two major sources, including customer funds located at banks in the form of a deposit account or credit account (including prepaid cards), or customer "stored-value funds" maintained by mobile network operators (MNOs). In some jurisdictions, such accounts may also take the form of current account, card account, payment account, or transaction account. As such, mobile payments are funded by links to accounts or payment instruments (credit cards are not necessarily linked to an account), and are different in terms of risks. Customers can "pay in advance" (with a prepaid card, gift card, prepaid deposits with a MNO), "pay now" (with a debit card or bank account number), or "pay later" (with a credit card or phone bill).

7. **They differ from traditional payment systems.** Traditional payment systems are mainly account-based electronic payment services. This is dominated by financial institutions such as banks and payment card companies, where a payer requires a payment instrument (e.g. credit transfers, direct debit, or card payments) to initiate a transaction with an equipment (e.g. payment terminal) with financial information routed through their service provider. For finality, payments must be processed and settled. If the payer holds an account in a different bank from the payee, there is interbank settlement. In a traditional setting, banks that provide mobile payments could use an interbank payment system such as an automated clearing house (ACH), for which they are participants, to typically generate net settlement position files for later settlement. The ACH, in principle, should have risk controls to manage potential participant defaults. If interbank settlement is not needed, transactions are settled on an "on-us" basis by a designated settlement bank.

8. **New players are introduced in the traditional landscape (Figure 1).** New players include MNOs, mobile device manufacturers, application providers, terminal providers, and third party agents. This new environment is not dominated by financial institutions as the payer is not normally required to hold an account with a bank to make a payment transaction. MNOs can offer services for users to charge purchases directly to their payment cards that

have been pre-registered with the service. Other common services include *reverse charging* (payments for goods and services are placed as additional items on the customer's post-paid phone bill), *premium-rate services* (purchases are made by routing the purchasing call through a premium rate phone number), and *pre-paid air time* (direct payment for non-telephone items from third parties) (Allen, 2003). While mobile device manufacturers traditionally produce phones that may have payment functions, players such as terminal and application providers have also developed card readers and/or software that can be conveniently installed on mobile phones to offer similar payment capabilities (for example, Square and PayPal). Agents include any third party (such as retail outlets) acting on behalf of a bank to deal directly with a customer. This can help reduce the cost of delivering financial services to low-income and underserved populations vis-à-vis bank branches. They can also engage sub-agents if permitted under law. Cash merchants are a type of agent that only provides cash-in and cash-out services, and do not open accounts or process loans.

Figure 1. Mobile Payment System



Source: Author.

9. **There are five common methods to make a mobile payment.** They include use of (i) Short Message Services (SMS); (ii) Near Field Communications (NFC); (iii) Quick Response (QR) Codes; (iv) mobile applications; and (v) web browsers for mobile phones. Each method relies on mobile communication protocols that transmits financial messages. SMS uses standards that allow fixed line or mobile phone devices to exchange short text messages. The NFC is a set of standards for smart phones and similar devices to establish radio communication with each other by touching them together or bringing them into close proximity. This could be a NFC sticker attached to, or a chip embedded into, a mobile phone that provide contactless payments. QR Codes are matrix-like barcodes, which are readable through barcode/QR code readers and camera phones, and may be used for payment transactions. For web browsers, Wireless Application Protocol (WAP) is a technical standard for accessing information over a mobile wireless network where a WAP browser enables a

mobile device to access the Internet and effect payments. As of 2013, WAP browsers have not been widely used in Europe or the United States as most modern mobile phones now support internet browsers that use the hyper text markup language or HTML. Moreover, they are being substituted by emerging technologies such as iBeacon (which enables electronic devices or other hardware to send push notifications to other devices in close proximity) and Host Card Emulation (presentation of a virtual and exact representation of a smart card using only software). Unstructured Supplementary Service Data is a protocol used by GSM cellular telephones to communicate in a more responsive real-time connection with the service provider's computers. Banks also develop their own mobile phone applications and web browsers to support their customers.

10. **Modalities differ and are based on contractual relationships.** *Bank-based models* utlilize traditional intrabank or interbank payment networks. They include a direct contractual relationship between the licensed bank and customer where the bank offers individual accounts that can be used through its electronic channels. *Nonbank-based models* operate within a closed loop system where there is a contractual relationship between the customer and the nonbank, the issuance of electronic value for cash, and the holding of matched-value assets in a pooled account in a licensed bank. Variations between these two modalities include banks that offer individual accounts that are accessed through nonbank agent networks or technological platforms, or where a bank issues electronic value which is purchased from the bank and redistributed by nonbanks directly to customers. Such differences need to be clearly understood, distinguished, and communicated to consumers by financial authorities. Failing to do so may risk the unintended use of the term "mobile banking" in advertisements by MNOs, which is nonbank-based and not equivalent to a bank account. Globally, banks continue to have an active role in mobile payments with over half of the countries surveyed reporting mobile access to bank accounts (World Bank, 2011). The global share of mobile payments exceeds nonbanks by industry estimates, representing around 87 percent of total volumes in 2014 (Capgemini and Royal Bank of Scotland, 2013).

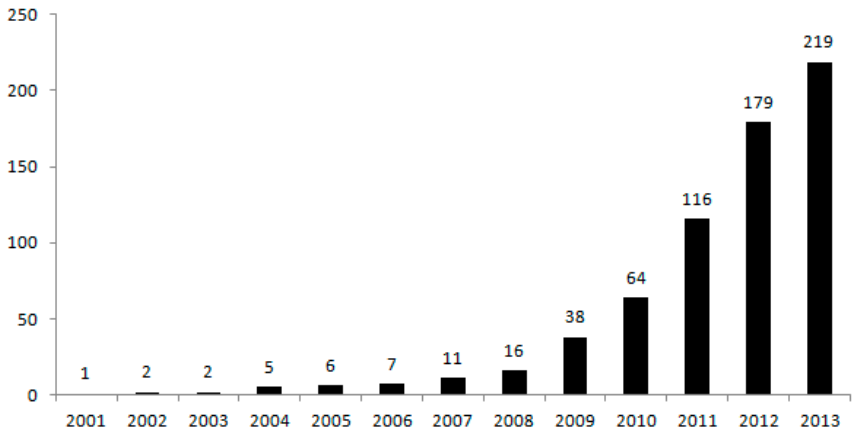
11. **Many mobile-related terms are in use, and there is a need to align them with terms set by the CPSS to establish universal definitions.** In fact, further work is needed in many areas of innovations in retail payments such as establishing definitions and updating the CPSS glossary (CPSS, 2012). Recent efforts have helped central banks and banking regulators establish a common understanding on the various forms of mobile innovations and harmonize regulatory approaches (AFI, 2012a). Commonly used terms in industry are as follows. *Mobile banking* is the use of a mobile phone to access banking services and execute financial transactions. This covers both transactional and non-transactional services, such as viewing financial information on a bank customer's mobile phone. The term mobile banking is often used to refer only to customers with bank accounts. Mobile banking is a type of electronic banking, which includes a broad array of electronic banking instruments and channels like the internet, point of sale terminals, and automated teller machines (ATMs). *Mobile financial services* share the same definition as mobile banking, but is distinguished with its coverage of mobile banking and mobile payments. *Mobile money* is defined as a mobile-based transactional service that can be transferred electronically using mobile networks. A mobile money issuer may, depending on local law and the business model, be a MNO or a third party such as a bank. It is often used synonymously with mobile financial services. *Mobile network operators* involve a company that has a government-issued license

to provide telecommunications services through mobile devices. MNOs are often referred to as a mobile phone operator or wireless service provider.

B. Market Potential

12. **Live deployments of mobile money services, an estimate of mobile payment market potential, reached 219 in 84 countries at the end of 2013 (Figure 2; Annex 1).**[2] Continued growth in global deployments during 2008-2013 coincided with the global financial crisis. This was partly driven by the need to adopt innovations to promote greater financial access, where over 2 billion adults were found to lack access to formal or semi-formal financial services and 1 billion people with mobile phones did not have a basic bank account (Access through Innovation Sub-Group, 2010). This was supported with the endorsement of the G20 Principles for Innovative Financial Inclusion at the Toronto Summit in June 2010 (Annex 2). Growth slowed down with a year on year increase of 22 percent between 2012 and 2013 as services became available in most developing markets.

Figure 2. Live Deployments of Mobile Money, 2001-2013



Source: Groupe Speciale Mobile Association (2014).

13. **GSMA views mobile money as use of the mobile phone to transfer money and make payments to the underserved for the purpose of its survey.** This is used to track deployments according to the following criteria: (i) the service must offer at least one of the following services: person-to-person transfer, bill payment, bulk payment, merchant payment, and international remittance; (ii) the service must rely heavily on a network of transactional points outside bank branches that make the service accessible to unbanked and under banked people. Customers must be able to use the service without having been previously banked. Services that offer the mobile phone as just another channel to access a

[2] The Groupe Speciale Mobile Association (GSMA), a grouping of mobile operators and related companies that support the standardization, deployment and promotion of the GSM mobile telephone system, surveys and closely monitors live and planned deployments of mobile money services worldwide (GSMA, 2014). See updated figures on live and planned deployments at: http://www.gsma.com.

traditional banking product are not included; and (iii) the service must offer an interface for initiating transactions for agents and/or customers that is available on basic mobile devices.

