Technology Inequality

Opportunities and Challenges for Mobile Financial Services

April 2017

AUTHOR

Leon Perlman, PhD

CENTER *for*
FINANCIAL
INCLUSION | accion

Foreword

When mobile money debuted a decade ago, observers marveled that a woman in rural Kenya with limited education or financial means could receive money instantly from her children in Nairobi through a cell phone. Ten years on, tens of millions of people use mobile financial services (MFS), and the sector is preparing for a switch to smartphones that will enable even more and better services.

Not so fast, cautions CFI Fellow Leon Perlman in this report. Like many techno-wonders of our world, the services used in Kenya and many other countries operate through distinct technologies that must interconnect seamlessly to complete transactions securely. These layers include data transmission connectivity, the handsets themselves and their operating systems, and the technologies delivering MFS menus and commands. These systems are continually evolving, subject to market and technology forces that do not necessarily prioritize mobile money.

In this report, Perlman steers readers through a primer on the technology that enables MFS to operate on basic, feature and smart phones. But more importantly, the report sounds a cautionary note about the readiness of the sector for a large-scale shift to smartphone and internet-based MFS, particularly for low-end consumers. While smartphones promise more intuitive and richer user interfaces, this promise will take some time to materialize fully and robustly.

The backbone of mobile financial services to date has been the combination of feature phones with USSD or STK platforms that display MFS menus. These combinations are well-adapted to low-end conditions, especially in rural areas in developing countries, because they operate reliably with inexpensive handsets in areas with poor (e.g., 2G) connectivity. The widespread coverage, low cost and reliability of the 'traditional' MFS systems make them essential for reaching financial inclusion target populations for the foreseeable future, according to Perlman.

On the other hand, the smartphone revolution is not yet mature. Gaps in geographic coverage of high-speed data transmission, $30 smartphone handsets that use substandard components, and numerous compatibility issues with smartphone apps all contribute to system fragility. Even though smartphones are penetrating markets, the handset capabilities, data transmission speeds and fraud protection must improve before the standards needed for MFS are consistently met.

This report urges regulators and technology providers to continue supporting MFS based on feature phones, even as they work to create paths for new-generation services. In fact, feature phone handsets are getting better, cheaper and smarter, and sales are rising. If mobile financial services are to be a force for financial inclusion, we must not prematurely abandon older technologies as we concurrently push to create a smartphone-based future.

Elisabeth Rhyne
Managing Director
Center for Financial Inclusion

Executive Summary

In the brief decade since they were introduced, mobile financial services (MFS) have become a pivotal and successful enabler of financial inclusion, bringing services to millions of people, many of whom had never before used a formal financial service. The potential for MFS to continue growing in reach and sophistication during the next decade is enormous. MFS may become a significant channel not only for transferring funds from person to person (its first major use), but also to store and save funds, make and receive payments, borrow, invest, buy insurance and manage personal or business finances.

The growth and success of MFS depends on technical components that work together to bring the customer a seamless, reliable, convenient and affordable experience, and on the regulations and business relationships that enable the technical harmony. From the handset to the user interface to the mobile network, each technology must fit with the others, even though a wide range of technologies and commercial and public interests are at play.

While these technical components have developed remarkably well and successfully over the past number of years, there are still numerous technical, cost, competition, capacity, security and access challenges that particularly affect people at the "base of the pyramid" (BoP) who tend to be the most excluded from financial services. There will invariably be trade-offs between access, cost, security and reliability of devices and services.

This study investigates existing and evolving technologies in MFS systems: mobile data "bearer" technologies, access platforms and user devices. We unpack the issues surrounding policy, pricing of bearer services, network access coverage, cost of devices, evolution of consumer-facing technology designs, security challenges, type and quality of devices being used, and the usability of various access devices. The report is meant to motivate providers, vendors and regulators to improve upon existing devices, system security and the regulatory environment as it affects the ability of BoP customers to access and use MFS effectively. We seek to generate a discussion on the technical and related challenges faced by the MFS ecosystem and to spark action to solve these key challenges.

