Emerging Trends in Sub-Saharan Africa

Policymakers' Perspectives

Silvia Baur-Yazbeck, Ivo Jenik, and Myra Valenzuela

October 2017

ABSTRACT

CGAP has conducted global research identifying, analyzing, and prioritizing trends and innovations in digital financial services that have potential impact on financial inclusion in Sub-Saharan Africa. We have identified more than 20 trends/developments that have been gaining traction over the last several years and are moving from the fringe into the mainstream. These trends are described in this report.

DISCLAIMER

This work was funded in whole or in part by CGAP. Unlike CGAP's official publications, it has not been peer reviewed or edited by CGAP, and any conclusions or viewpoints expressed are those of the authors, and they may or may not reflect the views of CGAP staff.

Table of Contents

Digital Financial Inclusion: Emerging Trends in Sub-Saharan Africa from Policymakers' Perspective

Executive Summary

The speed and complexity of technological change in financial markets is creating profound shifts in the financial inclusion space, with corresponding implications for policymakers, who must actively monitor and evaluate emerging trends, balance risks with benefits, and react adequately in a timely manner.

Under new strategic cycle CGAP VI (2018-2023), CGAP is proposing new work to support the capacity and strategic decision-making of regulators in emerging economies as they encounter new trends concerning financial services, products, and approaches that are aimed specifically at lower-income consumers. As part of the CGAP VI on-ramping research, CGAP's Policy Pillar has conducted global research identifying, analyzing, and prioritizing these new trends and innovations in digital financial services (DFS) that have potential impact on financial inclusion in Sub-Saharan Africa (SSA). The primary objective of this research is to flag impactful directions in the policy arena to be further explored under CGAP VI.

We have identified more than 20 emerging trends/developments in digital financial inclusion that have been gaining traction over the last several years and are moving from the fringe into the mainstream. The list of trends is based on desk research concerning a comprehensive overview of internal CGAP resources, complemented by analysis of other publications (by the World Bank, GPFI, AFI, FinCoNet, standard-setting bodies, consulting firms, academia, national policymakers), news articles, and informal stakeholder interviews. Our decision to include each of the trends was based on the following four criteria: (i) frequency of references, (ii) direct impact on low-income consumers, (iii) direct impact on supervisory capacity, and (iv) relevance to SSA.

We have further narrowed the list to the Top 10 priority trends. The Top 10 trends are of varying nature – many are **new technological innovations** (APIs, big data analytics, digital credit, digital identity, distributed ledger technology, most of which fall under the general 'movement' of FinTech); some are **consumer protection concerns** due to advancements in digital financial services (cybercrime, data privacy); while others can **aid policymakers with limited capacities** to do their job more efficiently and effectively (RegTech, innovation facilitators). In addition, we have included "a wild-card trend" that is at early stages of development, but has potentially far-reaching consequences for the entire financial sector - digital fiat currencies. All the trends are listed and briefly described below.

A. Priority Trends

I. Application Programming Interfaces (APIs)

Description: An application programming interface (API) "is an architecture that makes it easy for one application to 'consume' capabilities or data from another application" (Apigee). It is a protocol that allows software programs to "talk" to one another, defining what information should be supplied and what actions will be taken when it is executed. A common example is Uber's use of Google Maps or Waze's mapping services. Open APIs are widely available for other companies to consume.
APIs are important to financial inclusion because they connect third-parties to established payments platforms, essentially turning providers' platforms into "digital rails" that third-parties can leverage to deliver innovative services that address the needs of many customers.

Impact on supervisory capacity: Given the potential APIs hold, regulators may consider adopting policies to promote the use of open APIs (e.g., the EU Payments Directive 2). In the same time, (open) APIs present challenges for supervisors, including new risks due to the entrance of unregulated third party developers, and a need to collaborate with other regulators outside the financial sector (e.g. telecoms regulator). Direct benefits from regulators and supervisors stemming from open APIs revolve around collection of data for market monitoring and offsite supervision, where APIs may allow supervisors to get regulatory data in a streamlined way.

Direct impact on low-income consumers: APIs are important to financial inclusion because they connect third-parties to established payments platforms, essentially turning providers' platforms into "digital rails" that third-parties can leverage to deliver innovative services that address the needs of many customers.

Examples: In September 2015, **Safaricom** announced it was opening its M-Pesa API to third party developers. Shortly after, **Airtel Africa** introduced a partnership with IMImobile to launch an Africa-wide billing API for local merchants called Tap2Bill. In February 2016, **Vodacom Tanzania** also opened its M-Pesa API to developers. Three months later, in partnership with local tech hub Bongohive, **MTN Zambia** organized two developer workshops to present its API program. In **Ghana, Vodafone** is about to open its mobile money API (Vodafone Cash) and plans to open its SMS API in the coming months. In July 2015, **Orange** opened its SMS API to several countries across Africa (now up to 9 countries: **Botswana, Cote d'Ivoire, DR Congo, Egypt, Guinea Conakry, Mali, Niger, Senegal, Tunisia**).

References as of October 2017
-CGAP (2015), "Can Open APIs Accelerate the Digital Financial Ecosystem?"
-CGAP (2015), "Why Open APIs Matter: Tech Partnerships Power Development"
-CGAP (2015), "Partnership: Missing Ingredient to Mobile Money APIs"
-CGAP (2015), "Just How Open is Safaricom's Open API?"
-CGAP (2016), "Riding the 'Rails': Unlocking Innovation with Open APIs"
-CGAP (2017), "Are Open Platforms Smart Business for Payment Providers?"
-CGAP (2017), "5 Keys to Addressing the Needs of API Consumers"
-CGAP (2017), "Open APIs in Digital Finance: We Opened Up, Here's What Happened"
-CGAP (2017), "Four Drivers of Change for Financial Inclusion in 2017"
-GSMA (2016), "APIs: a bridge between mobile operators and start-ups in emerging markets"
-World Bank (2016), "2016 World Development Report: Digital Dividends"

II. Big data analytics

Description: "Big Data" has been defined in various ways. Many tend to highlight the following definitional features: (i) high-volume data, (ii) produced, collected, and processed with high speed, (iii) variety information

assets, and (iv) technology-based processing of data in a meaningful way to enhance insights and decision-making. See, e.g., Gartner IT Glossary. Among other things, big data analytics can help make financial products better suited to customers' needs, more accessible (alternative credit scoring, new ways of customer due diligence), and more affordable (cheaper compliance, better targeting). It can also improve the capacity to regulate and supervise financial service providers.

Impact on supervisory capacity: Since fintech firms are developing more quickly than the regulatory environments in which they operate, the entrance of new business models present new risks for regulators. Supervisors would also need to learn about the algorithms underpinning the Big Data platforms. Privacy and data protection is another important issue concerning Big Data. Digital credit (including crowdfunding) and digital identity are the two most prominent areas for financial inclusion-oriented FSPs to experiment with Big Data analytics.

Direct impact on low-income consumers: Big Data change financial service delivery in several important ways: (i) data that aggregates customer behavior across different dimensions (e.g., airtime consumption and savings behavior) can provide insights for a large aggregated pool of users, while at the same time provide highly individualized insights about individuals, which can, for instance, lead to improved access to credit for individuals with limited or no credit history; (ii) it opens the possibility of tailoring product characteristics to the needs of individuals; (iii) the availability of digital channels allows the deployment of data-enabled services at a large scale, opening the possibility of remotely issuing loans and reaching a wider market.

Examples: In Sub-Saharan Africa: AFB Airtel (**Kenya, Ghana, Tanzania**), Cignifi (Mexico, Chile, Brazil, **Ghana**), EcoCash Loans (**Zimbabwe**), First Access (**Tanzania**), Go Finance (**Tanzania**), inVenture (**Kenya**), Kopo Kopo (**Kenya**), Linda Jammi - Changamka (**Kenya**), M-Pawa (**Tanzania**), M-Shwari (**Kenya**), Mjara-MFS Africa (**Ghana, Cameroon**), Mode (**Kenya, Chad**), M-Kopa (**Kenya, Tanzania, Uganda**).

References as of October 2017

-Accion (2017), "Unlocking the Promise of Big Data to Promote Financial Inclusion"
-CGAP (2012), "Can Digital Footprints Lead to Greater Financial Inclusion?"
-CGAP & McKinsey (2014), "Projecting Impact of Non-Traditional Data and Advanced Analytics on Delivery Costs"
-CGAP (2014), "Hype or Hope? Implications of Big Data for Financial Inclusion"
-CGAP (2014), "Big Data for Financial Inclusion: Is Boring Better?"
-CGAP (2014), "How Analytics Drive Innovative Financial Services for the Poor"
-CGAP (2014), "Leveraging Mobile Phone Data: Tiaxa's Balance Advance"
-CGAP (2014), "It's Time to Listen to the Voice of the Customer"
-CGAP (2014), "Simple Messages Help Consumers Understand Big Data"
-CGAP (2014), "Informed Consent: How Do We Make It Work for Mobile Credit Scoring"
-CGAP (2015), "The Potential of Digital Data: How Far Can It Advance Financial Inclusion?"
-CGAP video, "The Data Journey"
-CGAP (2016) presentation, "Potential of big data and considerations in consumer protection"
-CGAP (2016), "Big Data for Good: How Impartial Institutions Can Contribute"
-Cartesian and Gates Foundation (2014), "Using Mobile Data for Development"
-Federal Trade Commission (2016), "Big Data: A tool for inclusion or exclusion"
-World Bank (2016), "2016 World Development Report: Digital Dividends"

III. Cybercrime

Description: Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones. (Debarati Halder and K. Jaishankar). As the process

of digitization of financial services continues, the vulnerability of those services to cybercrime will continue increasing, calling for more regulatory attention.

Impact on supervisory capacity: Cybercrime presents new risks that supervisors need to better understand, e.g. mobile money in Kenya has experienced numerous attacks through social engineering, malware, and account personifications. In 2016, Serianu produced a report that looks at the current state of Kenya's cyber-security landscape. They estimate the cost of cybercrime for the following countries: Nigeria: $550 million USD, Kenya: $175 million, Tanzania: $85 million, Ghana: $50 million, Uganda: 35 million. Estimate for all of Africa: $2 billion.

Direct impact on low-income consumers: One of the most critical challenges facing FSPs is the lack of awareness among technology users. Many of these users (including customers and employees) have little knowledge of the level of risk they are exposing themselves and their organizations to. These security lapses have exposed many users to phishing and other social engineering related attacks.

Examples: Kenya's cybercrime framework consists of the Kenya Information and Communications Technology Sector Policy of 2006, the Kenya Information and Communications Act of 1998 with its amendments and the Kenya Information and Communications Regulations of 2010, among other legal instruments. The Communication Authority of Kenya established the National Computer Incident Response Team Coordination Centre, which offers technical advisories on cyber security matters to relevant stakeholders nationally and coordinates cyber incident response in collaboration with relevant actors locally, regionally and internationally. **Uganda**'s Communications Commission, through the Ugandan National Task Force on cybercrime legislation, is now part of a regional initiative, called the East African Countries' Task Force on Cyber Laws, which is dedicated to an ongoing process of development and harmonization of cybercrime laws in the East African region. In **Zambia**, the Communications Authority was reported to have assisted in drafting new cybercrime-related legislation, namely the Electronic Communications and Transactions Act 2009. (ITU 2012)

References as of October 2017

-Basel Committee on Banking Supervision (2015), "Range of practice in the regulation and supervision of institutions relevant to financial inclusion"
-BBC (2015), "Cyber-crime is Africa's 'next big threat', experts warn"
-CGAP (2016), "Protecting Digital Financial Data: What Standard-Setters Can Do"
-CGAP (2015), "Doing Digital Finance Right"
-CGAP (2015), "Responsible Digital Finance for Kenyan Merchants: Five Priorities"
-Caruana speech for GPFI SSBs 2016 conference (2016), "Financial inclusion and the fintech revolution: implications for supervision and oversight"
-Convention on Cybercrime (aka "Budapest Convention")
-GPFI White Paper (2016), "Global Standard-Setting Bodies and Financial Inclusion: The Evolving Landscape"
-Global Forum on Cyber Expertise (2017), "Cyber crime and cyber security trends in Africa"
-ITU (2012), "Understanding cybercrime: Phenomena, challenges and legal response"
-Serianu (2016), "Kenya: Cybersecurity Report 2016"
-World Bank (2016), "2016 World Development Report: Digital Dividends"
-World Bank blog (2016), "Well-regulated financial technology boosts inclusion, fights cyber crime"

IV. Data Privacy

Description: Data privacy is defined as the appropriate use of (personal) data. The success of financial inclusion efforts largely depends on financial service providers' capacity to leverage available customer data for better delivery of more suitable financial services and products without compromising customers' privacy.