14. **A majority of deployments are in Sub-Saharan Africa (52 percent).** This compares to other regions as follows: South Asia (16.1 percent); East Asia and the Pacific (11.5 percent); Latin America and the Caribbean (13.3 percent); Middle East and North America (6 percent); and Europe and Central Asia (1.4 percent). Global Findex Database findings support this trend, having found that 16 percent of adults in Sub-Saharan Africa used a mobile phone in the past 12 months to pay bills or send or receive money (Demirguc-Kunt and Klapper, 2012). This compares with less than 5 percent in all other regions.[3]

15. **Mobile money accounts and transactions have grown worldwide (Table 1).**[4] Based on June 2013 data, there were 60 million active users out of 203 million registered mobile money accounts. Usage is measured by the initiation of at least one transaction through the account within the last 90 days. There were 326 million transactions whose values amounted to 3.2 billion U.S. dollars. These figures would increase to 431 million transactions totaling 7.4 billion U.S. dollars if cash-in and cash-out items are included. Such services mainly covered bill payments, person-to-person transfers, bulk payments, value storage (with or without interest), credit, or insurance, and largely relied on a network of transactional agents beyond bank branches.

Table 1. Number of Registered Mobile Money Accounts

Mobile Money Account/100,000 Adults	Total	East Asia and Pacific	Europe and Central Asia	Latin America and Caribbean	Middle East and North Africa	South Asia	Sub-Saharan Africa
June 2011	1,542	1,067	63	319	924	578	12,024
June 2012	2,315	1,387	75	878	2,729	1,445	15,832
June 2013	4,361	1,657	416	2,165	15,164	3,485	24,652

Source: Groupe Speciale Mobile Association (2014).

16. **Mobile money accounts outnumbered bank accounts in 9 countries, and could further increase if unregistered users were included.** These countries are located in Sub-Saharan Africa and include Cameroon, the Democratic Republic of Congo, Gabon, Kenya, Madagascar, Tanzania, Uganda, Zambia, and Zimbabwe. The GSMA 2013 survey also

[3] A few economies were noted as exceptions, including Albania, Algeria, Haiti, the Philippines, and Tajikistan.

[4]The GSMA defines mobile money accounts as '"an e-money account that is primarily accessed using a mobile phone that is held with the e-money issuer. In some jurisdictions, e-money accounts may resemble conventional bank accounts, but are treated differently under the regulatory framework because they are used for different purposes (for example, as a surrogate for cash or a stored value that is used to facilitate transactional services).')". The GSMA's June 2012 survey found nearly 30 million active users (from 81.8 million registered users), transaction volumes of 224.2 million, and transaction values of 4.6 billion U.S. dollars.

identified 17.3 million unregistered mobile money users where 4 services had more than 1 million unregistered users. Around 13 percent of mobile money services were found to be delivered mainly over-the-counter. This involves the agent performing transactions on behalf of customers who do not need to register to use the service.

17. **There were 6.8 billion mobile-cellular subscriptions with a penetration rate of 96 percent globally in 2013, which may further drive mobile payments.** This means that there are almost as many mobile-cellular subscriptions as people in the world (although one person may have more than one mobile phone subscription in practice). Over half of these subscribers (3.5 billion out of 6.8 billion total subscriptions) are in the Asia-Pacific region. However, as global penetration rates reaches saturation level, growth rates have also fallen to their lowest levels in both developed and developing economies. There were also 2.1 billion mobile broadband subscriptions, which experienced an average annual growth rate of 40 percent between 2007 and 2013. Africa has been the region with the highest growth rates over the past three years with mobile-broadband penetration at 11 percent in 2013.

C. Data Initiatives

18. **The lack of official statistics increases reliance on market surveys, making actual estimates of market size and growth difficult.** Apart from GSMA surveys, other industry estimates suggests that the global market for mobile payments could reach 721 billion U.S. dollars by 2017 (Gartner, 2013). This is based on a compounded annual growth rate of 35 percent. Others, using a readiness index, suggest that mobile payments have yet to reach a large share of the payments mix and note the leading country as Singapore (MasterCard, 2012). As noted, the underlying payment instrument used to make a mobile payment may vary from the use of debit cards, credit cards, store valued cards, credit transfer, direct debits, and online transfers (CPSS, 2004).[5] Such differences have existed for electronic money, but efforts were reached for a common definition to help collect and compare cross-country data (CPSS, 2012).[6] As a result, mobile payments have been defined as part of electronic money where value is stored electronically in a device such as a chip card or a hard drive in a personal computer, and also on servers or mobile phones (CPSS, 2013).

19. **Remittance flows, which are recorded in the IMF Balance of Payments statistics, provide another view of market potential.** Mobile payments provide a convenient channel for many economic migrants who lack access to the formal financial system and need to remit funds overseas. Remittance flows are projected to reach over 700 billion U.S. dollars by 2016, and were 3 times the size of official development assistance and larger than private

[5] The survey on developments in electronic money and Internet and mobile payments was based on information from participating central banks and monetary authorities in 95 countries and territories.

[6] CPSS statistical methodology captures mobile payments as electronic money storage under settlement media used by nonbanks. This is defined as instruments for storing electronic money funds that reside in cards, personal computers or servers (computer-based, of which software- or network-based) or other devices like mobile phones (mobile-based, with the funds stored locally on a mobile phone). The recording of card payments with cards issued in the country does not include electronic money transactions and mobile payments. Mobile payments are also not included in the collection of other payment instruments, unless specified otherwise.

debt and portfolio equity flows to developing countries. This exceeded foreign exchange reserves for some countries. The measurement of remittance flows have been refined with changes introduced in the Sixth Edition of the IMF Balance of Payments and International Investment Position Manual, which includes a new definition for personal remittance that includes two main components on personal transfers and compensation of employees.[7] However, IMF balance of payment statistics have been unavailable for some countries. While central banks report remittance flows from commercial banks, this has excluded data from money transfer operators, post offices, and mobile money transfer operators. Such reporting have also not been practiced in countries, and therefore, not captured in official statistics.

20. **The IMF Financial Access Survey (FAS) is a recent initiative in response to calls for greater financial inclusion by the G20.** Following endorsement of the G20 Basic Set of Financial Inclusion Indicators at the Los Cabos Summit in June 2012, the IMF FAS has served as the new data source on basic consumer financial services worldwide. This major effort has been the collaboration between the IMF, the Consultative Group to Assist the Poor, and the International Finance Corporation. Such data helps support the mandates of financial regulators tasked with promoting access to financial services in addition to ensuring the stability of financial markets. However, IMF FAS data focuses on data collection from financial service providers such as banks and microfinance institutions, but does not include other providers such as MNOs and third-party providers, including data from their respective agent networks (Ardic et al., 2013).

21. **The Alliance for Financial Inclusion (AFI) has also developed a more harmonized approach in the regulatory reporting of mobile payments for central banks and banking supervisors.** AFI comprises of central banks and other financial regulatory institutions from over 90 developing countries. The AFI's Mobile Financial Services Working Group has established minimum data and information requirements in four major areas, including risk management frameworks and data needs for risks relating to operations, liquidity, money laundering, and terrorist financing; consumer protection; public disclosure of information; and outreach and financial inclusion (AFI, 2012b). Guidelines are also available to measure access and usage indicators for mobile financial services (AFI, 2013). A Financial Inclusion Data Working Group is also dedicated to develop a common framework for members in measuring financial inclusion, and aims to promote its use in the broader international context. The African Mobile Phone Financial Services Policy Initiative, a grouping of 18 African regulatory institutions, was also set up with AFI support. AMPI has been instrumental in identifying solutions that can be implemented or promoted by regulators, policy makers and the private sector in scaling up mobile financial services access and usage in Africa.

[7] Personal transfers comprises of "all current transfers in cash or in kind made or received by resident households to or from nonresident households". Compensation of employees "represents remuneration in return for the labor input to the production process contributed by an individual in an employer-employee relationship with the enterprise." Capital transfers between households is also included under this new definition, but data on this item are difficult to obtain and hence reported as missing for almost all countries.

III. Risks and Oversight Issues

22. **This section focuses on five key risks issues—legal regime, financial integrity, fund safeguarding, operational resiliency, and payment systems—which have implications for the development of an effective oversight framework for new payment methods, including mobile payments.** A delicate balance is needed between development and stability objectives, which can include issues on competition, consumer protection, and interoperability. Financial authorities are faced with the challenge to protect public confidence and financial stability when diffusion becomes more widespread. For jurisdictions where there is limited capacity to supervise third party cash agent networks (who provide cash-in and cash out services), promote financial literacy, and encourage competition, this poses further issues to the central bank and other related authorities.

A. Legal Regime

23. **Legal uncertainty exists if mobile payment services are unlicensed.** A recent survey found that mobile phone operators or telecommunication companies that provide payment services in less than half of sample countries undergo licensing (World Bank, 2011). This was more apparent in the East Asia Pacific and European regions. Unlicensed service providers may provide a potential for abuse, particularly amongst those who are poor and vulnerable. Licensing regimes have sought to promote competition and innovation in some jurisdictions by setting initial capital requirements for nonbanks that are proportionate to their risk. For example, the initial capital requirement for European Union (EU) e-money institutions was lowered from 1 million euros to 350,000 euros to provide a lighter supervisory regime under Directive 2009/110/EC.

24. **Legal uncertainty may also arise if multiple laws and authorities are involved, making the understanding of the overall legal framework necessary.** The legal and supervisory framework in some jurisdictions may be fragmented, involving both financial and nonfinancial legislation on electronic funds transfers, consumer protection, data protection, deposit insurance, anti-money laundering, electronic transactions, exchange control, and financial transactions reporting. For example, the United States legal framework for mobile payments encompasses up to 8 laws or regulations (Drozdowski, 2012), including: Electronic Fund Transfer Act (Regulation E); Truth in Lending Act (Regulation Z); Truth in Billing; Unfair, Deceptive, or Abusive Acts or Practices under the Federal Trade Commission Act; Unfair, Deceptive, or Abusive Acts or Practices under the Consumer Financial Protection Act; Gramm-Leach-Bliley Act privacy and data security provisions; and Federal Deposit Insurance or National Credit Union Administration Insurance. The recent request for information on mobile financial services from the Consumer Financial Protection Bureau (CFPB), which oversees all consumer financial markets in the United States, reflects some concerns on customer service, security, and privacy issues despite the benefits. It also highlights the need for coordination amongst the relevant authorities, including the U.S. Federal Reserve, the Federal Deposit Insurance Corporation (FDIC), and CFPB.