While the report reveals many specific challenges and is optimistic overall about the future of MFS, it does have one clear bottom line. In brief, that bottom line is a call for providers and regulators to continue to ensure that the technical "combo" that has dominated MFS to date remains robust for the foreseeable future: feature phones using Unstructured Supplementary Service Data (USSD) or SIM Application Toolkit (STK) technologies and operating even where only slow second generation (2G)-type communication speeds are available. While smartphone-using apps and 3G or 4G networks are developing quickly and may become dominant in the future, bringing enhanced services with them, that future has not yet arrived, especially for customers in the developing world who live in rural areas or who cannot afford high-end smartphones. The smartphone MFS market still faces numerous growing pains that must be overcome before it can take the place of its more pedestrian forebears. Providers and policymakers must not prematurely rush toward a smartphone future if that means neglecting the feature phone present.

This report provides a primer on the technical elements that underpin MFS, and as it does so, it describes their current status, emphasizing the dynamism in both the feature phone and smartphone markets.

> **Part I** describes the access and user interface (UI) technologies that deliver MFS, detailing their pros, cons and (in layman's terms) technical requirements.

> **Part II** reviews the state of mobile network coverage in developing countries, looking at gaps in the move toward higher-speed 3G and 4G coverage.

> **Part III** discusses the evolving capabilities of basic, feature and smartphones, noting in particular the enhancements around feature phones and the shortcomings of lower-end smartphones.

> **Part IV** examines particular components of phones—operating systems, memory, battery and display—and their role in creating an MFS package that works for low-end consumers.

> **Part V** discusses the emerging problems of technology fraud and counterfeit phones.

> A brief but essential **Part VI** discusses competition issues that may hinder access and notes possible solutions.

Major Findings
For MFS to continue to grow, it is important to continue supporting feature phones with USSD and STK interfaces.

Mobile financial services for BoP users are currently provided largely on feature phones operating across 2G-type mobile networks and using menu-driven, text-based user interfaces (UI). The ease of use and accessibility of this combination of technologies has contributed greatly to the success of MFS. The main access and UI technologies in use are Unstructured Supplementary Service Data (USSD), the dominant mechanism; Short Message Service (SMS) in its SIM Application Toolkit (STK) incarnation, next in prevalence; and finally, Java applets.

Feature phones are likely to dominate MFS for BoP for the foreseeable future. While smartphones are penetrating BoP markets, the pace remains relatively slow. With user preferences having shifted away from basic phones, feature phone manufacturing is actually growing. As early mobile technology patents expire, costs will continue to drop and use will grow:

> Most feature phones lack high-speed 3G and 4G access, but many do have cameras, WiFi and Bluetooth capabilities, small non-touch displays, and 2G-type mobile data access speeds allowing use of Wireless Application Protocol (WAP) for browsing websites formatted to be viewed on small mobile screens.

> Feature phones are slowly becoming more sophisticated; few have factory-installed social media-type applications that operate over 3G and 4G networks. Devices are also emerging that use the Android operating system on non-touch small screens.

> System-on-a-Chip (SOC) fabrication allows multiple features to be placed on a single chip, which shrinks the device size while improving speed and reducing the retail cost of handsets to well under US$10.

> While Near Field Communication (NFC)-based contactless payment services are growing, most of them require smartphones. However, retrofitted NFC sticker technology for feature phones is beginning to appear for use at points of sale and transit applications (e.g., train, subway).

> Encrypted, sound-based access to MFS products is growing.

While smartphone-using apps and 3G+ networks may become dominant in the future, bringing enhanced services with them, that future has not yet arrived—especially for customers in the developing world who live in rural areas or who cannot afford high-end smartphones.