Impact on supervisory capacity: Policy makers are challenged to ensure that data generated by (low-income) consumers' use of mobile phones and digital financial services are appropriately protected and can be accessed

by appropriate users, while shielded from those who would abuse it. New technologies, new business models, and new players in the digital financial inclusion space raise new risks around data privacy (see Kopa Leo example in Kenya). Effective data and privacy protection requires substantial intra- and international coordination as the data is being generated and shared across sectors and jurisdictions.

Direct impact on low-income consumers: Data generated by low-income consumers' use of mobile phones and digital financial services can help expand financial inclusion (see Big data analytics), but its use can also result in the loss of privacy and other harm. As digital financial inclusion increases, more individuals and institutions (agents, MNOs, banks, and other financial and non-financial firms) are handling more personally identifying data of customers than ever before. Digital financial inclusion may technically enable easier and broader access that may facilitate large-scale surveillance and data appropriation. Customer-centered security measures such as the use of PINs may not provide appropriate protection in the inclusion context. Hacking risks, including the vulnerability of cheap smartphones to malware, and the possibility of large-scale cyber-attacks give rise to real concerns about data security. The future impact of such data loss and privacy breaches is difficult to assess as the ability to abuse data escalates in parallel with technological advances relating to the collection, retention, and analysis of data. A lack of data privacy can have unforeseen consequences. For example, stolen data (e.g., identity theft) can be used for fraud or other criminal purposes, and may result in a number of adverse effects, including material loss or blacklisting records in a credit bureau. Lack of data privacy can pose nonfinancial risks as well, such as access by government entities to sensitive personal data or its use for political purposes. If customers fear their privacy is being violated, and that their personal information may be used in ways they are not comfortable with, then they may be less likely to use formal financial services.

Examples: The Constitution of **Kenya** 2010 guarantees citizens the right to privacy and stipulates under Article 31 that "every person has the right to privacy, which includes the right not to have information relating to their family or private affairs unnecessarily required or revealed." In **Ghana,** there is a new Data Privacy Commission under the Ghana Data Protection Act 2012. This Commission was "established to protect privacy by regulation of the processing of information and by providing a process for collecting, using and disclosing personal information." This type of authority could coordinate with financial and telecommunications authorities to monitor data privacy in digital credit products. **Nigeria** also has a relatively positive policy and legal environment, including the passage of a cybercrime act to define penalties for breaches of data security. The agency also conducted a privacy assessment in 2013, while a set of policies on privacy have been adopted by the government. As a draft bill on data protection is currently being reviewed by Parliament, there are currently insufficient legal safeguards for privacy and data protection. **Côte d'Ivoire** passed a law on the Protection of Personally Identifying Information in 2013. The law is a codification of the 2008 Economic Community of West Africa States (ECOWAS) treaty and supplementary 2010 act on privacy. It is highly developed in a number of regards, including the establishment of a comprehensive legal system for processing and circulating PII for government and private entities irrespective of context, a prohibition against the transfer of personal data to third countries that do not offer adequate protection, recognition of the right to be forgotten, the right to personal data portability, and the right to refuse personal profiling. **Economic Community of West African States** has a Supplementary Act on data protection since 2010.

References as of October 2017

-CGAP (2012), "Implications of Data Tracking on Financial Inclusion"
-CGAP (2016), "Protecting Digital Financial Data: What Standard-Setters Can Do"
-CGAP (2016), "503.2 Million Reasons to Tackle Data Protection Now"
-CGAP (2016), "Making the Case for Privacy for the Poor"
-CGAP (2016), "Time to Take Data Privacy Concerns Seriously in Digital Lending"
-CGAP (2016), "3 Steps Policymakers Can Take Now on Digital Credit"
-CGAP (2017), "India Stack: Major Potential, but Mind the Risks"

-GPFI (2016), "Global Standard-Setting Bodies and Financial Inclusion: The Evolving Landscape"
-IIF (2017), "Deploying RegTech against financial crime"
-Serianu (2016), "Kenya: Cybersecurity Report 2016"
-ITU (2012), "Understanding cybercrime: Phenomena, challenges and legal response"
-African Union Convention on Cyber Security and Personal Data Protection
-World Bank (2016), "2016 World Development Report: Digital Dividends"
-World Bank (2017), "The State of Identification Systems in Africa"
-ID4Africa (2015), "Digital Identity: The Essential Guide"

V. Digital Credit

Description: Digital credit—offering quick small loans remotely over digital channels—is a rising trend in sub-Saharan Africa, with 20 deployments in Kenya alone. The most visible example is the rapid success of the small value credit and savings service M-Shwari in Kenya launched in late 2012.

Impact on supervisory capacity: The product features and business models associated with digital delivery of credit can create new risks, elevate existing risks or shift the incidence and the party responsible for managing risks. Among the potential financial consumer protection concerns are how transparency, fair treatment, prevention of over-indebtedness or debt stress, and effective recourse standards may be achieved when services are delivered digitally and key functions or roles of the lending process are shared or outsourced. Another concern is achieving adequate and equal protection for consumers when some digital lenders are licensed and supervised and others are not. Such risks could affect significant numbers of consumers that have relatively low levels of income, education and formal financial experience, since the models currently observed in various markets can and do scale rapidly and the lenders are not always supervised by financial authorities (particularly PAYG service providers may be out of the traditional supervisory remit).

Direct impact on low-income consumers: Digital credit can benefit borrowers as an alternative to informal lending sources - it can help meet emergency liquidity needs of poor households and provide a first step into formal financial services. Consumers may behave differently when presented with relatively "instant" loans in a completely confidential context, when compared with conventional small loans processes.

Examples: DRC (Libiki - cash advance)**, Ghana** (Mjara, Jumo)**, Malawi** (kutchova loan), **Niger** (orange emergency credit Aagadi)**, Rwanda** (MoKash, Jumo), **Tanzania** (M-Pawa, Timiza, Jumo), **Uganda** (MoKash, Jumo), **Kenya** (M-Shwari, Mkopo Rahisi, KCB M-Pesa, Eazzy Loan, Branch, pesa na pesa, Jumo, etc - as of 2016, there are more than 20 deployments), **Zambia** (Jumo), **Zimbabwe** (EcoCash Loan). Other digital credit deployments covered by CGAP include: Philippines (Instaloan), Mexico (mimoni), Pakistan (easypaisa), India (Mobikwik). Tiaxa offers balance advances (nano credit that can be as little as 2 cents) in Colombia, Peru, Mexico, Argentina.

References as of October 2017

-AFI (2015), "Digitally Delivered Credit: Policy Guidance Note and Results from Regulators Survey"
-Center for Financial Inclusion (2016), "Digital Credit in Africa: Are Nano Loans Safe for Consumers?"
-CGAP (2014), "Leveraging Mobile Phone Data: Tiaxa's Balance Advance"
-CGAP (2016), "Proliferation of Digital Credit Deployments"
-CGAP (2016), "Four Common Features of Emerging Digital Credit Offerings"
-CGAP (2016), "An Introductory Course to Digital Credit"
-CGAP (2017), "Digital Credit's Evolving Landscape: 3 Things You Need to Know"
-CGAP (2016), "The Unusual Financial Dynamics of Short-Tenor Digital Credit"
-CGAP (2017), "Consumer Protection in Digital Credit"
-Financial Stability Board (2017), "FinTech Credit: Market Structure, Business Models and Financial Stability Implications"
-ITWeb Africa (2016), "Tigo Tanzania launches nano lending scheme"
-MicroCapital (2016), "MicroCapital Brief: MyBucks Launches Mobile App Offering "Nano-loans" in Kenya"

-Omidyar (2016), "Big Data, Small Credit"
-OPIC (2015), "Tiaxa: Using Leapfrog Technologies to Provide "Nano-Credits" to Millions"

VI. Digital ID

Description: Digital identity is a set of electronically captured and stored attributes and credentials that can uniquely identify a person and individualize that person in a computer-based environment. Digital ID systems are registries that store personal data in digital form and credentials that rely on digital, rather than physical, mechanisms to authenticate the identity of their holder. Digital identity's importance is now recognized in the post-2015 development agenda, specifically as a Sustainable Development Goal (SDG).

Impact on supervisory capacity: Policy makers face the challenge of adopting a framework that would allow electronic identification of individuals and entities (e.g., using biometrics or Big data analytics), while ensuring right safeguards are put in place and avoiding unintended consequences such as inadvertent exclusions, onerous mandates that could deter individuals from accessing services, or increased rent-seeking involving registration or certificates. This includes identifying an authority (public or private) responsible for issuing IDs, building and overseeing a database with ID-related information etc. Supervisors may have concerns about how to best determine the types, extent, and use of information collected under digital ID schemes; how to safeguard the privacy of personal data. The opportunity for supervisors is in increasing capacity to monitor implementation of AML/CFT requirements.

Direct impact on low-income consumers: Over 1.5 billion people in the developing world lack any form of officially recognized identification, either paper or electronic-based. This identity gap is a serious obstacle for participation in political, economic, and social life—without a secure way to assert and verify her identity, a person may be unable to open a bank account, vote in an election, access education or healthcare, receive a pension payment, or file official petitions in court. Furthermore, poor identification systems mean that states will have difficulty collecting taxes, targeting social programs, and ensuring security. Digital ID systems like Aadhaar in India facilitate consumers' ability to open a bank account instantly and without any other documentation, get a loan, and receive government payments. At the same time, massive government databases raise fraud/security, privacy and civil liberties concerns.

Examples: The World Bank assessed the state of identification systems in 17 countries in Africa in 2017 through its ID4D program. Five countries have relatively advanced identity ecosystems compared to the rest: **Botswana, Kenya, Morocco, Namibia and Rwanda**. What sets these countries apart is the progress they have made in increasing the coverage and use of their foundational identity systems and ensuring that processes to register individuals and establish uniqueness are relatively robust. This robustness relies both on technology (e.g., biometric deduplication and credential security features) and local-level vetting and identity validation. In addition, they have partially or fully digitized and harmonized their identity ecosystems. In **Rwanda**, for example, the National ID is held by approximately 90 percent of the adult population (or 52 percent of the total population), and is used to access virtually all government services, travel in the EAC region, open bank accounts, and vote in elections. **Kenya** has adopted a government-wide e-Governance strategy, including shifting services to an "e-citizen" web portal that requires the NID number and name to log-on. As of the IMSA report, there were 295,000 registered e-citizen users, and the government received some KSH 8 million in fees and payments daily (e.g., renewing licenses and passports, etc.). Kenya's ability to uniquely identify the holders of bank and mobile accounts has also facilitated the integration of financial information, including the creation of a Credit Reference Bureau, which has led to a substantial decline in the share of non-performing loans. Intermediate identity ecosystems were found in the following countries: **Cameroon, Chad, Cote d'Ivoire, Madagascar, Nigeria, Tanzania, and Zambia.** These countries all have operational civil registration and identification systems; however, they have not yet reached the level of coverage, harmonization, or functionality of the more advanced countries. Nigeria has

tried to roll out a National e-ID system with limited success so far. However, Nigeria provides an example of a private sector driven initiative with Bank Verification Number (BVN) as an attempt to create means for identification of banking customers in the absence of a national ID.