25. **Mobile payment rules can fall under existing financial laws that help categorize the type of payment service providers.** This helps to identify the responsibilities of authorities in regulating and supervising retail payments, including mobile payments, which

may fall under the central bank or banking regulator. The scope of oversight could vary from RPSs, retail payment instruments, and retail payment services provided by banks and nonbanks. For example, the EU Electronic Money Directive and Payment Services Directive (PSD) provides a uniformed approach in establishing the rules for electronic money institutions and payment institutions, which can be illustrated by the categorization and scoping of payment service providers in Norway (Norges Bank, 2013) (Box 1).

Box 1. Norway: Payment Service Provider Categorization and Key Legislation

The Act relating to Financing Activities and Financial Institutions (Financial Institutions Act) of Norway establishes the different types of payment service providers. This includes: (i) credit institutions (banks and mortgage companies), (ii) payment institutions, (iii) electronic money institutions, (iv) post office giro institutions, (v) the central bank, (vi) Norwegian state, municipalities, and country authorities when not acting in their capacity as public authorities, and (vii) telecommunication providers. The key providers include:

Credit institutions, which are mainly banks permitted to take deposits from the public and grant credit, and are protected by deposit guarantees. Mortgage companies are also credit institutions, but may accept only other repayable funds and not deposits. Credit institutions fall under the Act relating to Savings Banks, Act relating to Commercial Banks, and Act relating to Financing Activities and Financial Institutions.

Payment institutions (which include mobile payments providers) are prohibited from taking deposits or other repayable funds where client funds must be held in a separate account (client account) by such institutions. As they are not treated as deposits, they are not covered by deposit guarantees. Payment institutions are required to place customer funds in a client account in a bank or invested in safe, liquid low-risk assets determined by the financial regulator. They are granted either ordinary or limited authorization with the latter category requiring lesser initial capital and own funds. Payment institutions are regulated by the Act relating to Financing Activities and Financial Institutions, and Regulation relating to Payment Institutions.

Electronic money institutions are also prohibited from taking deposits or other repayable funds where client funds must be held in a separate account (client account). They are also not covered by deposit guarantees. Electronic money institutions are subject to higher initial capital and own-funds requirements. Electronic money institutions are governed by Chapter 4c of the Act relating to Financing Activities and Financial Institutions, and Regulation relating to Electronic Money Institutions.

Telecommunication providers currently do not require authorization as a payment institution or electronic money institution as long as the MNO does not act solely as an intermediary and provides limited payment solutions (for example ring tones and directory enquiry services). Otherwise, it needs to obtain the appropriate license to offer payment solutions for physical products and services (vending machines, purchase of books and films delivered to a mobile device). Telecommunication providers fall under Section 11 (2) m of the Financial Contracts Act.

Source: Norges Bank.

26. **Legal reforms to strengthen safeguards for consumers and the payment system are under review in some advanced economies.** In Hong Kong, the growth in the size and significance of stored-value facilities (SVFs), including mobile payments, and retail payment systems (RPSs), have led the Financial Services and the Treasury Bureau and the Hong Kong Monetary Authority (HKMA) to propose amendments to the Banking Ordinance and Clearing and Settlement Systems Ordinance (Box 2) (HKMA, 2013). Under proposed amendments, SVFs fall under two major classifications. First, SVFs can be either multi-

purpose or single-purpose. Multipurpose SVFs are used as a means of payment for goods and services provided by participating merchants (similar to an electronic surrogate for coins and banknotes). Single-purpose SVFs can only be used as a means of prepayment for goods and services provided by a merchant who is also the issuer of the SVF. Second, SVFs can be device-based or non-device based. Device-based SVFs include stored value cards and other stored value physical devices (e.g., watches). Non-device based SVFs normally have their value stored on a computer network-based account or a mobile network-based account rather than on a physical device.

27. **Similar SVF guidelines were introduced by the Monetary Authority of Singapore (MAS) in June 2006.** This defines it as a facility that is used for payment of goods or services up to its stored value, and makes references to security guidelines for mobile banking and payments. MAS SVF Guidelines establishes 4 major stakeholders (user, holder, operator, and merchant) for a SVF, and lays down 5 key principles, including timely redemption, security and reliability, rights and responsibilities, disclosure, and prevention of money laundering and terrorist financing. It also serves as the minimum standards, and requires prospective SVFs to further comply with all relevant laws and regulations, particularly the Payment Systems (Oversight) Act of 2006.

28. **The European Commission is also reviewing the PSD in response to changes in the card, internet and mobile payments landscape (EC, 2012).** This effort to modernize the legislative framework for retail payments has focused on three main issues (Norges Bank, 2013). First, the merger between the PSD and the Electronic Money Directive, which does not appear to be practicable at this stage as some member countries have not yet adopted the latter directive. Second, the elimination of certain exemptions, particularly for telecommunication providers, in the PSD. And third, expanded access to regulated payment systems, which may pose legal and practical issues that may require further amendments to the Settlement Finality Directive. As of June 2014, amendments to the PSD have not yet been enacted.

29. **A sound legal basis helps establish an effective oversight framework to monitor and mitigate potential risks, and balances development versus stability objectives.** This identifies the sources of central banks' oversight responsibilities and powers, which can include treaties, statutes, regulations, or other documents external to the central bank (CPSS, 2005). As such, mobile payments form part of wider efforts to conduct the oversight of RPSs and instruments. There are 5 general principles that central banks should consider in developing effective oversight arrangements, which include: (i) setting out publicly oversight policies, including the policy requirements or standards for systems and the criteria for determining which systems these apply to; (ii) adopting, where relevant, internationally recognized standards for payment and settlement systems; (iii) ensuring adequate powers and capacity to carry out oversight responsibilities effectively; (iv) applying oversight standards consistently to comparable payment and settlement systems, including systems operated by the central bank; and (v) cooperating with other relevant central banks and authorities to promote the safety and efficiency of payment and settlement systems.

Box 2. Hong Kong: Stored-Value Facilities and Retail Payment Systems Regulation

Proposed amendments to the Clearing and Settlement Systems Ordinance is aimed at introducing a mandatory licensing regime for SVFs, establishing a designation regime to empower the central bank to designate and oversee RPSs that are important to the general public and financial stability, and empowering the central bank with supervisory, oversight, and investigative authority over SVF licensees and RPSs. This will broaden the regulatory regime for multi-purpose cards to emerging non-device based (non-card based) products and services.

Licensing Regime for SVFs

Criteria: The issuance of a SVF without a license will be considered an offence in Hong Kong. Licensing criteria includes: (i) *Physical presence.* The company must be incorporated under the laws in Hong Kong, with a local registered office; (ii) *Principal business.* The principal business must be for the issuance of multi-purpose SVF; (iii) *Adequate financial resources.* On-going minimum (paid up) capital requirement of HK$25 million; and (iv) *Other licensing conditions*. For example, fit and proper requirements on management and ownership, prudential and risk management requirements, AML/CFT requirements, purpose and soundness of scheme, restrictions on business, higher capital requirements, or others.

Exemptions: Under current practices of the Banking Ordinance, licensed banks are considered licensed. Licensing exemptions applies to single-purpose SVFs as they are similar to prepayment for specific goods and services provided by the issuer rather than electronic surrogate for coins and notes, and certain SVFs if it poses minimal risk to the users or the payment and financial systems of Hong Kong.

Float: Float must be managed by segregation from the SVF issuer's own funds and at least 100 percent protected by safeguarding measure such as a guarantee from a licensed bank in Hong Kong, or the establishment of a trust account with a licensed bank in Hong Kong. Investment of float must be discussed with the HKMA in advance.

Limits: The HKMA may impose a limit on the maximum value that can be stored on a SVF on a case-by-case basis by attaching a licensing condition. In line with the existing treatment under the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance, SVF licensees are required to comply with customer due diligence and recordkeeping requirements with stored value limit over HK$3,000.

Designation Regime for RPSs

Eligibility: RPSs that operate and provide retail payment services in Hong Kong; or process Hong Kong dollar or other prescribed currencies (e.g. RMB/USD).

Criteria: A RPS may be designated if any disruptions to the RPS have implications to the monetary or financial stability of Hong Kong; public confidence in payment systems or the financial system of Hong Kong; or day-to-day commercial activities in Hong Kong.

Coverage: This potentially includes: credit card schemes, debit card schemes, merchant acquirers, payment gateways, and mobile payment infrastructures.

Requirements: Safety and efficiency requirements (similar to the existing CSSO, e.g. sufficient expertise commensurate with its business schemes, measures to ensure data integrity, appropriate contingency measures, proper risk management controls, etc). Proper operating rules in place (e.g. soundness of system operations, relevant default arrangements, etc). Exemption of designated RPS established outside Hong Kong from certain requirements if it is already subject to adequate supervision by the home regulator.