Because of the continued widespread use of MFS systems based on feature phones and USSD or STK interfaces and the relatively slow pace of adoption of MFS-ready smartphones, regulators must continue to develop and maintain policies that support these systems.

> Poor mobile signals and antenna design may hinder successful USSD sessions. Timeouts and dropped sessions occur, due to: poor signal quality, response time limits or long data entry strings (e.g., for account numbers). Fear of timeouts and dropped service encourages users to request agents to perform transactions over the counter, and may discourage users altogether.

> Incompatibility between chips from various manufacturers means that ubiquitous installation use of Java-based MFS applications is problematic.

Realizing the promise of smartphones for MFS first requires improving their technical specifications and the presence of high-speed networks (3G or 4G). Smartphones—which allow third party applications to be installed on the device—offer many new features, such as enhanced UI and user experience (UX). These features could support a range of additional MFS products and capabilities. For example, smartphones with built-in biometric identity capture and authentication can allow higher anti-money laundering/know your customer (AML/KYC) tiered authentication and use and boost access to merchant and government services, including social benefit payments.

Though the general pace of growth of smartphones is relatively slow in developing markets, the emergence of new, inexpensive brands using system-on-a-chip (SOC) chipsets may speed that growth.

Cheap smartphones are not yet sophisticated enough to support MFS. Many entry-level smartphones sold in the developing world:

> Do not support 3G or 4G mobile data

> Contain low power capacity batteries

> Have low resolution and fragile touch or non-touch screens

> Have small touch screens making them liable to "fat finger" data input mistakes

> Have low processing power and storage, making it difficult to run all but very simple apps

> Use thin film transistor display technology that suck up power (higher-end phones use thin active matrix organic LED displays that use less power)

Android is the most popular smart phone operating system worldwide. Particular issues however with Android phones include the lack of backwards compatibility in many cases, meaning that newer MFS applications will not work on smartphones using older versions of Android or which have low memory storage. In addition, STK, a mainstay for access to many MFS implementations around the world, does not work on all Android phones.

Smartphone MFS applications usually require faster mobile data network access. To provide a media-rich UX, MFS apps require 3G mobile data speeds or above. "Data-lite" smartphone apps could however be developed for use on slow 2G networks.

Gaps in high-speed 3G mobile data coverage persist, especially in MFS-focused rural and peri-urban areas. Where there is no 3G coverage, there is usually no 4G coverage either. Mobile network operators (MNOs) can satisfy their universal service obligations in providing 2G-type voice and slow mobile data coverage, even though that may not equate to universal

quality of service. While 3G (and 4G) coverage is predominant in urban areas and along major highways, rural areas still receive mainly 2G-type coverage.

Costs, for both providers and customers, are the source of many of the bottlenecks identified here.

MNOs face high costs for acquiring spectrum and building infrastructure in rural areas in order to expand and upgrade service. However, the release by telecommunications regulators of 700 and 800 MHz frequency bands (a process resulting from the global analog TV switch-off) will allow for increased 3G and 4G coverage (and much later, 5G), including in rural areas. The spread is likely to take several years and could be curtailed if the spectrum purchase costs are too high. There are however emerging technologies that may fill high-speed mobile data coverage gaps without as-large capital outlays.

Handset manufacturers reduce capabilities in order to keep prices affordable for the mass market. Patents add at least 5 percent to smartphone costs.

Data costs for use of 3G (and 4G) by data-hungry smartphones may be prohibitive for many users.

Security threats are emerging for MFS channels and devices.

Signaling System 7 (SS7), a 1970s-era technology, is used by both fixed line and mobile networks to communicate with each other, with their base stations and with customer handsets. This technology has however been exploited by bad actors, putting the integrity of MFS transactions and systems at risk. USSD and any financial systems that rely on unencrypted SMS for communication and authentication—both of which operate through SS7—are especially vulnerable.

The standard mobile air interface is vulnerable to interception by relatively cheap do-it-yourself data interception devices performing "man-in-the-middle" interception of any mobile voice, SMS and data traffic.