References as of October 2017
-CGAP (2014), "Could India's Unique ID be a Financial Inclusion Game-Changer?"
-CGAP (2015), "Digital Financial Inclusion: Implications for Customers, Regulators, Supervisors, and Standard-Setting Bodies"
-CGAP (2017), "India Stack: Major Potential, but Mind the Risks"
-European Commission (2017), "Ministerial Declaration on eGovernment - the Tallinn Declaration"
-FSD Africa (2017), "Anti-Money Laundering, Know Your Customer, and Curbing the Financing of Terrorism"
-GPFI (2015), "Innovative Digital Payment Mechanisms Supporting Financial Inclusion: Stocktaking Report"
-GSMA, World Bank, Security Identity Alliance (2016), "Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation"
-ID4Africa (2015), "Digital Identity: The Essential Guide"
-World Bank Identification for Development (ID4D)
-World Bank (2014), "Digital identity toolkit: a guide for stakeholders in Africa"
-World Bank (2016), "2016 World Development Report: Digital Dividends"
-World Bank (2017), "The State of Identification Systems in Africa"
-Wharton Fintech (2016), "The Bedrock of a Digital India: An overview of the India Stack and its disruptive potential"

VII. Digital Fiat Currency

Description: Digital fiat currencies are national currencies issued in digital form by central banks. Not implemented yet, the idea of digital fiat currencies is being actively explored by several governments. The idea has been largely inspired by a related concept of cryptocurrencies or virtual currencies (VCs) that are digital representations of value, issued by private developers, and denominated in their own unit of account. The concept of VCs covers a wider array of "currencies," ranging from simple IOUs of issuers (such as Internet or mobile coupons and airline miles), VCs backed by assets such as gold, and cryptocurrencies such as Bitcoin. While the significance of VCs largely depends on use cases, a digital fiat currency may (and likely will) disrupt the way our society transacts and uses money.

Impact on supervisory capacity: Digital fiat currency will present new risks to supervisors given the new technology involved, but it will also reduce use of cash and related AML/CFT risks. DFC will also give the central bank better control over money flows. A central bank-issued digital fiat currency may improve the oversight capacity, while providing new methods of monetary policy.

Direct impact on low-income consumers: The adoption of digital fiat currency is expected to drive the expansion of the digital payments ecosystem by offering a secure, interoperable payment instrument.

Examples: Countries exploring digital fiat currencies include: Australia, Canada, China, Ecuador, Sweden, **Tunisia**, Ukraine. The United Kingdom is experimenting with the concept. **India** has also announced its intention to pursue digital fiat currency.

References as of October 2017
-Bloomberg (2015), "JPMorgan says not to worry as Ecuador promotes digital currency"
-Economic Times India (2016), "Time for a digital fiat currency in a digital India"
-Financial Times (2016), "Central banks explore blockchain to create digital currencies"
-Forbes (2016), "Canada has been experimenting with a digital fiat currency called CAD-COIN"
-The Guardian (2015), "Ecuador launches new digital currency - but most residents know little about it"
-Indian Ministry of Finance (2016), "Committee on Digital Payments: Medium Term Recommendations to Strengthen Digital Payment Ecosystem"

-ITU blog (2017), "How digital fiat currency issued by Central banks will drive financial inclusion"
-ITU (2017), "ITU Creates New Focus Group to Investigate Digital Currency Including Digital Fiat Currency"

VIII. Distributed Ledger Technology

Description: Distributed ledger technology (DLT) is a new type of secure ledger for keeping track of various records in digital form, but without the need for a centralized controller of this data. Instead, the data is shared in a peer-to-peer manner across multiple sites, countries, or institutions. DLT has the potential to speed up and reduce the cost of transactions, give individuals more control over their personal data, reduce or remove the need for costly intermediaries, provide secure 'smart' legal contracts that execute without user intervention, bolster data security due to enhanced cryptography, and revolutionize regulatory compliance.

Impact on supervisory capacity: Impact of DLT on policymakers (regulators and supervisors) is largely unknown. Perhaps even more than with other innovations mentioned in this document, it is true that policymakers need to pay increased attention to DLT and the way it evolves in order to be able to adopt appropriate regulatory and supervisory actions.

DLT may pose new or different risks, including: (i) potential uncertainty about operational and security issues arising from the technology; (ii) the lack of interoperability with existing processes and infrastructures; (iii) ambiguity relating to settlement finality; (iv) questions regarding the soundness of the legal underpinning for DLT implementations; (v) the absence of an effective and robust governance framework; and (vi) issues related to data integrity, immutability and privacy. DLT is an evolving technology that has not yet been proven sufficiently robust for wide scale implementation. Potentially, the most significant impact may be in improving financial markets infrastructure, its resilience, and the capacity to regulate and oversee financial markets.

Direct impact on low-income consumers: Use cases can vary and include virtual currencies, digital ID and others described in this document. However, due to novelty of this innovation it remains to be seen what use cases will have largest impact on financial inclusion. Some applications that may be particularly useful for financial inclusion include: remittances; developing new identity systems; interoperability between digital financial services (DFS) and banking platforms; innovative, self-executing 'smart contracts'; micro-insurance uses; clearing and settlement in payment systems; credit provision; and property and land registration.

Examples: Bitpesa is a Kenya-based remittance provider that enables the exchange of bitcoin for Kenyan Shillings, and allows users in **Kenya, Nigeria, Uganda** and **Tanzania** to send fiat funds to popular DFS wallets. It also has a corridor to China. See www.bitpesa.co. In **Nigeria**, Stellar (which operates as a decentralized protocol for fund transfers in any pair of currencies), and Oradian, a cloud-based software provider for microfinance institutions in developing countries, have partnered to bring instant money transfers to Nigeria. In **Ghana** (pilot using DLT as a decentralized land registry), **Nigeria** (money transfers using DLT), **Kenya** (WB supported project on blockchain bonds).

References as of October 2017

-Bank of Canada, Payments Canada, and R3 (2017), "Project Jasper: A Canadian Experiment with Distributed Ledger Technology for Domestic Interbank Payments Settlement"
-Center for Global Development (2017), "Making Blockchain Technology Work for Development: The Need for Data and Dialogue"
-CGAP (2016), "Protecting Digital Financial Data: What Standard-Setters Can Do"
-Coindesk (2017), "World Bank to Support Blockchain Bonds Trial in Kenya"
-Cognizant (2016) for the World Bank, "Blockchain Powered Financial Inclusion"
-CPMI Report (2017), "Distributed ledger technology in payment, clearing and settlement - An analytical framework"
-European Central Bank (2016), "In Focus: Distributed Ledger Technology"

-Federal Reserve speech of Governor Brainard (2016), "The Use of Distributed Ledger Technologies in Payment, Clearing, and Settlement"
-GPFI White Paper (2016), "Global Standard-Setting Bodies and Financial Inclusion: The Evolving Landscape"
-IIF (2017), "Deploying RegTech against financial crime"
-IMF (2016), "The Internet of Trust"
-IMF Staff Discussion Note (2016), "Virtual Currencies and Beyond: Initial Considerations"
-ITU-T Focus Group DFS (2017), "Distributed Ledger Technologies and Financial Inclusion"
-Let's Talk Payments (2016), "How Blockchain Is Facilitating Financial Inclusion in Africa"
-UK Government Chief Scientific Adviser (2015), "Distributed Ledger Technology: beyond the block chain"
-World Bank (2016), "2016 World Development Report: Digital Dividends"

IX. FinTech

Description: FinTech is an amalgamation of the words "financial" and "technology". It refers to the use of new technologies in the financial services industry to improve operational and customer engagement capabilities by leveraging analytics, data management, and digital functions. At a faster pace than ever before, technology is shaping the future of financial services, creating new opportunities for reaching previously financially excluded consumers but also new challenges for regulators and policymakers to ensure such technologies are deployed in a way which does not compromise consumer protection or financial stability.

Impact on supervisory capacity: With FinTech, supervisors are facing important challenges to carry out their mandates effectively in the context of an increasingly complex financial sector landscape, with evolving risks and multiple types of actors, products, services, and channels. Supervisory frameworks developed for different circumstances may leave important actors and activities outside the supervisory perimeter and may open new opportunities for regulatory arbitrage. In multiple jurisdictions, financial supervisors are being called upon to work with other government entities to adapt their legal, regulatory, and supervisory frameworks and redefine their supervisory perimeter, for example, through the creation of new categories of financial institutions or by assigning to financial supervisors the responsibility for financial institutions that were previously under the remit of other authorities or excluded from financial regulation and supervision altogether.

In recent years, supervisory agencies have seen their responsibilities expanding substantially and their capacity and resources lagging behind, while the international community has not developed enough guidance on ways to improve supervisory effectiveness. This is especially true in emerging and developing economies where digital financial inclusion is advancing. Supervisors once responsible only for prudential supervision of a few banks now may also find themselves supervising microfinance institutions and issuers of electronic money, may have seen financial consumer protection, financial education and financial inclusion added to their mandates, and must in any event keep abreast of fast-paced technological innovations (including a proliferation of FinTech companies).

Direct impact on low-income consumers: As new tools and technologies are developed, and old business models are challenged, financial services can be provided to consumers with greater speed, accountability, and efficiency. Access to financial products and services is becoming more attainable than ever, especially for consumers that live in rural locations or regions without the structures of a modern economy. Not only can fintech make financial products and services more accessible (particularly taking into account availability of affordable mobile phones and cellular networks), it can also make them more affordable by lowering the cost of doing business for the financial institution, a savings which can be passed on to the consumer.

Examples: See examples in FinTech-related emerging trends, including Application Programming Interfaces (APIs), Big data analytics, Digital Credit, Digital Fiat Currency, Digital ID, Distributed Ledger Technology, and RegTech. Also, refer to this CGAP blog post "Mapping Africa's Latest Innovations in Digital Finance".

References as of October 2017

-Basel Committee on Banking Supervision (2017), "Implications of fintech developments for banks and bank supervisors - consultative document"
-CGAP (2014), "5 Sources of Untapped Innovation in Digital Finance"
-CGAP (2015), "Global landscape of innovations in digital finance"
-CGAP (2015), "What Could Digital Finance Look Like in 10 Years?"
-CGAP (2016), "Risk-Based Supervision in the Digital Financial Inclusion Era"
-CGAP (2016), "Six Tips for Policy on Disruptive Digital Financial Inclusion"
-CGAP (2017): "Mapping Africa's Latest Innovations in Digital Finance"
-CGAP (2017), "Digital Finance in China"
-GPFI (2016), "Global Standard-Setting Bodies and Financial Inclusion: The Evolving Landscape"
-Financial Stability Board (2017), "FinTech Credit: Market Structure, Business Models and Financial Stability Implications"
-FSB - Mark Carney's speech (2017), "The Promise of FinTech – Something New Under the Sun?"
-FSB (2017), "Financial Stability Implications from Fintech"
-InterAmerican Development Bank (2017), "FINTECH: Innovaciones que no sabías que eran de América Latina y Caribe"
-IMF (2017), "Fintech and Financial Services: Initial Considerations"
-Accenture (2016), "Fintech and the evolving landscape: landing points for the industry"
-World Economic Forum (2015), "The Future of FinTech: A Paradigm Shift in Small Business Finance"
-World Bank (2017), "Leveraging 'SupTech' for financial inclusion in Rwanda,"
-World Bank(2017), "Can 'fintech' innovations impact financial inclusion in developing countries?"

X. Innovation Facilitators

Description: Innovation facilitators are designed to promote and facilitate financial innovation, particularly FinTech. They may be set up by private sector stakeholders, public sector stakeholders and/or as a PP partnership. They may take different forms (sandboxes, incubators, accelerators etc.) and shapes (e.g., a policy framework, a platform, testing infrastructure etc.).