Source: Hong Kong Monetary Authority

30. **Authorities' oversight responsibilities are reiterated in the new international standards for financial market infrastructures and provide a general framework to further assess risks and responsibilities (CPSS-IOSCO, 2012).** Although the new standards primarily apply to systemically important payment systems and other major FMIs (securities settlement systems, central securities depositories, central counter parties, and trade repositories) they provide a general framework to assess potential risks in mobile payments and the responsibilities of relevant authorities (Annex 3). Some central banks have already considered the application of a lighter approach of the CPSS-IOSCO Principles for Financial Market Infrastructures (PFMIs) to RPSs, which will balance the need for safety and efficiency against the demand for accessible and affordable financial services for the unbanked population (India). Further steps include establishing oversight objectives, standards, institutional arrangements (e.g. oversight unit for mobile payments in the central bank), and collaboration frameworks between different authorities (e.g. memorandum of understanding between the central bank and banking regulator) at both domestic and international levels (for cross-border mobile payments). For example, virtual currency schemes have been assessed for their potential legal, liquidity, operational, and credit risks using earlier standards for systemically important payment systems (ECB, 2012). Also applicable are the General Principles for International Remittance Services, which provide a good oversight framework for mobile payments (CPSS and World Bank, 2007).

B. Financial Integrity

31. **From the financial integrity perspective, mobile payments may be considered a good tool for reducing reliance on the use of anonymous cash, especially in countries that are predominantly cash-based.** Mobile payments are generally more traceable than cash and can be made subject to transaction monitoring and restrictions. However, mobile payments do increase complexity and give rise to money laundering and financing of terrorism risks as such services are often distributed by a much wider range of service providers, including nonbank service providers and their agents than the more traditional payment methods provided by banking institutions. This may create regulatory challenges in determining where to place appropriate responsibility for AML/CFT controls. The Financial Action Task Force (FATF) "Guidance for a Risk-Based Approach, Prepaid Cards, Mobile Payments and Internet-Based Payment Services" of 2013 provides guidance to countries as to which entities could be considered the responsible party (or parties), and therefore subject to AML/CFT regulation (FATF, 2013; FATF, 2010). In addition, the FATF standard (AML/CFT international standard) provides room for flexibility, enabling countries to craft effective and appropriate controls without compromising financial inclusion.

32. **AML/CFT risks must be adequately addressed.** Such risks may stem, among others, from lack of face-to-face relationships, customer identification and verification, and checks on funding sources; difficulty in compiling or aggregating transactions across different agents; geographical reach; access to cash through prepaid cards; involvement of non-traditional players (such as telecommunication companies) and their agents which may not be regulated for AML/CFT purposes, or regulated at a lower level than banking institutions, and absence of obligation for the providers and agents to detect and report suspicious activity.

33. **The effective and proportionate application of the AML/CFT framework would help mitigate the risks associated with mobile payment systems.** Given the potential for financial inclusion, regulators should seek to strike a balance between addressing the AML/CFT risks and promoting innovation. The FATF Recommendations support the development and implementation of a risk-based approach to AML/CFT. Countries, financial institutions and other entities should identify, assess and understand the risks that may arise by mobile payments before establishing their measures. This is an essential step in the process, which enables financial institutions and other entities to ensure that an effective and proportionate framework is in place to subject players and agents involved in money transmission to AML/CFT regulation and supervision. In this context, countries could require financial institutions and other entities to perform appropriate mitigating measures such as customer due diligence, record keeping, transaction monitoring and suspicious activity reporting, placing limits to loading, value and geographical reach, and restricting the sources of funding.[8]

C. Fund Safeguarding

34. **Customer funds held by nonbanks may be at risk if unprotected.** Experience in advanced economies suggests that such protection can be a grey area, particularly where mobile payments are linked with prepaid phone deposits or phone bills where the wireless carrier may provide voluntary protections (against fraud, theft, or errors) that are normally not disclosed in customer contracts (United States House of Representatives, 2012; Martindale and Hillerbrand, 2011; Hillerbrand, 2008). This contrasts with traditional credit and debit cards, which have clear mandatory protections.

35. **Many low to moderate income households are vulnerable to financial losses if risks controls for mobile payments are weak, which could be a major issue for LICs.** Such shortcomings may pose risks to protecting customer funds if there is the failure of a nonbank payment service provider. In LICs, customers that are deemed most in need of protection could extend beyond retail and small business depositors to the unbanked population. Thus, requirement for an insurance policy or some other comparable guarantee from an insurance company or a credit institution, which does not belong to the same group as the nonbank payment service provider itself, provides some level of protection. This is specifically illustrated by fund safeguarding provisions in the EU PSD (Box 3). A survey on innovative retail payment products found that customer funds were fully protected in about 60 percent of cases (World Bank, 2012).[9] While one third of the innovative retail payment products surveyed (including mobile payments) were protected by deposit insurance, only

[8] See Chatain et al., 2011 for a discussion on international experiences in implementing AML/CFT measures.

[9] The survey on customer fund protection for173 innovative retail payment products (including mobile payments) identified the following: 20 percent has no protection; 36 percent reported the balance in the account is covered by a deposit insurance scheme; 22 percent noted that the issuer is required by the law or a regulation to fully back up the monetary value; 14 percent noted that the issuer is required by the law or a regulation to partially back up the monetary value issued with a deposit in an account or other assets; 23 percent reported specific capital requirements for the issuer; and 17 percent has other types of protection mechanisms.

25 percent were fully backed by deposits (which remains risky) and around one-fifth of the innovations were not protected. As the survey results did not distinguish between the type of product, and bank versus nonbank issuers, it is difficult to pinpoint precisely the concentration of potential risks from nonbank mobile payment schemes.

36. **Mobile payments are SVFs and are different from deposits.** Existing deposit insurance schemes would normally cover mobile payment services provided as part of banking services (e.g., through a smart phone application) and linked to a customer's account in a bank that is licensed and subject to prudential regulation. Deposit insurance normally covers potential losses from bank insolvency (and not the loss of card, chip, etc) and may be subject to limits. This is not necessarily the case for nonbank payment service providers, which can involve an issuer of electronic money (which is not treated as deposits) whose monetary value is stored on an electronic device such as a chip, prepaid card, mobile phone, or computer system (Tarazi and Breloff, 2010).

37. **Deposit insurance laws differ or may be less common across jurisdictions.**[10] Moreover, while deposit insurance protects some parts of customer funds in the event of failure of a depository or credit institution, such schemes may not apply for nonbank entities. For example, U.S. Federal Deposit Insurance or National Credit Union Administration Share Insurance provides protection for funds underlying a mobile payment that are deposited in an account covered by deposit insurance or share insurance up to an applicable limit, but does not guarantee that customers funds will be protected following a bankruptcy or insolvency of a nonbank entity in the mobile payment chain (Drozdowski et al., 2012). Such exclusions were found in some advanced economies where the deposit insurance system does not cover nonbank institutions that take deposits from the public and also participate in the national payment system (FSB, 2012). This has led to the licensing of the postal operator as a bank in order for it to protect its deposits (Switzerland). To avoid adverse implications in times of stress, international standards suggest that such nonbank entities should not take deposits from those that are deemed most in need of protection or should be included in the deposit insurance system. This is to observe Principle 8 (Compulsory Membership) of the Core Principles for Effective Deposit Insurance Systems, which states "membership in the deposit insurance system should be compulsory for all financial institutions accepting deposits from those deemed most in need of protection (such as retail and small business depositors) to avoid adverse selection." (BCBS -IADI, 2009). This may, however, discourage financial inclusion if there are no alternatives to deposit-taking, particularly in LICs. Deposit insurance, however, are normally provided on a limited basis up to a nominal amount, and may create distortions, moral hazard, and other costs. Therefore, its extension to nonbank mobile payment service providers such as MNOs needs to be carefully assessed.

[10] Surveys have found that 75 percent of high income countries offered deposit insurance with limits as compared to LICs at 16 percent (Demirguc-Kunt et al., 2008). Deposit insurance was widespread in Europe and Latin America, but less common in the Middle East (29 percent) and sub-Saharan Africa (11 percent).

Box 3. European Union: Fund Safeguarding in the Payment Services Directive

Article 9 states: "The Member States or competent authorities shall require a payment institution which provides any of the payment services listed in the Annex and, at the same time, is engaged in other business activities referred to in Article 16(1)(c) to safeguard funds which have been received from the payment service users or through another payment service provider for the execution of payment transactions, as follows:

- they shall not be commingled at any time with the funds of any natural or legal person other than payment service users on whose behalf the funds are held and, where they are still held by the payment institution and not yet delivered to the payee or transferred to another payment service provider by the end of the business day following the day when the funds have been received, they shall be deposited in a separate account in a credit institution or invested in secure, liquid low-risk assets as defined by the competent authorities of the home Member State;

- they shall be insulated in accordance with national law in the interest of the payment service users against the claims of other creditors of the payment institution, in particular in the event of insolvency; and

- they shall be covered by an insurance policy or some other comparable guarantee from an insurance company or a credit institution, which does not belong to the same group as the payment institution itself, for an amount equivalent to that which would have been segregated in the absence of the insurance policy or other comparable guarantee, payable in the event that the payment institution is unable to meet its financial obligations."

Source: European Commission Payment Services Directive.

38. **"Pass through" deposit insurance has been introduced in the United States.** Basically this extends the protection of bank deposits in existing deposit insurance laws to funds in stored value facilities, including mobile payments. However, such application is subject to the definition of "deposits" in existing legislation and the fulfillment of conditions such as the establishment of custodial relationships, and the recording of identities and amount of funds of each actual owner (Box 4). From a competition perspective, such criteria help establish a functional equivalence for similar services that may have deposit features and make them eligible for participation in the deposit insurance scheme.

39. **Similar "pass through" provisions are under consideration in the deposit insurance law of Kenya.** This follows the enactment of the Kenya Deposit Insurance (KDI) Act in 2012, which established the Deposit Insurance Fund to replace the Deposit Protection Fund. The Kenya Deposit Insurance Corporation (KDIC) also succeeds the former Deposit Protection Fund Board. Under the authorities' "Derived Protection Model" principle, third party beneficiaries of funds that are held under a trust account operated for and on their behalf by a MNO, for example, are entitled for compensation to limited amounts under the deposit insurance law. This is subject to the condition that the MNO has identified itself to be a trustee, acting in a fiduciary capacity, for and on behalf of certain identifiable beneficiaries. Kenya is in the process of enacting and implementing statutory laws to operationalize such provisions. Section 29 of the KDI Act specifically provides cover to entities that manage trust accounts. KDI Regulations of 2013 (Regulation 9) also addresses issues on trust accounts in which attendant rights and duties of parties are established, including (i) the definition and nature of a trustee account; (ii) the inherent parties entitled to manage, operate, and benefit from the operation of a trustee account; and (iii) the attendant rights and duties

pertaining to the deposit insurer, bank/financial institution, trustee and beneficiary in matters relating to the account. As such, the KDIC, as deposit insurer, would need to monitor innovations (trust accounts), develop regulations to help maintain public confidence and financial stability, and implement updated off-site risk assessment methodologies to examine the exposure level of the insurance fund. This may imply the need to assess the daily, weekly, monthly, and annual fluctuations in such accounts, and the eventual exposure to the deposit insurer.

Box 4. United States: "Pass-Through" Deposit Insurance

The FDIC's Notice of New General Counsel's Opinion No. 8 (November 13, 2008) establishes that all funds underlying stored value products and other nontraditional access mechanisms will be treated as "deposits" to the extent that the funds have been placed at an insured depository institution. As a result, all such funds will be subject to FDIC assessments. Also, all such funds will be insured up to the insurance limit.

The FDIC is entitled to rely upon the account records of a failed insured depository institution in determining the owners of deposits. In cases in which a separate account has been opened in the name of the holder of the access mechanism, the FDIC will recognize the holder as the owner of the deposit.

In some cases, in an agency or custodial capacity, the distributor of the access mechanisms (or agent on behalf of the distributor) might open a pooled account for all holders of the access mechanisms. In such cases, the FDIC may provide "pass through" insurance coverage (coverage that passes through the agent to the holders). Such coverage is not available, however, unless 3 conditions are satisfied, including:

- ***Custodial relationship disclosure:*** The account records of the insured depository institution must disclose the existence of the agency or custodial relationship.
- ***Identity and funds disclosure:*** The records of the insured depository institution or records maintained by the custodian or other party must disclose the identities of the actual owners and the amount owned by each such owner.
- ***Actual ownership:*** The funds in the account actually must be owned (under the agreements among the parties or applicable law) by the purported owners and not by the custodian (or other party).

If these 3 requirements are not satisfied, the FDIC will treat the custodian (the named accountholder) as the owner of the deposits. Then the deposit account will be treated as one account and only covered up to the limit of 250,000 U.S. dollars. In other words, the deposit insurance would cover only the insured amount of the total deposit and not the eligible amounts for each individual beneficiary.

Source: Federal Deposit Insurance Corporation.

40. **Financial authorities should consider adopting fund safeguarding measures even when such protection may not be explicitly covered in existing deposit insurance or payment laws.** Some of these measures include:

- ***Usage restrictions:*** Restricting customer funds for money transfers and prohibiting use for other purposes such as extending credit (which makes such schemes similar to a bank) or covering operating expenses of the nonbank entity. Introducing liquidity requirements

for nonbank mobile payment schemes, which should include limiting the liquid asset categories to be held that are equivalent to the total value of customer funds collected;[11]

- ***Protection requirements:*** Insulating customer funds against the claims of other creditors of the nonbank in the event of its insolvency. Introducing insurance or comparable guarantees of electronic values for nonbank mobile payment schemes. Adopting mechanisms to guarantee traceability of customer funds in the event of mass conversion of electronic values to cash, or potential nonbank failure; and

- ***Float management:*** A segregated trust account is held by a third party with a licensed and prudentially regulated bank. Maintaining multiple accounts at different banks to diversify risks. Holding of other forms of safe assets such as government securities.

D. Operational Resiliency

41. **Operational risks can undermine public confidence.** Recent operational disruptions to mobile banking services and telecommunication networks in advanced economies illustrate how public confidence in mobile payments could be undermined.[12] The potential risks faced by consumers could be higher in LICs, if there is the lack of effective oversight arrangements, limited supervisory capacity, and weak risk mitigation measures. Some of the reasons for operational disruptions stem from capacity constraints, antiquated technologies, or differences in technology platforms following a bank merger, acquisition, or separation. Business continuity plans are particularly important in jurisdictions where mobile devices are largely used to access financial services and communication networks are prone to natural disasters. Recent failure to sustain business operations under existing payment laws has led some central banks (Zambia) to revoke operating licenses. Future challenges include ensuring that mobile network capacities can cope with the rise in demand for communication and payment needs, and preventing potential systemic risks from operational disruptions that may result from their greater dependency in making payments.

42. **Cyber risk, which is a potential source of systemic risk that has wide economic impact, is an emerging issue faced by financial authorities.** Such risks involve possible

[11] This contrast with the financial intermediation role of banks, which need to fulfill reserve and liquidity requirements with a small portion of total deposits kept in liquid form (cash) for potential depositor claims.

[12] Royal Bank of Scotland customers were unable to access mobile banking services on the morning of May 24, 2013 due to computer failures. Around 2 million customers have such applications on their smart phones and tablet computers (for example, this could include postpaid payments for purchasing small items such as ring tones, apps, virtual goods, or online games). This followed earlier problems during June and July 2012 that left 17 million customers without access to their accounts for up to 3 weeks. The bank had to pay compensation cost of 175 million pound sterling. TSB Bank experienced a temporary glitch to its Internet banking services in the morning of September 9, 2013, after its separation from Lloyds Banking Group but continued to use its mobile and online banking platforms. O2, a U.K. mobile operator, had to pay compensation after its network failed for 3 days and affected 7 million customers in July 2012. Another outage occurred in the same year during October, making 10 percent of the operator's 23 million customers unable to access the Internet, make or receive calls, or text messages (Sources: Financial Times, BBC News, the Guardian).

security breaches in the communications networks that support mobile payment services, which have raised concerns from banking regulators (FCA, 2013). Financial authorities have considered cyber risks as a threat to financial stability with their systemic risk implications (Tendulkar, 2013; Murphy, 2013; Bank of England, 2013a; Ruggiero and Foote, 2011). Authorities in the United States and United Kingdom, for example, have responded with simulated attacks to test industry preparedness and network resiliency. NFC has also been prone to attacks on the reader or tag, relay attacks, eavesdropping, data destruction, data insertion, and man in the middle intrusions (Boer and Boer, 2009). The safety of cloud based infrastructures, which involves distributed computing over a network, may also be uncertain as compared to more standardized and secured interbank financial telecommunication networks like SWIFT, which are largely used by banks and has an oversight board with central bank representatives. The economic impact from cybercrime and cyber espionage has been estimated to be as high as 140 billion U.S. dollars in the United States, and could reach 500 billion U.S. dollars globally (Center for Strategic and International Studies, 2013).

43. **Roaming risks also exist for international remittances through mobile phones.** Roaming agreements now allow interoperability and exchange of payment data in addition to voice data, but may also be exposed to interception and fraud (Merritt, 2010). Industry efforts, mainly coordinated through the GSMA, have strengthened security standards in these areas to minimize such risks. This includes, for example, recommendations for near-real-time roaming data exchange technology to be implemented by operators in different jurisdictions to reduce roaming fraud. Operators are also required to send roaming data to partners within a prescribe limit. The association has also cooperated with regional bodies to develop requirements and specifications for trusted third parties in mobile contactless payment schemes (EPC and GSMA, 2010).

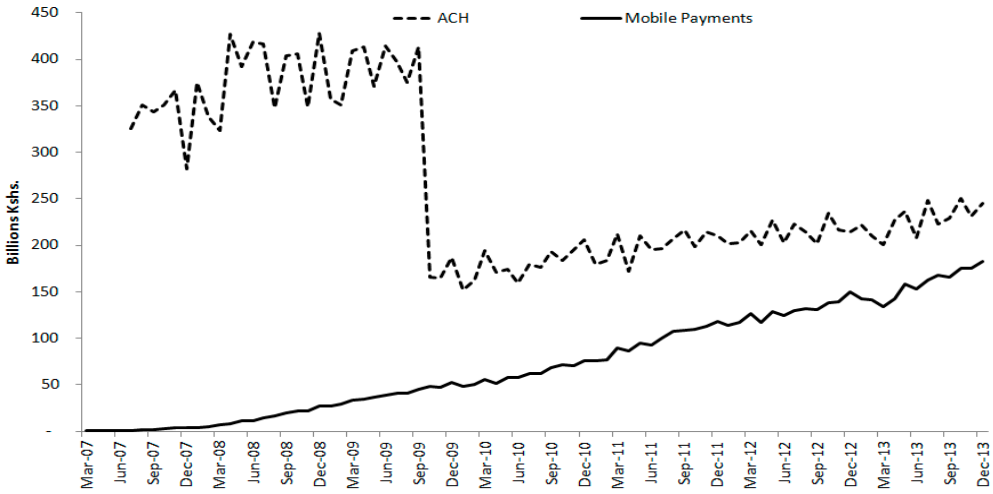
E. Payment System

44. **The aggregate value of mobile payment flows can be significant relative to tightly regulated payment systems in some countries where activity has heightened.** The Central Bank of Kenya illustrates how authorities can monitor and compare the growth of mobile payments against systemically important payment systems. Although the aggregate transaction values of mobile payments (from M-Pesa, Airtel, and Yu) are significantly smaller to the real-time gross settlement (RTGS) system, their growth is approaching the level of the ACH, which is also regulated and supervised by the central bank (Figure 3). Such statistics also monitor the number of agents and the number of registered customers and accounts (Central Bank of Kenya, 2013). Value-capping measures, introduced on October 1, 2009, to remove 60 percent of value and 5 percent of volume from the ACH to the RTGS system, were aimed at moving high-value transactions and mitigating potential settlement risk in the ACH. This has led to a sharp decline in aggregate flows in the ACH in 2009. Both the ACH and RTGS system are systemically important payment systems.