Impact on supervisory capacity: For regulators, among the most important benefits of regulatory sandboxes include: containing risks of innovations while not stifling them and generating insights to inform regulation and supervision of the new innovations. A regulatory sandbox, however, creates a demand for supervisory resources given that the regulator advises the sandboxed entity on legal and regulatory requirements. As FinTech startups become an immense part of the global financial system, an appropriate environment is required to understand and leverage opportunities presented by new entrants. Regulatory sandboxes have become a framework in which regulators, financial institutions, entrepreneurs and industry professionals can interact and better understand each other. For innovative companies, benefits of participating in an innovation facilitator are: reduced time to market, opportunity to contain consequences of failure, enhanced access to capital, curated quality of products reaching national markets, and regulatory relief. Over the past couple years, a few (~18) international financial authorities have launched or announced regulatory sandboxes, creating safe environments to take risks

Direct impact on low-income consumers: As new tools and technologies are developed, and old business models are challenged, financial services can be provided to consumers with greater speed, accountability, and efficiency. Access to financial products and services is becoming more attainable than ever, especially for consumers that live in rural locations or regions without the structures of a modern economy.

Examples: Kenya (CMA consulting a regulatory sandbox concept), *Sierra Leone* (interested in a regulatory sandbox), UK, Hong Kong, Malaysia, Singapore, Australia, Abu Dhabi, Indonesia, Ontario Securities Commission (Canada), Thailand. Proposed regulatory sandboxes in: US, India, Switzerland, Netherlands, Norway, Russia, Dubai, and Taiwan. Insurance regulators are also starting to take a test and learn approach (different from a regulatory sandbox): in **Ghana**, the National Insurance Commission (NIC) allows mobile insurance products to be tested on a case-by-case basis, checking the commercialization agreements between the MNO, the Technical Service Provider and Insurer in advance and closely monitoring activities thereafter.

References as of October 2017
-CGAP (2016), "Six Tips for Policy on Disruptive Digital Financial Inclusion" -CGAP (2017), "Regulatory Sandboxes and Financial Inclusion" -CGAP (2017), "RegTech: Are Supervisors Ready for the Data Revolution?" -Bank of England, speech of Mark Carney (2017), "The Promise of Fintech - Something New Under the Sun?" -FSD Africa (2017), "Crowdfunding in East Africa: Regulation and Policy for Market Development" -Forbes (2016), "Asian Fintech Sandboxes - Can They Work and Do We Need Them?" -GPFI (2017) "Digital Financial Inclusion: Emerging Policy Approaches" -Industry Sandbox (2017), "A Development in Open Innovation: Consultative Report" -ITU-T Focus Group DFS (2017), "Distributed Ledger Technologies and Financial Inclusion" -Let's Talk Payments (2016): "International FinTech Regulatory Sandboxes Launched by Forward-Thinking Financial Authorities" -Monetary Authority of Singapore (2016), "FinTech Regulatory Sandbox Guidelines" -University of Oxford (2016), "Overview of Regulatory Sandbox Regimes in Australia, Hong Kong, Malaysia, Singapore and the UK" -UNCDF (2017), "A Regulatory Diagnostic Toolkit for Analyzing the Regulatory Frameworks for Digital Financial Services (DFS) in Emerging Markets" -United Kingdom FCA (2017), "Regulatory sandbox lessons learned report"

XI. RegTech

Description: RegTech focuses on the technologies that may facilitate the delivery of regulatory requirements more efficiently or effectively than existing capabilities (UK's Financial Conduct Authority) and can be divided into two categories, (i) regulator-facing, focusing on work flow and process automation, offsite supervision, and market monitoring ("SupTech"), and (ii) industry-facing, focused on reducing the cost of compliance and enabling compliance (e.g., AML/CFT requirements).

Impact on supervisory capacity: RegTech solutions can improve the quality and efficiency of supervision by improving the timeliness and accuracy of reporting of FSPs. With this new wealth of information at its disposal, supervisors can also adapt their supervisory processes and methodologies to fully leverage the collected data and allocate supervisory resources more efficiently. At the FSPs level, RegTech can improve internal compliance and risk management processes, leading to improved stability, integrity and market conduct.

Direct impact on low-income consumers: RegTech solutions can lower costs of FSP compliance, leading to lowers costs of products that may be passed on to the customer. In addition, better supervisory tools for the regulator lead to strengthened stability, integrity, and market conduct, thus improving customer trust.

Examples: Rwanda (National Bank of Rwanda is in the process of implementing an automated financial reporting and supervision system that will allow BNR to automatically pull data from financial institutions' core MIS (for those that have them), thus improving the accuracy, integrity, and timeliness of offsite reporting data); Vizor - a tech company offering a RegTech platform for supervisors, serves regulators and supervisors in **Botswana, Ghana, Kenya, Namibia, and Tanzania**. Austria (OeNB), in collaboration with the banking industry, introduced a new software platform 'Aurep' to streamline the data collection and regulatory reporting process for banks in Austria. The UK FCA has Project Innovate, the regulatory sandbox and the dedicated robo-advice unit, while the Bank of England has launched FinTech Accelerator to incentivize fintech startups to work on RegTech solutions for BoE. The **Philippines and Mexico** (along with **Ghana**) are part of the RegTech for Regulator Accelerator (R2A). In **Brazil**, the Central Bank of Brazil has developed a technology solution for what is called remote examination. Through a system called Siscom (Integrated System for Supervision Support and Communication), supervisors can collect data and documents remotely and interact online with financial institutions. It standardized supervisory tasks,

automated bureaucratic functions (such as filing documents), and allowed supervisors to reach small financial institutions in a cost-effective way, increasing the productivity of supervision teams.

References as of October 2017

-AFI (2017), "Opening remarks by AFI Chair Prof. Benno Ndulu at the 9th G24/AFI Roundtable"
-CGAP (2016), "Risk-Based Supervision in the Digital Financial Inclusion Era"
-CGAP (2017), "RegTech: Are Supervisors Ready for the Data Revolution?"
-Deloitte (2015), "RegTech is the new Fintech"
-Digital Frontiers Institute video, "What is regtech and why does it matter?"
-Ernest & Young (2015), "Innovating with RegTech: Turning a Regulatory Compliance Into a Competitive Advantage"
-Financial Times (2016), "Market grows for 'regtech', or AI for regulation"
-Forbes (2016), "The Rise of RegTech and What It Means For Your Business"
-GPFI (2017), "Digital Financial Inclusion: Emerging Policy Approaches"
-Institute of International Finance (2016), "RegTech in Financial Services: Technology Solutions for Compliance and Reporting"
-Institute of International Finance (2017), "Deploying RegTech against financial crime"
-Medium (2016), "RegTech is real and 120+ startups to prove it"
-NextBillion (2017), "RegTech for Regulators: Reimagining Financial Supervision and Policymaking"
-Northwestern Journal of International Law & Business (2016), "FinTech, RegTech and the Reconceptualization of Financial Regulation"
-TechCrunch (2017), "The real promise of regulatory technology"
-World Bank (2017), "8 key approaches to accelerate financial inclusion"

B. Other Trends

XII. Artificial intelligence (machine learning)

Description: Artificial intelligence (AI) is a computer system able to perform tasks that normally require human intelligence. Examples include tasks such as visual perception, speech recognition, decision-making under uncertainty, learning, and translation between languages. Faster computing, "big data," and better algorithms have helped propel recent breakthroughs in AI. The field of AI has produced a number of cognitive technologies (performing specific tasks that only humans used to be able to do), including machine learning and speech recognition. Machine learning refers to the ability of computer systems to improve their performance by exposure to data without the need to follow explicitly programmed instructions. At its core, machine learning is the process of automatically discovering patterns in data. Once discovered, the pattern can be used to make predictions. A sub-category of machine learning is deep learning. (Ro)bots are machines and/or software capable of carrying out a complex series of actions automatically either based on their artificial intelligence or programmed code. Chatbots are computer programs designed to simulate conversation with human users, especially over the Internet.

Impact on supervisory capacity: AI presents challenges to supervisors in the form of new risks arising from the entrance of unregulated fintech firms, use of Big data analytics and the changing nature of activities performed by FSPs (supervision of individuals vs. supervision of algorithms). Unresolved are many questions surrounding liability (civil, criminal, administrative) of AI for the acts it performs. AI also presents an opportunity for supervisors in the form of AI-powered supervisory tools (see RegTech).

Direct impact on low-income consumers: FinTech innovators use artificial intelligence (specifically, machine learning) to assess credit worthiness and offer new digital credit products to the underserved (eg MyBucks, Lenddo). AI has a wide variety of consumer-level applications for smarter and more error-free user experiences. Personal finance applications are now using AI to balance people's budgets based specifically to a user's behavior. AI now also serves as robo-advisors to casual traders to guide them in managing their stock portfolios. For enterprises, AI is expected to continue serving functions such as business intelligence and predictive analytics. Merchant services such as payments and fraud detection are also relying on AI to seek out patterns in customer behavior in order to weed out bad transactions. Chatbots are being tested for purposes of financial education, marketing, complaints handling. AI and bots can be used by FSPs and financial sector regulators/supervisors to streamline their internal processes.

Examples: MyBucks, a German listed FinTech company that holds three brands GetBucks, GetSure and GetBanked, has an in-house AI team to help with assessing credit worthiness, assist in collections, and fraud detection. They operate in **Ghana, Kenya, Tanzania** and **Mozambique**. Fintech companies are using AI technologies to offer digital credit (see Big data analytics). CGAP has also worked with Juntos, a two-way conversational platform that uses machine learning, in partnership with mobile money providers and banks, to increase usage of mobile wallets and deposits in savings accounts. Juntos had a pilot in **Tanzania** (as well as Colombia, Mexico, Indonesia, Philippines). Arifu in cooperation with TechnoServe has piloted a chatbot (over USSD channel) to improve financial literacy of micro and small entrepreneurs in Tanzania.

References as of October 2017
-World Bank (2016), "2016 World Development Report: Digital Dividends -Microfinance Gateway, "Five InsureTech Trends and What They Mean for Microinsurance" -Deloitte University Press (2014), "Demystifying artificial intelligence"

-Wired (2017), "How AI is transforming the future of fintech"
-IT News Africa (2016), "FinTech business in Africa makes use of AI and credit technology"
-World Bank blog (2015), "Are we heading towards a jobless future?"
-The Financial Services Forum, "The Application of AI in Financial Inclusion"
-The Next Web, "Why AI will determine the future of fintech"

XIII. Biometrics

Description: Biometrics technology measures an individual's unique physical or behavioral characteristics, such as fingerprints, facial characteristics, voice pattern and gait, to recognize and confirm identity. See also Digital ID.

Impact on supervisory capacity: With biometrics supporting a digital ID system, AML/CFT regulatory concerns are eased. While these technologies come with great potential, they also bear risks such as the risk of fraud and issues concerning data protection and privacy, which needs to be addressed by regulators and supervisors.

Direct impact on low-income consumers: In many developing countries, the identification of poor people is a challenge, since the poor often do not hold formal identity documents such as birth certificates, ID cards, driver's licenses or passports. Biometrics may provide a solution to this problem. Identification based upon fingerprints, facial metrics or voice scans promises to establish secure identities. Secure identification is a precondition for accessing financial services. It is likely that remote identification through biometrics will become more important with the rise of mobile banking. Across the world an increasing number of countries are introducing biometric identity cards. The latest—and largest—examples is India, where Aadhaar - an online biometric identity service, has enrolled more than 1 billion people and is used for KYC for financial institutions and transfers of social payments, among other services. Biometrics establish unique identity, thereby reducing the barriers for customers to open a financial account, meeting FSPs' identification requirements. Biometrics can also increase financial security (protection from fraud). However, if biometric data is compromised (e.g. biometric databases could be hacked), it can have a strong negative impact on the individual's life. Therefore, it is important that identification data is kept securely, periodically updated, and should the data be compromised, there must be the possibility of re-issuance.