45. **The effectiveness of existing risk controls to handle the sharp growth in mobile payments, however, raises oversight challenges for financial authorities if their**

aggregate activity continues to rise and surpass the ACH.[13] As earlier discussed, financial authorities have addressed this issue through recent proposed changes in Kenya's deposit insurance law to account for "pass through" provisions to protect customer funds in the event of a bank failure. This is important if the bank holds the trust account of an MNO.

Figure 3. Kenya: ACH and Mobile Payment Monthly Transaction Values, 2005-2013



Source: Central Bank of Kenya.

46. **A payment system should strengthen its risk controls to manage potential credit and liquidity risks that may stem from heightened payment activity, including from mobile payments.** This has been a key issue for many countries where deferred net settlement (DNS) systems were found to be unprotected against liquidity risk that arise from an inability to settle on the part of one of more participants (World Bank and IMF, 2002). Some of the systems have continued reliance on unwinding arrangements, which lack observance to international standards. Other systems have no provisions for such an event, or implicitly rely either on direct lending by the central bank or on obtaining access to a continuing high level of required reserves. Risks could exacerbate from direct bank participants in the payment system (that offer electronic payment services) or from nonbank participants (such as postal operators).

47. **New international standards require increased protection for payments systems.** Under the PFMIs, Principle 7 on liquidity risk requires FMIs to effectively measure, monitor, and manage their liquidity risk. DNS systems, such as the ACH, that have been designated as

[13] Global Findex Database findings also suggest potential growth in Kenya. Around 79 percent of adults surveyed were found to have a mobile phone in their household and 68 percent used it in the past 12 months to pay bills, or send or receive money (Demirguc-Kunt and Klapper, 2012). This means that 86 percent of all mobile phone users use mobile payments. The rapid diffusion of mobile phones and support by the central bank has supported this growth (Jack and Tavneet, 2011). Its success has also raised interest for some countries in Eastern Europe (Romania) in promoting access to financial services.

a systemically important payment system would need to observe such risk controls. Sufficient liquid resources also need to be maintained in all relevant currencies to effect same-day and, where appropriate, intraday and multiday settlement of payment obligations with a high degree of confidence under a wide range of potential stress scenarios that should include, but not be limited to, the default of the participant and its affiliates that would generate the largest aggregate liquidity obligation for the FMI in extreme but plausible market conditions. Liquidity risk mismanagement could lead to credit risk, whereby a bank does not have sufficient funds to cover a transaction that has been earlier credited to customers before settlement. Principle 4 on credit risk would further require an FMI to effectively measure, monitor, and manage its credit exposures to participants and those arising from its payment, clearing, and settlement processes. The FMI also needs to maintain sufficient financial resources to cover its credit exposure to each participant fully with a high degree of confidence.

48. **Default arrangements are being strengthened in some countries, which will help cope with an expected increase in faster payments (Box 5).** Such improvements focus on developing credit and liquidity risk mitigation measures to accommodate the sharp rise of faster payment transactions, which could be further driven by a rise in mobile payments activity from financial institutions and possibly other payment service providers (Bank of England, 2014, 2013b; Faster Payments Scheme, 2013). Faster payment schemes speed up the settlement time for retail payments to a near real-time basis from their deferred settlement period that may range from different intervals during a day, at the end of day, or several days. This not only makes the features of the retail payment infrastructure nearly similar to RTGS systems, but also enhances service availability to consumers on a daily and around the clock basis. The UK Faster Payments Scheme (FPS), for example, started to service mobile payments in April 2014. This scheme, which currently handles internet and phone banking payments, will provide access to 49 million current account holders who can send security-protected payments by mobile phones. This involves simple text messages where disclosure of account details and sort codes are not required. While financial institutions would initially provide the service, future participation in the mobile payments scheme will be open to any payment service providers that have access to the FPS and/or the LINK ATM network. Other faster payment schemes that have been in operation, or under development, are in Australia (Fast Payments Solution), Denmark (NETS), India (Immediate Payment Service), Norway (NETS), Singapore (G3), and Sweden (Bankgirot).

49. **Access criteria are also an emerging issue in many payment systems.** Access to designated payment systems is permitted only to banks in many countries with nonbank participation through direct or indirect channels more limited. For many nonbanks, this could create an unlevel playing field as they are obliged to use the settlement services of a bank. More importantly, it may also restrict them from risk mitigation measures that help prevent settlement risks. For the FMI, admission of nonbank participants may be a source of vulnerability if the risk criteria used for their admission is weak, or they are not properly supervised, regulated, or aligned with international standards. Such criteria could ensure that participants meet appropriate operational, financial, and legal requirements. If an FMI admits non-regulated entities, it should take into account any additional risks that may arise from their participation and design its participation requirements and risk management controls accordingly. As discussed, access to payment networks is under review in the EU, which

involves proposed revisions to the PSD to allow nonbank participation in payment and settlement systems. There have also been recommendations to establish objective and transparent rules for payment institutions to access indirectly (through direct participants) designated payment systems (EC, 2013). However, such changes remain under review as of June 2014.

Box 5. United Kingdom: Risk Control in Retail Payment Systems

Faster Payments Service (FPS) is a systemically important payment system recognized by the finance ministry and overseen the central bank in the United Kingdom. It is operated by Faster Payments Scheme Limited (FPSL) and processes standing orders and electronic retail transactions, including transactions generated in telephone and internet banking.

Value limits: Per transaction value limits and daily limits apply, and are established differently by bank and mode of payment (online or phone payments versus standing order payments). Value limits may range from GBP 5,000 for a retail customer making a phone or internet payment to GBP 100,000 for a corporate customer using the same payment channel. Limits for standing orders range from GBP 10,000 to GBP 100,000. Limits for sending mobile payments have been set at GBP 250 per day, although banks and building societies may offer a higher daily limit to consumers.

Loss sharing arrangement: To mitigate settlement risk, Faster Payments Members' net settlement positions are limited using hard debit caps. The caps are partially collateralized as a requirement of the Scheme's Liquidity and Loss Share Agreement (LLSA). If a member bank fails to settle, the LLSA also requires surviving Members to provide liquidity to meet any shortfall in the settlement obligations of the failed member (up to the value of the largest member). Surviving members are subsequently partially refunded through liquidation of the failed member's collateral. It is in the Schemes corporate strategy that all collateral will be 'pre-funded' in cash by the end of 2014 eliminating any credit risk of default.

Pre-funding: 'Pre-funding' involves members covering their positions in advance in full with cash held at the Bank of England. This completely eliminates settlement risk.

The Bank of England acts as the settlement agent and as the trustee for the collateral posted under the LLSA. The System is settled in the Bank of England's RTGS system in the same way as other clearings (such as Bacs and Cheque and Credit Clearing). RTGS sends Faster Payments Scheme Members advices of the amounts to be settled via the Enquiry Link system.

Source: Bank of England; Faster Payments Scheme.

50. **Leveraging ACH to support mobile payments is also under review in the United States.** The establishment of a ubiquitous platform for mobile payments by leveraging existing clearing and settlement system, such as the ACH or card payment networks, has also been proposed as a key success factor in the United States (Crowe et al., 2013; Contini et al., 2011). Currently, use of the ACH network to handle mobile payments has grown, particularly for bill payments where many financial institutions and nonbank payment service providers have developed Internet and applications that clear and settle mobile payments through the ACH. The transaction speed for mobile payments ranges from real-time to several days where they could be handled in-house or through interbank payment systems.

IV. CONCLUSION

51. **Oversight issues in mobile payments are emerging, and financial authorities need to safeguard public confidence and financial stability if necessary.** Growth in this emerging retail payment method has been shaped by increased worldwide deployments (half of which are in Sub-Saharan Africa), mobile phone penetration, financial inclusion, and continued demand for convenient, faster, and more economical means of payments.

52. **This presents financial authorities with the following challenges.** *First*, legal regimes, oversight frameworks, and licensing requirements need to be clearly established. *Second*, AML/CFT measures to protect mobile payment systems from financial integrity risks need to be proportionate to avoid stifling innovation. *Third*, fund safeguarding measures need to be strengthened, particularly in jurisdictions where there has been a rise in mobile payments activity. Such measures may involve regulations on usage restrictions, protection requirements, and float management. Some LICs, where such innovations have proliferated, have started to strengthen customer fund protection, which is in line with similar arrangements in advanced economies. In principle, this can include insurance requirements, similar guarantee schemes, or "pass through" provisions in the deposit insurance law. *Fourth*, operational resiliency needs to be ensured against potential disruptions or compromises on system integrity. And *fifth,* risk controls in retail payment systems need to be strengthened to cope with increased usage of emerging payment methods (including mobile payments) and the adoption of faster payment schemes. Access criteria are also needed to ensure that appropriate operational, financial, and legal requirements are met.

53. **Oversight frameworks need to be strengthened to protect those who are vulnerable, particularly in LICs, who may loose a great portion (if not all) of their assets to risky and unprotected mobile payment schemes.** While half of the world's live mobile money deployments were found in Sub-Saharan Africa, there is less evidence that oversight arrangements are being improved in such jurisdictions to safeguard customer funds. Recent developments in the region (Kenya) suggest that financial authorities recognize the potential risks from mobile payment systems and are taking regulatory steps to safeguard public confidence and financial stability. This helps protect small to moderate income households from the potential risk of loosing funds held in a trust account by a MNO in an insured, but failed bank. This may also be relevant for more advanced economies where fund safeguarding issues remain a grey area or are currently missing from the legal framework. Going forward, competition and interoperability issues may also emerge that would further challenge the oversight framework. This may include the creation of a level playing field between bank and nonbank payment service providers in terms of regulatory requirements, access to regulated payment systems, and protection under deposit insurance schemes.

Annex 1. Selected Mobile Payment Schemes by Region

Region	Country	Service Provider
Sub-Saharan Africa	Benin	Areeba
	Burkina Faso	Airtel
	Burundi	Econet Wireless
	Cameroon	MTN; Orange
	Chad	Airtel; Tigo (Millicom)
	Cote d'Ivoire	Moov (Etisalat); MTN; Orange; CelPaid
	Democratic Republic of Congo	Airtel; Vodacom
	Gabon	Airtel; BICIG
	Ghana	Airtel; Tigo (Millicom); Txtnpay
	Kenya	Airtel; Orange (Telkom Kenya); Safaricom; Tangaza
	Liberia	Lonestar
	Madagascar	Airtel; Orange
	Malawi	Airtel; TNM
	Mali	Orange
	Mozambique	Mcel
	Niger	Airtel
	Nigeria	eTranzact; Ecobank Nigeria Plc; FETS; Fortis; mKudi; Parkway Projects; Teasy Mobile
	Rwanda	Airtel; MTN
	Sierra Leone	Airtel
	Somalia	Golis Telecom; Telesom
	South Africa	FNB; MTN
	Tanzania	Airtel; Vodacom
	The Republic of Congo	Airtel
	Uganda	Airtel; MTN; Housing Finance Bank
	Zambia	Airtel; Zoona
	Zimbabwe	Econet Wireless
East Asia and Pacific	Cambodia	Wing
	Fiji	Digicel; Vodafone
	Indonesia	Bank Sinar; Indosat (Ooredo); mCoin; Telkomsel
	Malaysia	Maxis
	Papua New Guinea	Maxis
	Philippines	Smart (PLDT); Globe Telecom
	Samoa	Digicel
	Thailand	AIS; True Move
	Tonga	Digicel
	Vanuatu	Digicel
South Asia	Afghanistan	Roshan (TDCA)
	Bangladesh	Banglalink (Orascom); bKash; Grameenphone (Telenor); Robi (Axiata)
	India	Airtel (Maxis); IDEA Cellular; MMPL; Oxigen; Vodafone
	Nepal	Finaccess; FonePay
	Pakistan	Telenor; UBL Bank; Habib Bank Limited
	Sri Lanka	Dialog Telekom (Axiata)
Middle East and North Africa	Iran	Jiring
	Jordan	Zain
	Qatar	Ooredoo
	Tunisia	Tunisiana; Viamobile
Latin America and the Caribbean	Brazil	Zuum
	Colombia	DaviPlata
	Guatemala	Tigo (Millicom)
	Guyana	GT&T
	Paraguay	Tigo (Millicom)
Europe and Central Asia	Armenia	VivaCell (MTS)
	Turkey	Turkcell

Source: Groupe Speciale Mobile Association (2014).

Annex 2. G20 Principles for Innovative Financial Inclusion

Innovative financial inclusion means improving access to financial services for poor people through the safe and sound spread of new approaches. The following principles aim to help create an enabling policy and regulatory environment for innovative financial inclusion. The enabling environment will critically determine the speed at which the financial services access gap will close for the more than two billion people currently excluded. These principles for innovative financial inclusion derive from the experiences and lessons learned from policymakers throughout the world, especially leaders from developing countries.

1. **Leadership**: Cultivate a broad-based government commitment to financial inclusion to help alleviate poverty.
2. **Diversity**: Implement policy approaches that promote competition and provide market-based incentives for delivery of sustainable financial access and usage of a broad range of affordable services (savings, credit, payments and transfers, insurance) as well as a diversity of service providers.
3. **Innovation**: Promote technological and institutional innovation as a means to expand financial system access and usage, including by addressing infrastructure weaknesses.
4. **Protection**: Encourage a comprehensive approach to consumer protection that recognizes the roles of government, providers and consumers.
5. **Empowerment**: Develop financial literacy and financial capability.
6. **Cooperation**: Create an institutional environment with clear lines of accountability and co-ordination within government; and also encourage partnerships and direct consultation across government, business and other stakeholders.
7. **Knowledge**: Utilize improved data to make evidence based policy, measure progress, and consider an incremental "test and learn" approach acceptable to both regulator and service provider.
8. **Proportionalit**y: Build a policy and regulatory framework that is proportionate with the risks and benefits involved in such innovative products and services and is based on an understanding of the gaps and barriers in existing regulation.
9. **Framework**: Consider the following in the regulatory framework, international standards, national circumstances and support for a competitive landscape: an appropriate, flexible, risk-based Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) regime; conditions for the use of agents as a customer interface; a clear regulatory regime reflecting for electronically stored value; and market-based incentives to achieve the long-term goal of broad interoperability and interconnection.

These principles are a reflection of the conditions conducive to spurring innovation for financial inclusion while protecting financial stability and consumers. They are not a rigid set of requirements but are designed to help guide policymakers in the decision making process. They are flexible enough so they can be adapted to different country contexts.

Source: Access through Innovation Sub-Group (2010).

Annex 3. Principles for Financial Market Infrastructures

There are 24 principles under the CPSS-IOSCO PFMIs, 18 of which are applicable to payments systems:

Principle 1: Legal basis
An FMI should have a well-founded, clear, transparent, and enforceable legal basis for each material aspect of its activities in all relevant jurisdictions.

Principle 2: Governance
An FMI should have governance arrangements that are clear and transparent, promote the safety and efficiency of the FMI, and support the stability of the broader financial system, other relevant public interest considerations, and the objectives of relevant stakeholders.

Principle 3: Framework for the comprehensive management of risks
An FMI should have a sound risk-management framework for comprehensively managing legal, credit, liquidity, operational, and other risks.

Principle 4: Credit risk
An FMI should effectively measure, monitor, and manage its credit exposures to participants and those arising from its payment, clearing, and settlement processes. An FMI should maintain sufficient financial resources to cover its credit exposure to each participant fully with a high degree of confidence.

Principle 5: Collateral
An FMI that requires collateral to manage its or its participants' credit exposure should accept collateral with low credit, liquidity, and market risks. An FMI should also set and enforce appropriately conservative haircuts and concentration limits.

Principle 6: Margin
Not relevant to payment systems.

Principle 7: Liquidity risk
An FMI should effectively measure, monitor, and manage its liquidity risk. An FMI should maintain sufficient liquid resources in all relevant currencies to effect same-day and, where appropriate, intraday and multiday settlement of payment obligations with a high degree of confidence under a wide range of potential stress scenarios that should include, but not be limited to, the default of the participant and its affiliates that would generate the largest aggregate liquidity obligation for the FMI in extreme but plausible market conditions.

Principle 8: Settlement finality
An FMI should provide clear and certain final settlement, at a minimum by the end of the value date. Where necessary or preferable, an FMI should provide final settlement intraday or in real time.

Principle 9: Money settlements
An FMI should conduct its money settlements in central bank money where practical and available. If central bank money is not used, an FMI should minimize and strictly control the credit and liquidity risk arising from the use of commercial bank money.

Principle 10: Physical deliveries
Not relevant to payment systems.

Principle 11: Central securities depositories
Not relevant to payment systems.

Principle 12: Exchange-of-value settlement systems
If an FMI settles transactions that involve the settlement of two linked obligations, it should eliminate principal risk by conditioning the final settlement of one obligation upon the final settlement of the other.

Principle 13: Participant-default rules and procedures
An FMI should have effective and clearly defined rules and procedures to manage a participant default. These rules and procedures should be designed to ensure that the FMI can take timely action to contain losses and liquidity pressures and continue to meet its obligations.

Principle 4: Segregation and portability
Not relevant to payment systems.

Principle 15: General business risk
An FMI should identify, monitor, and manage its general business risk and hold sufficient liquid net assets funded by equity to cover potential general business losses so that it can continue operations and services as a going concern if those losses materialize. Further, liquid net assets should at all times be sufficient to ensure a recovery or orderly wind-down of critical operations and services.

Principle 16: Custody and investment risks
An FMI should safeguard its own and its participants' assets and minimize the risk of loss on and delay in access to these assets. An FMI's investments should be in instruments with minimal credit, market, and liquidity risks.

Principle 17: Operational risk
An FMI should identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls. Systems should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and fulfillment of the FMI's obligations, including in the event of a wide-scale or major disruption.

Principle 18: Access and participation requirements
An FMI should have objective, risk-based, and publicly disclosed criteria for participation, which permit fair and open access.

Principle 19: Tiered participation arrangements
An FMI should identify, monitor, and manage the material risks to the FMI arising from tiered participation arrangements.

Principle 20: FMI links
Not relevant to payment systems.

Principle 21: Efficiency and effectiveness
An FMI should be efficient and effective in meeting the requirements of its participants and the markets it serves.

Principle 22: Communication procedures and standards
An FMI should use, or at a minimum accommodate, relevant internationally accepted communication procedures and standards in order to facilitate efficient payment, clearing, settlement, and recording.