Examples: MasterCard and South African Social Security Agency distributed 10 million MasterCard debit cards to social grant beneficiaries in **South Africa**. The cards allow for authentication of identities using biometrics, e.g. fingerprints, voice detection. In **Nigeria**, the Central Bank of Nigeria's Bank Verification Number program captures an individual's biometric data including facial image, 2 thumbs and index fingerprints. The individual can then use their BVN to verify their identity at their bank, at which point, they will be given a permanent unique number which will be synchronized for other banking transactions. **Pakistan** has a Computerized National Identity Card and biometric SIM verification for remote mobile wallet account opening. In **India**, see above on Aadhar.

References as of October 2017

-GPFI (2017), "Digital Financial Inclusion: Emerging Policy Approaches"
-Biometric update (2015), "Nigeria's Central Bank extends biometric identification deadline"
-MasterCard press release (2013), "Ten Million SASSA MasterCard Cards Issues to South African Social Grant Beneficiaries"
-CGAP (2004), "Biometrics Technology"
-CGAP (2014), "Could India's Unique ID be a Financial Inclusion Game-Changer?"

-CGAP (2015), "From Cash to Digital Transfers in India: The Story So Far"
-CGAP (2016), "Unlocking Financial Inclusion Using Biometrically Verified SIMs"
-CGAP (2017), "India Stack: Major Potential, but Mind the Risks"
-FSD Africa (2017), "Anti-Money Laundering, Know Your Customer, and Curbing the Financing of Terrorism"
-LiveMint (2017), "Aadhar arguments: For and against"
-AFI (2013), "Biometric Identification of Customers - Pathway to Greater Financial Inclusion?"
-IIF (2017), "Deploying RegTech against financial crime"
-World Bank (2016), "2016 World Development Report: Digital Dividends"

XIV. Cloud computing and cloud banks

Description: Cloud computing is computing that uses data stored on an external server, accessed via the Internet. It's defined as ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing drives down the cost of storing data, but also the cost of implementing IT solutions through services such as "software as a service" (SaaS), infrastructure as a service (IaaS), platform as a service (PaaS), and desktop as a service (DaaS). What is today known as 'Cloud Computing' involves a major transformation of the way businesses and individuals access and use computing resources. This change is propelled by the dramatic economic advantages of cloud-based services that offer access to computing resources otherwise unaffordable to all but the largest organizations. Cloud computing eliminates the need for end users to invest in expensive hardware and software, allowing them instead to pay for access to sophisticated computing resources on an as-needed basis. While the economic advantages of cloud computing are compelling, these come at a price. Users of cloud-based services are entrusting physical custody of their data and control of critical applications to third parties. Without a clear understanding of the details behind the services upon which they are relying, end users of cloud-based services lack the ability to anticipate and address the risks that inevitably accompany this type of outsourcing arrangement. However, certain jurisdictions require that cloud computing services use facilities located within its national territory, which makes cloud computing inoperable in certain countries.

Impact on supervisory capacity: Regulators need to decide on how to regulate providers of cloud computing-related services and FSPs leveraging those services to ensure benefits brought about by cloud technologies, while providing sufficient safeguards without creating unnecessary barriers. In situations where FSPs rely on cloud-based services, supervisors may need to examine outsourcing agreements and decide where to draw the line between outsourcing and direct provision of a regulated service that should be subject to authorization and oversight. In addition, cloud computing presents challenges to supervisors including the security, integrity, and privacy of information stored in the data centers. Supervisors may also need to deal with possible systemic risks in cases where a disruption or failure of a cloud service might impact the larger economy or financial system. Benefits to regulators and supervisors have to do with digitization of the internal processes (see RegTech).

Direct impact on low-income consumers: Cloud-based services, which are often used by mobile money providers to host their software platforms, have a direct impact on lower-income customers by improving their access to DFS by driving costs of financial services down, but also by improving UI/UX due to digitization of FSP's operations.

Examples: Vodacom **Tanzania** announced that it has invested in customized Internet of Things (IoT) solutions (e.g. vehicle tracking, monitoring of retail points, etc.) and cloud computing services. MTN **Ghana** has launched cloud computing services for SMEs. IBM opened its first cloud data center in **South Africa**. Microsoft has partnered with Soft Solutions Limited in **Nigeria** to offer cloud computing services; IBM also offers cloud computing in Nigeria. Data center services for M-PESA in **Kenya** used to be hosted in Germany until 2015, when Safaricom moved the servers locally.

References as of October 2017
-USAID (2011), "Cloud Computing & Financial Services For the Poor"
-CGAP (2016), "Big Data for Good: How Impartial Institutions Can Contribute"
-ENISA (2009), "Cloud Computing: Benefits, risks, and recommendations for information security"
-ENISA (2015), "Secure Use of Cloud Computing in the Finance Sector"
-BBVA Research (2016), "Cloud Banking or Banking in the Clouds?"
-IT Web Africa (2016), "SA market geared for cloud computing"
-European Commission (2014), "Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination"
-Ghana News Agency (2013), "MTN Ghana launches cloud computing services for SMEs"
-ITU (2012), "Cloud Computing in Africa: Situation and Perspectives"
-Government of Rwanda (2014), "Rwanda to lead growth in cloud computing"
-C4DLab (2014), "Policy Brief: Cloud Computing in Kenya"
-IDG Connects (2014), "Research: Pan African Cloud Expansion"
-Telegeography (2016), "Vodacom Tanzania develops IoT, cloud computing"
-World Bank (2016), "2016 World Development Report: Digital Dividends"

XV. Competition in digital financial services

Description: As the digital financial services (DFS) ecosystem grows and becomes more competitive, a range of competitive issues relating to and affecting existing and potential market participants have emerged, including those relating to: market access and licensing; technical access to telecommunications and payment infrastructure; differential rules on the use of agents; ability to interoperate; capital requirements and safeguarding of funds; service pricing; cross-subsidization of services; quality of service; taxation; and access to big data. To promote both quality and diversity in DFS products, and in turn financial inclusion, it is important to ensure a competitive ecosystem that facilitates entry into the market, the development of innovative DFS products, and high-quality, value-for-money services. Policy makers, donors, and others promoting financial inclusion may give priority to facilitating first-movers' testing and innovating to bring products to scale and prove the viability of DFS business models during early market development, with competition issues taking a backseat. However, as DFS markets mature and become more fully integrated into the economy and consumers' financial lives, effective competition becomes increasingly important to ensuring that markets work well and to promoting financial inclusion.

Impact on supervisory capacity: Promoting and ensuring effective competition in DFS markets is central to promoting financial inclusion. Effective competition helps ensure that consumers will have access to high-quality, innovative, value-for-money products and services, which in turn will promote increased uptake and use of DFS, and creates sufficient space for new innovators to enter the market and further expand the range of products offered via mobile money channels. Market imbalances may result from unequal policy frameworks or from market conduct. The former may be from regulatory bans on or restricted access to: DFS ecosystems; disproportionate and unequal compliance and capital requirements; and inconsistent and

disproportionate tax regimes. The latter could relate to a market participant's access to fair reasonable and non-discriminatory terms to technology; critical and scarce infrastructure, services used for channel or wholesale access, discriminatory pricing of services, cross-subsidization of services, quality of service, and access to big data. There are typically three relevant regulators around competition: financial, telecommunications, and competition regulators. The overlapping jurisdiction and differences in basis for assessment and process means that coordination among the different regulators is critical.

Direct impact on low-income consumers: Price: Effective competition among DFS providers drives them to operate more efficiently and price their products competitively to attract customers, which can lead to lower costs passed on to consumers. Quality of products: Effective competition also incentivizes providers to ensure that the products they provide are high quality to retain consumers, helping adopters of products remain active users—all the more pertinent given high dormancy rates experienced by some DFS providers. Variety and diversity of products: Effective competition also incentivizes providers to introduce new and innovative DFS products and services, which promote increased uptake use. Service quality: Where consumers have increased options for products and services, service quality will be promoted as firms compete on service for fear of consumers switching providers. In DFS markets, service can impact product quality in multiple ways, including the quality of the financial product, but also the quality of the telecommunications channels and agent networks through which these services may be accessed.

Examples: In **Kenya**, Equity Bank reportedly launched Equitel, an MVNO operating over Airtel's network, chiefly in order to provide mobile financial services without the high costs imposed by dependence on competitor Safaricom's USSD prices. Kenya introduced the National Payments Act in 2014, which helped to helped to clarify questions of regulatory jurisdiction across authorities as well as set common standards for different types of firms offering DFS (e.g., banks and MNOs). Kenya also issued mobile virtual network operator (MVNO) licenses in 2014 to allow new entrants to challenge MNOs by establishing their own telecommunications networks on which they can offer DFS. A 2014 ruling by the Competition Authority of Kenya (CAK) put an end to agent exclusivity clauses in Kenya, allowing individual agents to serve more than one MFS provider. In addition, CAK issued rules in 2015 requiring greater transparency of pricing for Lipa na M-Pesa, a mobile money-based merchant payment platform. In 2016, CAK mandated disclosures of pricing for USSD based transactions. **Zambia**'s competition authority fined MTN because they were restricting access to Zoona. The Competition and Tariff Commission in **Zimbabwe** investigated Econet for charging different access prices for customers depending on whether they were using Econet's mobile money service or that of a competitor. **Uganda**'s Communications Commission is weighing different options for regulatory interventions into USSD access and pricing. In **Tanzania**, interoperability agreements among MNOs in 2014 and 2015 facilitated across network mobile money transfers.

References as of October 2017
-ITU-T FG DFS (2017), "Competition Aspects of Digital Financial Services"
-ITU (2016), "GDDFI Discussion Paper: Digital Financial Services: Regulating for Financial Inclusion, An ICT Perspective"
-GSMA (2015), "Competition Policy in the Digital Age: A practical handbook"
-CGAP (2015), "USSD Access: A Gateway and Barrier to Effective Competition"
-CGAP (2015), "Promoting Competition in Mobile Payments: The Role of USSD"
-CGAP (2016), "Competition in Mobile Financial Services: Lessons from Kenya and Tanzania"
-CGAP (2016), "Competition and Mobile Financial Services: Move Past 'Test & Learn"
-CCRED (2017), "Competition Authority of Kenya (CAK) Rules on USSD Pricing"

XVI. Crowdfunding

Description: "Crowdfunding" typically describes a method of financing whereby small amounts of funds are raised from large numbers of individuals or legal entities to fund businesses, specific projects, individual consumption, or other needs. It involves bypassing traditional financial intermediaries and using online web-based platforms to connect users of funds with retail funders. Crowdfunding typically means (i) raising funds in small amounts, (ii) from many to many, (iii) using digital technology.

Impact on supervisory capacity: Crowdfunding is a new type of financial service, involving a new type of FSP - a crowdfunding platform. Therefore, regulators and supervisors need to consider an appropriate regulatory framework for regulation and supervision of crowdfunding. This also raises a question of what regulatory authority should be responsible for regulation and supervision of (often distinct models of) crowdfunding. By design, a crowdfunding platform often matches consumers (funders) with a consumer (a fundraiser). This creates a peculiar regulatory
challenge that requires a framework to be in place to protect funders and fundraisers. However, thus far, policy makers are predominantly focused on the risks faced by the supply side (investors, lenders, and other suppliers of funds), while neglecting the fact that the platform is often the only "professional" in the crowdfunding transaction, where both the investor and the fundraiser are equally vulnerable and inexperienced individuals or small businesses. Another important regulatory issue is the use of alternative data by crowdfunding platforms to score creditworthiness of their borrowers. New and proprietary credit scoring models need to be tested to prove their predictability through out the credit cycle.

Direct impact on low-income consumers: The idea of matching people who need money with the people who have money to invest is not new. What is new is the role of technology to make this concept easier and practical. Crowdfunding has the potential to transform retail financial services as the use of technology, increasing connectivity through mobile phones and other devices, the legal and regulatory framework, and constantly changing economic conditions allow new and innovative firms to compete. This competition could foster economic growth and entrepreneurship, especially in countries with less developed financial systems. Africa is the second most dynamic continent for crowdfunding in terms of annual growth (after Asia) with 177% growth y-o-y in 2016. However, in terms of crowdfunded volumes it lags behind other markets. For instance, according to AlliedCrowds data, crowdfunding activity in East Africa reached only $37.2m raised in 2015, out of a total of $430m raised in the developing world (excluding China). Examples of how crowdfunding may potentially benefit financially excluded and underserved people include improving access to finance to unserved and underserved borrowers; creating cheaper, community-based insurance products; and facilitating access to digital investments by people who currently have limited or no options to get financial returns on their savings.

Examples: **Kenya** (M-Changa, PesaZetu), **Nigeria** (Imeela), **South Africa** (RainFin), **Uganda** (Akabbo), **Ghana** (Farmable.me), **Cote d'Ivoire** (Orange Collecte)

References as of October 2017
-CGAP (2017), "Crowdfunding and Financial Inclusion"
-CGAP (2016), "Will Crowdfunding Help Financial Inclusion of Unserved Crowds?"
-CGAP (2016), "Six Tips for Policy on Disruptive Digital Financial Inclusion"
-CGAP (2014), "Boon for the Base: Crowdfunding for the Base of the Pyramid"
-World Bank/Infodev (2013), "Crowdfunding's Potential for the Developing World"
-World Bank (2015), "Crowdfunding in Emerging Markets: Lessons from East African Startups"

-GPFI White Paper (2016), "Global Standard-Setting Bodies and Financial Inclusion: The Evolving Landscape"
-GPFI (2016), "Issues Paper: Crowdfunding at the base of the pyramid and related developments: ramifications for regulation, supervision, and oversight"
-FSD Africa (2017), "Crowdfunding in East Africa: Regulation and Policy for Market Development"
-Allied Crowds (2016), "East AFrica Crowdfunding Landscape Study"
-Deloitte (2013), "Let's Get Together: Crowdfunding Portals Bring in the Bucks"
-FSB (2017): "FinTech credit: Market structure, business models and financial stability implications"
-IOSCO (2015), "Crowdfunding: 2015 Survey Responses Report"
-IOSCO (2014) Staff Working Paper, "Crowd-funding: An Infant Industry Growing Fast"

XVII. Crypto currency

Description: Cryptocurrencies or virtual currencies (VCs) are digital representations of value, issued by private developers, and denominated in their own unit of account. VCs can be obtained, stored, accessed, and transacted electronically, and can be used for a variety of purposes, as long as the transacting parties agree to use them. The concept of VCs covers a wider array of "currencies," ranging from simple IOUs of issuers (such as Internet or mobile coupons and airline miles), VCs backed by assets such as gold, and "cryptocurrencies" such as Bitcoin. Decentralized VC schemes use techniques from cryptography for their operations—hence the "cryptocurrency" moniker. In decentralized systems, there is no central party (for example, a central bank) administering the system or issuing VCs. Rather, the central party is replaced by a framework of internal protocols that govern the operation of the system and allow the verification of transactions to be performed by the system participants themselves. As payments and transactions are made through the system, these participants (often referred to as "miners") are rewarded in newly minted "currency" for performing the payment processing function. This approach serves two purposes: it introduces newly minted VCs into the system and enables the decentralized operation of the VC scheme. In contrast to fiat currency, a cryptocurrency does not represent a liability on anyone. Most cryptocurrencies are "pseudo-anonymous"—while cryptocurrency transactions are publicly recorded, users are known only by their VC "addresses," which may not be traced back to users' real-world identity. The value of cryptocurrencies does not have any backing from any source. They derive value solely from the expectation that others would also value and use them.

Impact on supervisory capacity: The actual risks and benefits will largely depend on the innovation concerned. However, anonymous cryptocurrencies may compromise the capacity of regulators and supervisors to enforce AML/CFT requirements. Specifically, regulators/supervisors face increased AML/CFT risks, such as anonymity provided by the trade of cryptocurrency on the internet; limited ID and verification of participants; and lack of clarity re: responsibility of AML/CFT compliance and supervision for such transactions that cross country borders. In addition, many virtual currencies are opaque and operate outside of the conventional financial system, making it difficult to monitor their operations. There is also a need to increase cooperation across different government agencies since virtual currencies cut across regulatory responsibilities. Similarly, to other innovations, regulators/supervisors face the challenge of allowing the innovation to responsibly flourish.

Direct impact on low-income consumers: If cryptocurrency is to play a role in helping the underserved get improved access to financial services, it will almost certainly do so by helping people transfer and transact more quickly, safely, and cheaply. While over the long term this may enable new forms of credit, micropayments, and online commerce, in the near term the most concrete opportunity is to decrease the costs of international remittances, particularly as it becomes easier and cheaper to cash-in, cash-out, and

exchange currencies cross-border (as companies like Ripple are trying to do with a distributed exchange or "trust network" solutions).

Examples: BitPesa in **Kenya** uses Bitcoin to provide inexpensive remittance services to Kenya; another startup is using crypto currency technology to cut the operating costs of group saving schemes that are popular in Kenya. Savings and Credits Cooperatives (SACCOs) help members combine their savings into investments, sharing the profits of those investments among the group. ChamaPesa co-founder Ken Griffith said that by using a cryptographic finance technology, they plan to allow SACCOs access investments that today only multinational banks could offer. A **Ghana**-based IT company has recently created a bitcoin-producing farm, adding capacity to the global pool, thus promoting Bitcoin development in Africa. In countries like **South Africa, Ghana, Kenya, Botswana, Zimbabwe and Nigeria**, there is a semblance of digital currencies, primarily bitcoin, taking roots. These countries have exchanges and start-ups in the crypto space, and their businesses are recognizing the significance of cryptocurrencies in fostering cross-border trade and payment. In **South Africa**, there are more than 1000 merchants accepting Bitcoin.

References as of October 2017

-IMF Staff Discussion Note (2016), "Virtual Currencies and Beyond: Initial Considerations"
-CGAP (2014), "Bitcoin and Financial Inclusion: Not Much of a Link for Now"
-CGAP (2014), "Bitcoin vs Electronic Money"
-CGAP (2014), "Digital Currencies and Financial Inclusion: Revisited"
-CGAP (2014), "Digital Currencies and Financial Inclusion: 5 questions"
-CFI (2014), "Bitcoin and the Bottom of the Pyramid: How Cryptocurrency Can Make Good On Its Promise of Financial Inclusion,"
-World Bank (2014), "Why You Should Care About Bitcoin - Even if You Don't Believe In It,"
-World Bank (2016), "2016 World Development Report: Digital Dividends"
-FATF (2014), "Virtual Currencies: Key Definitions and Potential AML/CFT Risks"
-World Economic Forum (2015), "5 ways digital currencies will change the world"
-CPMI (2015), "Digital currencies"
-GPFI (2015), "Innovative Digital Payment Mechanisms Supporting Financial Inclusion: Stocktaking Report"
-CNBC (2017), "'We are about to see massive disruptions': IMF's Lagarde says it's time to get serious about digital currency"
-Price Waterhouse Coopers (2015), "Money is no object: Understanding the evolving cyrptocurrency market"
-Financial Times (2017), "Six global banks join forces to create digital currency"
-IT News Africa (2016), "Could cryptocurrencies be the next big thing in Africa?"
-Cryptocoins News (2017), "Africa is ripe for bitcoin and cryptocurrencies"
-Fast Company (2015), "Bitcoin's Big Opportunity in Africa"

XVIII. Cyber-laundering

Description: Cyber-laundering is a form of cybercrime described above and refers to money laundering over the internet, e.g. through fake online auctions, online sales, virtual credit cards, online gambling websites, online games, virtual worlds, converting money to Bitcoins or other digital currencies anonymously, money mule scams, and work from home scams to launder money.

Impact on supervisory capacity: Supervisors face new risks due to operational and security issues arising from the technology used, or new unregulated players. There may also be an increased need for supervisors to collaborate across borders due to the trans-national nature of online money laundering.

Direct impact on low-income consumers: Consumers, particularly with low level of digital literacy, could fall prey to money mule scams, in which a person receives and transfers funds acquired illegally for others. Most mules receive a commission for their efforts. Another scam is to offer people jobs in which they can make a substantial income working from home. However, the 'job' involves accepting money transfers into their accounts and then passing these funds on to an account set up by the employer.

Examples: In **Kenya**, M-Pesa has been used to launder fake currencies, to bribe corrupt officials, and to facilitate kidnapping and extortion and a range of other crimes. (Quartz 2013) The US State Department points out that tracking and investigating suspicious transactions within mobile payment or banking systems remain difficult despite the checks already in place. "For example, criminals could potentially use illicit funds to purchase mobile credits at amounts below reporting thresholds." Other regional remittance channels like hawala (a type of informal money transfer system popular in Kenya and Somalia) for international funds transfers make it harder to track transactions. Unlike M-Pesa which is closely regulated and has daily transfer limits of $1,400, the hawala system allows transfer of large sums of money, is multi-currency and can be used without identification document requirements. (Quartz 2017; US State Department report 2017)

References as of October 2017

-UN Office on Drugs and Crime (2013), "Laundering Money Online: a review of cybercriminals' methods"
-MIT Technology Review (2013), "The Secrets of Online Money Laundering"
-Fraud Magazine (2016), "The virtual future of money laundering"
-FATF (2008), "Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems"
-FATF (2010), "FATF Report: Money Laundering Using New Payment Methods"
-FATF (2013), "Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments, and Internet-Based Payment Services"
-Presentation at International Banking AML Seminar (2012), "Money Laundering in the Cyber Era"
-Springer (2014), "Legal Principles for Combatting Cyberlaundering"
-ITU (2012), "Understanding cybercrime: Phenomena, challenges and legal response"
-Quartz article (2013), "How mobile payments might be the global money laundering machine criminals have dreamed about"
-Quartz article (2017), "US State Dept thinks Africa's leading mobile money platform is vulnerable to money laundering"
-US Department of State, "International Narcotics Control Strategy Report, Vol. 2, Money Laundering and Financial Crimes"
-Security Intelligence (2016), "It All Comes Out in the Wash: The Most Popular Money Laundering Methods in Cybercrime"

XIX. Cyber-security

Description: Cyber-security refers to an activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation. Cyber-security is pursued through measures that protect and defend information and information systems by assuring their availability, integrity, authentication, confidentiality and non-repudiation. Attackers use social engineering to get customer details such as ID number, last called number and Pin which they then use to perform a SIM swap and mobile money account reset.

Impact on supervisory capacity: Maintaining and ensuring that information is secured and protected is paramount for financial sector stability and integrity, as well as consumer protection and inclusion. Supervisors need to better understand how they can protect their own information systems within the agency as well as mechanisms to protect information kept by financial service providers. New technologies and business models are working based on collection and sharing of consumer data and information, which can create huge harm to consumers and the sector. Providers are becoming increasingly aware of the threats from cybercrime and developing risk management frameworks and processes. Regulators and supervisors seek guidance for setting standards regarding provider processes, staff capabilities and functions as well as provider reporting standards and how to identify weaknesses early.

Direct impact on low-income consumers: Digital financial services are delivered through digital channels and therewith reliant on information technology and systems that are at risk of being accessed by fraudsters and misused or exploited. A cyber-attack could directly affect consumers if their data is stolen and being misused, they might lose some or all of their assets or valuable personal information. Cyber threats and cyber-attack incidents have significant reputational impacts on the financial service provider, and the industry as a whole, and can therewith encourage exclusion due to lack of trust and confidence in DFS. University of Florida research finds: Mobile-money services are growing at a rapid clip in the developing world, but new research suggests many of the apps that give the poor access to banking services have woeful security protections, leaving users exposed to fraud and theft. Computer scientists at the University of Florida studied seven mobile-money apps from Brazil, India, Indonesia, Thailand and the Philippines, and found what they considered major security flaws in six.