Principle 23: Disclosure of rules, key procedures, and market data
An FMI should have clear and comprehensive rules and procedures and should provide sufficient information to enable participants to have an accurate understanding of the risks, fees, and other material costs they incur by participating in the FMI. All relevant rules and key procedures should be publicly disclosed.

Principle 24: Disclosure of market data by trade repositories
Not relevant to payment systems.

Source: Committee on Payment and Settlement Systems and Technical Committee of the International Organization of Securities Commission (2012).

REFERENCES

Access through Innovation Sub-Group, 2010, *Innovative Financial Inclusion,* Principles and Report on Innovative Financial Inclusion from the Access through Innovation Sub-Group of the G20 Financial Inclusion Experts Group, May 25.

Alliance for Financial Inclusion, 2014a, *Guideline Note on Consumer Protection in Mobile Financial Services*, Mobile Financial Services Working Group, March.

_____, 2014b, *Guideline Note on Supervision and Oversight of Mobile Financial Services*, Mobile Financial Services Working Group, February.

_____, 2013, *Guideline Note on Indicators for Measuring Access and Usage*, Mobile Financial Services Working Group, August.

_____, 2012a, *Guideline Note on Mobile Financial Services Basic Terminology*, Mobile Financial Services Working Group, July.

_____, 2012b, *Guideline Note on Mobile Financial Services Regulatory Reporting*, Mobile Financial Services Working Group, September.

Allen, Hellen, 2003, "Innovations in Retail Payments: E-Payments", *Bank of England Quarterly Bulletin*, Winter, pp. 428-438.

Ardic, Oya P, Kathryn Imboden, and Alexia Latortue, 2013, *Financial Access 2012: Getting to a More Comprehensive Picture*, Consultative Group to Assist the Poor and International Finance Corporation, June.

Basel Committee on Banking Supervision and International Association of Deposit Insurers, 2009, *Core Principles for Effective Deposit Insurance Systems*, Bank for International Settlements, June.

Bank of England, 2014, *The Bank of England's Supervision of Financial Market Infrastructures – Annual Report*, March 17.

_____, 2013a, *Systemic Risk Survey: Survey Results*, 2013 H1.

_____, 2013b, *Payment Systems Oversight Report 2012*, March.

Boer, Remco and Tonnis de Boer, 2009*, Mobile Payments 2010: Market Analysis and Overview*, Innopay and Telecompaper, November.

Braun, Michele, James McAndrews, William Roberds, and Richard Sullivan, 2008, "Understanding Risk Management in Emerging Retail Payments", *Federal Reserve Bank of New York Economic Policy Review*, September, pp. 137-159.

Capgemini and Royal Bank of Scotland, 2013, *World Payments Report 2013*.

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

Center for Strategic and International Studies, 2013, *The Economic Impact of Cybercrime and Cyber Espionage*, July.

Central Bank of Kenya, 2013, *Annual Report*.

Chatain, Pierre-Laurent, Andrew Zerzan, Wameek Noor, Najah Dannaoui, and Louis de Koker, 2011, *Protecting Mobile Money against Financial Crimes,* World Bank.

Committee on Payment and Settlement Systems, 2013, *Statistics on Payment, Clearing and Settlement Systems in the CPSS Countries*, Bank for International Settlements, September.

_____, 2012, *Innovations in Retail Payments*, Bank for International Settlements, Report of the Working Group on Innovations in Retail Payments, May.

_____, 2005, *Central Banks Oversight of Payment and Settlement Systems*, Bank for International Settlements, May.

_____, 2004, *Survey of Developments in Electronic Money and Internet and Mobile Payments*, Bank for International Settlements, March.

Committee on Payment and Settlement Systems and Technical Committee of the International Organization of Securities Commissions, 2012, *Principles for Financial Market Infrastructures*, Bank for International Settlements, April.

Committee on Payment and Settlement Systems and World Bank, 2007, *General Principles for International Remittance Services*, Bank for International Settlements, January.

Contini, Darin, Marianne Crowe, Cynthia Merritt, Richard Oliver, and Steve Mott, 2011, *Mobile Payments in the United States: Mapping Out the Road Ahead*, Federal Reserve Bank of Atlanta, Federal Reserve Bank of Boston, and Better Buy Design, March 25.

Crowe, Marianne, Susan Pandy, Elisa Tavilla, and Cynthia Jenkins, 2013, *U.S. Mobile Payments Landscape – Two Years Later*, Federal Reserve Bank of Boston and Federal Reserve Bank of Atlanta, May.

Demirguc-Kunt, Asli and Leora Klapper, 2012, "Measuring Financial Inclusion: The Global Findex Database", *World Bank Policy Research Working Paper* No. 6025, April.

Demirguc-Kunt, Asli, Edward Kane, and Luc Laeven, 2008, "Deposit Insurance Design and Implementation: Policy Lessons from Research and Practice", in *Deposit Insurance Around the World*, MIT Press, Cambridge.

Dittus, Peter and Michael Klein, 2011, "On Harnessing the Potential of Financial Inclusion", *BIS Working Paper,* No. 347, May.

Drozdowski, Robert C, Matthew W. Homer, Elizabeth A. Khalil, and Jeffrey M. Kopchik, 2012, "Mobile Payments: An Evolving Landscape", Federal Deposit Insurance Corporation *Supervision Insights*, Vol. 9, Issue 2, pp. 3-11.

European Central Bank, 2012, *Virtual Currency Schemes*, October (Frankfurt).

European Commission, 2013, *Commission Staff Working Document: Impact Assessment*, July 24, Brussels.

_____, 2012, *Green Paper on Towards an Integrated European Market for Card, Internet and Mobile Payments*, Brussels.

European Payments Council and GSMA, 2010, *Mobile Contactless Payments Service Management Roles, Requirements, and Specifications*, Document No. EPC 220-08, Version 2.0, October.

Faster Payments Scheme, 2013, *CPSS-IOSCO Self-Assessment Public Disclosure for Faster Payments Scheme Limited*, December 12.

Financial Action Task Force, 2013, *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services*, June (Paris).

_____, 2010, *Money Laundering Using New Payment Methods*, October (Paris).

Financial Conduct Authority, 2013, *Mobile Banking and Payments – Supporting an Innovative and Secure Market*, Thematic Review 13/6, August.

Financial Stability Board, 2012, *Thematic Review on Deposit Insurance Systems: Peer Review Report*, February 8.

Flood, Darren, Tim West, and Daniel Wheadon, 2013, "Trends in Mobile Payments in Developing and Advanced Economies", *Reserve Bank of Australia Bulletin*, March, pp. 71-79.

Gartner, 2013, *Forecast: Mobile Payment, Worldwide, 2013 Update*.

Groupe Speciale Mobile Association, 2014, *State of the Industry 2013: Mobile Financial Services for the Unbanked*, GSM Association.

Hillerbrand, Gail, 2008, "Before the Grand Rethinking: Five Things to do Today with Payments Law and Ten Principles to Guide New Payments Products and New Payments Law", Symposium on Rethinking Payments Law, *Chicago-Kent Law Review*, No. 2, pp. 769-811.

Hong Kong Monetary Authority, 2013, "Stored Value Facilities and Retail Payment Systems in Hong Kong: A Proposed Regulatory Regime", *Quarterly Bulletin*, June, pp. 1-5.

International Monetary Fund, 2012, *Enhancing Financial Sector Surveillance in Low Income Countries: Case Studies*, April 16.

Jack, William and Tavneet Suri, 2011, "Mobile Money: The Economics of M-PESA", *National Bureau of Economic Research Working Paper* 16721, January.

Martindale, Suzanne and Gail Hillerbrand, 2011, "Pay at Your Own Risk? How to Make Every Way Pay Safe for Mobile Payments", *Banking and Finance Law Review*, 27, pp. 265-283.

MasterCard, 2012, *The Mobile Payments Readiness Index: A Global Market Assessment*, May.

Merritt, Cynthia, 2010, *Mobile Money Transfer Services: The Next Phase in the Evolution in Person-to-Person Payments*, Retail Payments Risk Forum White Paper, Federal Reserve Bank of Atlanta, August.

Murphy, Edward, 2013, *Financial Stability Oversight Council: A Framework to Mitigate Systemic Risk*, Congressional Research Service, May.

Norges Bank, 2013, *Annual Report on Payment Systems 2012*, May.

Ruggiero, Paul and Jon Foote, 2011, *Cyber Threats to Mobile Phones*, Carnegie Mellon University, United States Computer Emergency Readiness Team.

Tarazi, Michael and Paul Breloff, 2010, "Nonbank E-Money Issuers: Regulatory Approaches to Protecting Customer Funds", Consultative Group to Assist the Poor, *Focus Note* No. 63, July.

Tendulkar, Rohini, 2013, *Cyber-Crime, Securities Markets and Systemic Risk*, Staff Working Paper 1/2013, International Organization of Securities Commissions and World Federation of Exchanges, July 16.

United States House of Representatives, 2012, Testimony of Suzanne Martindale, Staff Attorney, Consumers Union of U.S., Inc. on *The Future of Money: How Mobile Payments Could Change Financial Services* before the Committee on Financial Services, Subcommittee on Financial Institutions and Consumer Credit, March 22.

World Bank, 2012, *Innovations in Retail Payments Worldwide*, Financial Infrastructure Series, Payment Systems Policy and Research, October.

_____, 2011, *Payment Systems Worldwide: A Snapshot of Outcomes of the Global Payment Systems Survey 2010*, Financial Infrastructure Series, Payment Systems Policy and Research.

World Bank and International Monetary Fund, 2002, *Financial Sector Assessment Program—Experience with the Assessment of Systemically Important Payment Systems*, April 19.