Examples in the market: **MyAirtel** used encryption but tried to protect the data using an unusually weak "key," a series of numbers and letters that encode the information. Most keys are random, but for MyAirtel, the key was always the same series of eight numbers and letters followed by the person's phone number and account number, making it extremely easy for an attacker to figure out. **In Kenya:** (i) There has been an increased number of conmen who hack the system and cheat unsuspecting customers to send them money through some mobile phones accounts; (ii) Fraud in Telco and 2 Banks resulting from visibility in authentication details that allowed administrative employees to change user passwords, circumventing Segregation of Duty maker checker controls and transfer funds to fraudulent MSISDNs; (iii) In 2 MFIs (Saccos), fraudsters targeted dormant customer accounts. In one case this was perpetrated by the MFI employees who accessed the customer account and changed the MSISDN linked to the account then pilfered the funds from that account. In the second case, the fraudster came to the MFI's banking call, filled in a change of account form where they provided the new MSISDN. This form did not go through proper checks e.g. calling the account owner, verifying the signing mandate and the change was carried out. Again, this would have an element of insider collusion since the fraudster has been told which accounts are dormant etc.; (iv) Kenyan fraudsters have created a malware which is being used as a keylogger. The fraudsters obtain the code from the underground (deep dark web) and perform some modifications on it, creating the malware. According to

my sources, this keylogger has been used in all banks and MFIs (Saccos) in Kenya. The biggest impact has been in MFIs which do not have skilled manpower to detect this; quantification of the attempted money lost would be in billions of KES and actualized money lost would be in hundreds of millions KES. Antiviruses such as Symantec and Kaspersky do not have these signatures therefore detection has proven to be difficult.

Examples of regulatory responses: In 2014, the **African Union** adopted a Convention on Cyber Security and Personal Data Protection, which was signed by 8 out of the 54 countries (Benin, Chad, Congo, Guinea Bissau, Mauritania, Sao Tome and Principe, Sierra Leone, and Zambia). The **African Cyber Risk Institute** (ACRI), said in an interview "there is no law that force local companies that have suffered hacking and data breach to tell their clients. There is no conceited effort to report, there should be a law that force companies that have been hacked to tell the regulator." The Bank of **Ghana** is collaborating with CGAP and GIZ to identify demand and supply side concerns and practices regarding cyber threats, in order to inform regulatory measures for improved cybersecurity and cyber threat reporting in Ghana's DFS sector. The Communications Authority of **Kenya** has a Cybersecurity Unit. **Rwanda** is working on implementing a "Regional cyber-crime center of excellence", which will host a digital forensic laboratory (mobile and disk forensics, and malware analysis), cyber fusion center and cybercrime investigations.

References as of October 2017

-IIF (2017), "Deploying RegTech against financial crime"
-Serianu (2016), "Kenya: Cybersecurity Report 2016"
-Serianu (2016), "Africa Cyber Security Report"
-ITU (2012), "Understanding cybercrime: Phenomena, challenges and legal response"
-African Union Convention on Cyber Security and Personal Data Protection
-IEEE Spectrum (2016): "Nigerian Scammers Infect Themselves With Own Malware, Revealing New "Wire-Wire" Fraud Scheme"
-Wall Street Journal Blog (2015), "Researchers Find Security Flaws in Developing-World Money Apps"
-CSO (2016), "How sandboxing can help in the fight against cybercrime"

XX. De-risking

Description: De-risking is a phenomenon whereby large global banks terminating or severely restricting relationships with categories of clients has been a significant, unintended consequence of changing risk management and regulatory frameworks. De-risking can manifest itself in a number of ways, with the most frequent responses including: > banks limiting their exposure to certain high risk customer sectors, e.g. money transfer operators/remittance providers; > taking steps to avoid an overconcentration to a particular type of risk, e.g. correspondent banking; > limiting the types of services offered to higher risk relationships, e.g. cash clearing activity, bank notes, etc.; > curtailing certain products and services in, and for, certain countries and customer sectors. The banks' drive to limit their own risk exposure is also causing some banks to shed correspondent banking relationships in countries perceived as risky. Poor countries, particularly those in conflict, are more likely to be perceived as risky. This raises the spectra that entire economies and regions – including some of the most vulnerable – could find themselves excluded from the global financial system. This danger has raised sufficient concern to cause the Financial Stability Board join forces with the World Bank, the Financial Action Task Force, the Committee on Payments and Market Infrastructures, and other bodies to investigate the implications of financial exclusion for global systemic stability, as well as possible steps to address it. A decline in the number of correspondent banking relationships is a source of concern for the international community because it may affect the ability to send and receive international payments, or drive

some payment flows underground, with potential consequences on growth, financial inclusion, as well as the stability and integrity of the financial system

Impact on supervisory capacity: When consumers are excluded from the formal financial system and consequently use informal financial services, it increases financial integrity risks for supervisors. In addition, due to the cross-border nature of de-risking, it increases the burden on regulators and supervisors to communicate and share information with other countries.

Direct impact on low-income consumers: For customers, de-risking can mean having their accounts closed or being unable to use certain products or services (e.g., send or receive remittances). De-risking may not only undermine financial inclusion but also potentially hold broader implications for the global financial system, as the termination of correspondent banking relationships may lead to restricted access to the global banking system with potentially significant implications for poverty reduction and economic development efforts.

Examples: The CPMI report on correspondent banking published in July 2016 shows that the most pronounced absolute decline in active correspondents has occurred in European regions. For African regions, the CPMI notes that the picture is mixed, with pronounced declines in Northern Africa and partly in Southern Africa, but substantial increases in other regions. According to the World Bank's Fact Finding Summary from De-Risking Surveys conducted in 2015, roughly half the banking authorities indicated a decline in correspondent banking relationships, with the Caribbean region being the most severely affected.

References as of October 2017
-CGAP (2016), "Deepening Insights on Financial Exclusion Risks"
-FSB (2016), "FSB action plan to assess and address the decline in correspondent banking"
-FATF Guidance (2016), "Correspondent Banking Services"
-CPMI (2016), "Correspondent Banking"
-FSD Africa (2017), "Anti-Money Laundering, Know Your Customer, and Curbing the Financing of Terrorism"
-GPFI White Paper (2016), "Global Standard-Setting Bodies and Financial Inclusion: The Evolving Landscape"
-World Bank (2016), "De-risking in the Financial Sector"
-World Bank (2015), "Fact finding summary from de-risking surveys"
-World Bank (2015), "Withdraw from correspondent banking: where, why, and what to do about it"
-World Bank (2015), "Report on the G20 survey in de-risking activities in the remittance market"
-World Bank (2016), "World Bank Makes Progress to Support Remittance Flows to Somalia"
-World Bank (2016), "The World Bank's Data Gathering Efforts: De-risking? Key Findings and Recommendations" presentation
-IMF Staff Discussion Note (2016), "The Withdrawal of Correspondent Banking Relationships: A Case for Policy Action"
-AFI (2016), "Stemming the Tide of De-Risking Through Innovative Technologies and Partnerships"

XXI. InsurTech

Description: "InsurTech" is a sub-category of fintech and refers to technology-driven innovations in the insurance industry, including smartphone apps, claim acceleration tools, personalized insurance solutions, online policy handling, crowdfunded/P2P insurance etc. “InsurTechs” can also refer to technology-led companies that enter the insurance sector, taking advantage of new technologies to provide coverage to a more digitally savvy customer base. Over the past few years, InsurTechs have emerged in the insurance space.

Investments have grown by leaps and bounds—whereas USD 140 million was invested annually in 2011, investment climbed to USD 270 million in 2013, and USD 2.7 billion in 2015. (McKinsey).

Impact on supervisory capacity: Implications of InsurTech for insurance regulators and supervisors include: (i) Speed of technological innovation challenges existing regulatory & supervisory frameworks; (ii) Need to accommodate and manage new players and power relationships; (iii) Some models challenge definition of "insurance" and "intermediary services"; (iv) Various consumer protection risks arise, including Aggregator, Sales, Policy Awareness, Payment, and Post-sale risks, as well as consumer data protection and privacy risks.

Direct impact on low-income consumers: InsurTech involves more inclusive business models, such as: policy origination without face-to-face interaction, reduced distribution & premium collection costs whilst increased convenience for customer, claims lodging and settlement streamlined through mobile phones, sensors, big data analytics, smart contracts, etc, and allows for more tailored offerings such as on-demand insurance initiatives that cover consumers for specific periods where they need that coverage.

Examples: In some locations, regulatory barriers have been lowered. In Australia, Singapore, and the UK, for example, InsurTechs have been encouraged to test their innovative business plans on specific client segments without the need to conform to the full regulatory frameworks that apply to conventional business. Like FinTechs, InsurTechs are extending innovation throughout the sector, creating a competitive threat to incumbents but also potentially valuable opportunities for partnering on the changing terrain. BIMA, a leading InsurTech player that offers mobile microinsurance, has operations in 16 countries including **Ghana**, **Senegal** (in partnership with Tigo Senegal), **Tanzania**, and **Uganda**. MicroEnsure also offers mobile microinsurance in 9 countries, including **Ghana, Kenya, Malawi, Niger, Nigeria,** and **Zambia.** PlaNet Guarantee Senegal offers crop insurance in **Benin, Burkina Faso, Mali, and Senegal** using satellite index. ACRE/Syngenta Foundation for Sustainable Agriculture offers index-based insurance products in **Rwanda** and **Tanzania**. After the US, the UK and then Germany are the homes of most InsurTech companies. The Asia-Pacific region, which now accounts for only 14 percent of the InsurTechs, is expected to be the fastest growing region in the coming years. (McKinsey).

References as of October 2017

-PWC report, "InsurTech: A golden opportunity for insurers to innovate"
-McKinsey: "InsurTech: The Threat That Inspires"
-Cenfri (2017): "The role of InsurTech in microinsurance: How is InsurTech addressing 5 challenges in microinsurance?"
-A2ii (2017), "Regulating Mobile Insurance: Status and Regulatory Challenges"
-Swiss Re Institute (2017), "Insurance: adding value to development in emerging markets"
-Financial Technology Partners (2016), "Prepare for the InsurTech Wave: Overview of Key Insurance Technology Trends"
-Forbes (2016), "How InsurTech is rapidly changing insurance and health tech industries"
-FSD Africa (2017), "Getting ahead of the curve: how the regulatory discourse on m-insurance is changing"
-KPMG (2017), "The Pulse of Fintech Q4 2016: Global analysis of investment in fintech"
-Insurance Thought Leadership (2017), "Top 10 InsurTech Trends for 2017"
-Vertafore (2016), "What is InsurTech and How Can You Harness Its Disruptive Powers"
-CGAP (2013), "M-Insurance: Ensuring Take-off While Doing No Harm"
-CGAP (2014), "The Emerging Global Landscape of Mobile Microinsurance"
-CGAP (2013), "Mobile Life Insurance: Innovations from Pakistan"

-IAIS (2017) presentation on "Towards an Application Paper on the Use of Digital Technology in Inclusive Insurance"
-Microfinance Gateway, "Five InsureTech Trends and What They Mean for Microinsurance"
-CGAP (2014), "Three Lessons from Mobile Microinsurance in Bangladesh"

XXII. Internet of Things

Description: The ITU has defined the Internet of Things (IoT) as "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies" (Recommendation ITU-TY.2060). The IoT clearly includes machine-to-machine communication (referring specifically to communication directly between devices, used in a vast array of applications and for a variety of purposes), but broader definitions of IoT technologies also include ambient intelligence and smart environments. (ITU 2015) As per the World Bank's Digital Dividends (2016) report, the IoT refers to the interconnection of objects to internet infrastructure through embedded computing devices, such as radio frequency identification (RFID) chips and sensors. IoT products can be classified into five broad categories: wearable devices, smart homes, smart cities, environmental sensors, and business applications. Some experts believe that the IoT will mark a new stage of the internet's development, since it has the potential to revolutionize the way people live, work, interact, and learn. However, there are still significant barriers to full commercialization of IoT, such as the fragmented landscape of standardization, which is preventing interoperability; and the relatively high cost of embedded devices. There are also significant privacy and security concerns. As more devices are connected to networks, hacking unsecure devices could have repercussions that far exceed the damage posed by conventional security threats. Over the coming years, IoT will undoubtedly have an enormous impact on how we interact with the devices that populate the world around us, from the mundane to the arcane. Billed as one of the disruptive technologies of the next decade, connected devices are expected to grow from 9 billion today to between 50 billion and 1 trillion within the next decade. By 2020, the IoT sector is projected to create $7 trillion of value, with 45 percent coming from machine-to-machine applications. (Cisco)

Impact on supervisory capacity: For regulators and supervisors, IoT ushers in new actors and new business models, along with their associated risks. IoT also increases consumer protection concerns such as privacy, security, consent, and discrimination. As IoT will lead to tighter and more widespread integration of (or bundling with) financial services into other (non-financial) services, the need to coordinate intra- and internationally will increase.

Direct impact on low-income consumers: Fintechs are combining machine-to-machine (M2M) technology with new payment mechanisms to create commercially viable ways for the underbanked to access basic products and services like solar lamps and charging stations, water pumps, refrigerators and even on-grid utilities like electricity. M2M technology is expanding access to credit by enabling two new payment methods: pay-as-you-go ("PAYG") asset financing, which allows consumers to pay for products over time, and prepaid, where consumers pay for services on an as-needed basis. For underbanked consumers, prepaid utilities/smart meters offer financial inclusion by providing a method of payment that circumvents the need to obtain credit from the energy company and/or put down a prohibitively large one-time deposit to establish service.

Examples: In **Kenya**, M-Kopa Solar is leveraging M2M technology and integrating with M-PESA to provide pay-as-you-go asset financing for solar power solutions [M-KOPA is also in **Tanzania** and **Uganda**]. In Kenya, Syngenta's Kilimo Salama ("Safe Farming") project is a connected weather station that monitors agricultural events and facilitates linkages with insurance firms. The aim is to mitigate the risks associated with adverse weather, thereby providing a much-needed safety net for farmers while promoting agricultural investment

and improved livelihoods. Safaricom's M-Pesa mobile banking system assists Kilimo Salama in keeping index insurance premiums more affordable, helping transform smallholder farmers into a commercially viable market segment for insurance firms. Vodacom **Tanzania** announced that it has invested in customized IoT solutions (e.g., vehicle tracking, monitoring of retail points, etc.) and cloud computing service. In 2014, CGAP conducted a global landscaping study of digital finance plus (DF+) companies/solutions innovating in the energy, water, education, health and agriculture sectors. Out of the 55 businesses compiled in the CGAP database, 70 percent are in Africa - over half are located in Kenya and Tanzania. **Nigeria** (as well as the UK) recently launched state-sponsored initiatives to accelerate the rollout of smart meters. Prepaid smart meters with integration into payment networks are attracting much-needed investment into emerging market energy infrastructure while also providing new, previously unserved consumers with access to the electricity market. Smart meters accomplish both these tasks by offering innovative prepaid payment solutions enabled by mobile data networks and M2M technology. **South Korea's** Ministry of Science, ICT, and Future Planning was given a mandate to drive IoT adoption as a priority (see report by the European Commission).

References as of October 2017

-World Bank (2015), "Media Revolutions: The future of the Internet of Things and wearables"
-World Bank (2016), "2016 World Development Report: Digital Dividends"
-ITU (2005), "The Internet of Things"
-ITU (2015), "Harnessing the Internet of Things for Global Development"
-McKinsey Global Institute (2015), "The Internet of Things: Mapping the Value Beyond the Hype"
-McKinsey Global Institute (2013), "Disruptive technologies: Advances that will transform life, business, and the global economy"
-Deloitte University Press (2016), "Internet of things: from sensing to doing"
-Deloitte University Press (2015), "The derivative effect: How financial services can make IoT technology pay off"
-European Commission (2014), "Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination"
-Telegeography (2016), "Vodacom Tanzania develops IoT, cloud computing"
-CGAP (2013), "Global Landscape of Digital Finance Plus"
-CGAP (2014), "Digital Finance: Catalyzing New Energy Business Models"
-Texas Law Review (2014), "Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security, and Consent"
-Next Billion, "Next Thought Monday - Financial Inclusion and the Internet of Things: How Smart Machines Can Benefit the Poor"

XXIII. Interoperability

Description: In its Dec. 2016 working paper, CGAP describes interoperability as, "The ability for mass market users of digital financial services (DFS) accounts to perform specific use case payment transactions between accounts at different providers." Interoperability is attracting a high level of attention among experts in digital finance. For providers, there is growing demand for interoperability as a way to increase transaction volumes and create new business opportunities. For development agencies and governments, interoperability is considered important for financial inclusion because it has the potential to introduce economies of scale and scope, create network effects, and allow customers to more easily carry out desired transactions.

Impact on supervisory capacity: While the regulatory approach should "follow the market," the GPFI white paper suggests that during the early stages of development of digital transactional platforms, regulators

should focus their attention on ensuring that interoperability is technologically feasible. The paper also recommends that regulators have authority to take action where there is evidence that a provider is exploiting its dominant position. This might mean, as some regulators have done, mandating interoperability or specifying a timeframe for interoperability. As regulators consider the impact of interoperability on digital financial inclusion and a country's payment system more generally, and determine what role to play, they will need a thorough understanding of the potential new risks posed by the interoperability of banks and non-banks (including legal, operational, and financial risks) and how to address such risks while maintaining a level playing field for all players.

Direct impact on low-income consumers: Interoperable payment systems have the potential to make it easier for people to send payments to anyone and receive payments from anyone quickly and cheaply. Interoperability has the potential to lower fees and the cost per transaction by avoiding duplication of payment acceptance and point-of-sale (POS) device infrastructure. It can also increase the value and usage of new payment infrastructures by allowing users to do business with more people and services.

Examples: CGAP 20-country scan includes the following: Bangladesh, Brazil, Cote d'Ivoire, Ecuador, Egypt, **Ghana**, India, Indonesia, Jordan, **Kenya**, **Madagascar**, Mexico, **Nigeria**, Pakistan, Peru, Philippines, **Rwanda**, Sri Lanka, **Tanzania**, Thailand. The scan found that some form of interoperability is present in each market, but progress remains slow in increasing the number of use cases and volume of transactions per use case. Conditions on the ground are complex, with all 20 countries in the scan showing multiple approaches in play at the same time. In **Tanzania**, the four licensed mobile money providers established their own interoperability scheme, defining operating rules and governance collectively, but leaving detailed business agreements and technical integration to be handled bilaterally between providers. It is also limited to the P2P payment use case. The same providers rely on third parties (e.g., aggregator Selcom) for other use cases and engage in wholly bilateral arrangements with other providers for transfers to bank accounts. The **Rwandan** Government has recently taken a significant step toward nationwide interoperability through the setting up of a national interconnecting switch, supported by Ericsson. When established, financial and payment service providers will be required to connect to this central switch. This innovative use of new information and technical software has been driven by the Ministry of Finance and Economic Planning for Rwanda with strong involvement and guidance from the financial regulator.

References as of October 2017

-CGAP working paper (2016), "Digital Finance Interoperability & Financial Inclusion: a 20-Country Scan"
-GPFI (2017), "Digital Financial Inclusion: Emerging Policy Approaches"
-CFI (2017), "Modelo Peru: Unique Model, Unique Challenges, Bright Future"
-Business Daily (2017), "Kenyans set to enjoy cross-network mobile money transfer from July"
-CGAP (2017), "Interoperability and Financial Inclusion: The Regulator's Role";
-ITU-T Focus Group on DFS (2017), "The Regulator's Perspective on the Right Timing for Inducing Interoperability"
-World Bank (2016) blog, "Solving payments interoperability for universal financial access"
-World Bank and CPMI (2016), "Payment Aspects of Financial Inclusion"
-AFI (2014), "Guideline Note 15: Mobile Financial Services - Accessing Levels of Interoperability"
-AFI (2016), "Interoperability of Digital Financial Services in Tanzania"
-GSMA (2012), "The case for interoperability: Assessing the value that the interconnection of mobile money services would create for customers and operators"
-GSMA (2014), "Interoperability: the role of rules and standards"
-GMSA (2016), "The impact of mobile money interoperability in Tanzania: Early data and market perspectives on account-to-account interoperability"

-Microfinance Gateway (2016), "Ericsson and Rwandan Government to Collaborate on Financial Inclusion"

XXIV. KYC Utilities

Description: A Know-Your-Customer (KYC) utility is a central repository that stores the data and documents required to support a financial institution's procedures relevant to implementation of AML/CFT measures, specifically customer due diligence (CDD). Once a customer's data has been entered into a utility, member financial institutions can access and leverage the information for their own individual CDD. Thus, KYC can support 100% digital customer acquisition and onboarding. According to a survey published in May 2016 by Thomson Reuters, banks and other financial institutions spend up to $500 million a year meeting CDD. Conforming to the regulations is not getting any easier: the European Union's fourth Anti-Money Laundering Directive is due to be implemented by 2017 and new rules on customer due diligence by US Financial Crimes Enforcement Network came into effect in May 2016. Implementing KYC rules is not just costly and time-consuming; banks also complain that service suffers, with delays to onboarding new customers, who also face repeated requests for the same information from each new provider. The experience leads to poor first impressions and leaves customers less likely to buy other products and services. In a 2014 survey by Forrester Consulting, 98% of global banks surveyed said deficiencies in onboarding had resulted in lost deals and revenue. In other cases, large banks have reacted to heightened levels of regulatory attention and increasing costs of compliance with AML and KYC rules by getting rid of certain clients (See also De-risking).

Impact on supervisory capacity: Regulators and supervisors will benefit from the standardization and consistent quality of data KYC utilities bring. However, regulators may still be cautious about services they see as outsourcing compliance activities, as well as concerns around data protection and privacy (See also De-risking). The key challenge with KYC utility is to ensure that the data stored in the utility is correct and up to date. This issue goes to the point of who should be allowed to feed data into the utility, whose responsibility would be accuracy and quality of data, what governance structures should be in place, what kind of oversight should apply, what liability should be associated with use of data, provided by a third party etc.

Direct impact on low-income consumers: KYC utilities save customers who have already given their information to a participating member from having to supply it again. KYC utilities may also make it easier for customers to access new products and services available online.

Examples: **South Africa** (Thomson Reuters launched "Org ID" KYC utility in partnership with Barclays Africa, Rand Merchant Bank and Standard Bank of South Africa in July 2016). The Monetary Authority of **Singapore** has introduced eKYC - a utility that allows for digital customer acquisition.

References as of October 2017

-CGAP (2016), "Six Tips for Policy on Disruptive Digital Financial Inclusion"
- GPFI (2017) "Digital Financial Inclusion: Emerging Policy Approaches"
-CPMI (2016), "Correspondent banking"
-BCBS (2017), "Guidelines: Revised annex on correspondent banking"
-Price Waterhouse Coopers (2015), "Share and share alike: Meeting compliance needs together with a KYC utility"

-Press release (2016): “Thomson Reuters Launches Know Your Customer Solution for Africa”
-Brookings Institution, "Financial inclusion in Latin America: Regulatory trends and market opportunities"
-FinExtra (2017): “MAS to roll out national KYC utility for Singapore”
-Fenergo (2014), "KYC Utilities and the Future of Regulatory Onboarding"
-Financial News London (2016), "Utilities begin to make their mark in KYC"