Some MFS-type smartphone apps are designed with insufficient security, although a growing awareness of the security gaps is helping to address them. However, MFS apps based on feature phones and written in the Java computer programming language mostly use encrypted SMS, and so they could provide a secure and ubiquitous means of transacting.

Given the potential for security breaches, terms and conditions offered to consumers need revision. As currently written, most service agreements assume that networks are secure and leave financial loss due to technology exploits with the customer.
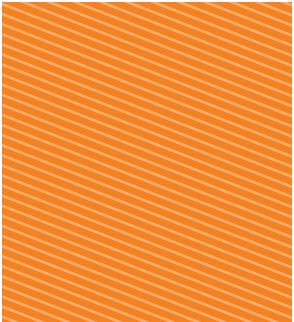
Counterfeit and stolen phone sales are increasing, especially for Nokia, Samsung and BlackBerry devices. Potential harms to purchasers of such phones include:

> Inability to set up and use mobile networks due to the lack of proper serial numbers or International Mobile Equipment Identifiers (IMEIs), which bad actors tamper with. Regulators blacklist phones identified through their IMEI number as stolen or counterfeit, rendering the phone inoperable on the country's mobile networks and so cutting off customer access to MFS accounts. Millions of stolen and counterfeit phones have already been switched off.

> Health dangers through high radiation and the possibility of batteries exploding.

> Risk of exposure to factory-installed malware.

Policy makers must address competition issues for MFS systems. Access to service gateways should be fair, reasonable and non-discriminatory. Technological solutions may be available.

MNOs may be gatekeepers for access to services and infrastructure for competing MFS providers. Those competing service providers may be handicapped ("foreclosed") by being denied access to USSD or STK gateways and short codes or through prohibitive pricing. Also, MNOs and non-bank service providers may be denied access to payment infrastructures required to interoperate or provide services such as merchant acceptance or ATM withdrawals.

Thin SIM technology is being implemented in several countries as a technical fix to evade such blockages.

Introduction

Mobile financial services (MFS) sit at the leading edge of a great transformation bringing universal and affordable access to basic financial services for customers at the base of the pyramid (BoP). These services include person-to-person payments, cash-in/cash-out transactions, mobile airtime purchases and some bill payments. Customers can also store value on mobile wallets, and in some jurisdictions, limited credit is also available. Mobile network operators (MNOs), in partnership with non-bank third party service providers, have been the pathfinders in providing these services, enabled by regulatory innovations allowing non-banks to provide MFS. As of December 2016, there were 277 MFS offerings available in 92 countries.[1] They provide MFS to over 500 million people, many of whom live in rural areas.[2]

MFS depend on specific access and user interface (UI) technologies, all with varying degrees of ease of access, ease of use, efficacy, cost, security, and reliability.[3] Together, these technologies constitute the enabling infrastructure for MFS, and thus it is of utmost importance for the spread of MFS that the technologies be robust and compatible, even as technologies evolve.

Most MFS technologies use the GSM (i.e., Global System for Mobile Communications) mobile infrastructure (see Annex A on Mobile Technologies).[4] Developed initially the 1980s, these digital technologies have since evolved to include second generation (2G) mobile technologies such as Unstructured Supplementary Service Data (USSD), Short Message Service (SMS) and various low data speed capabilities. The late 1990s saw the introduction of higher-speed third generation (3G) technologies, and more recently, a number of markets have introduced fourth generation (4G) technology. Fifth generation (5G) technology is still under development, and will most likely only be available commercially in markets by 2020. The most frequently used user interfaces in MFS include USSD, SMS, SIM Application Toolkit (STK), Java computing language-based applications, and Wireless Application Protocol (WAP), a method for displaying simple web pages on small mobile screens. Some markets feature applications that provide over-the-top (OTT) services—that is, over the Internet access to MFS for smartphone users.
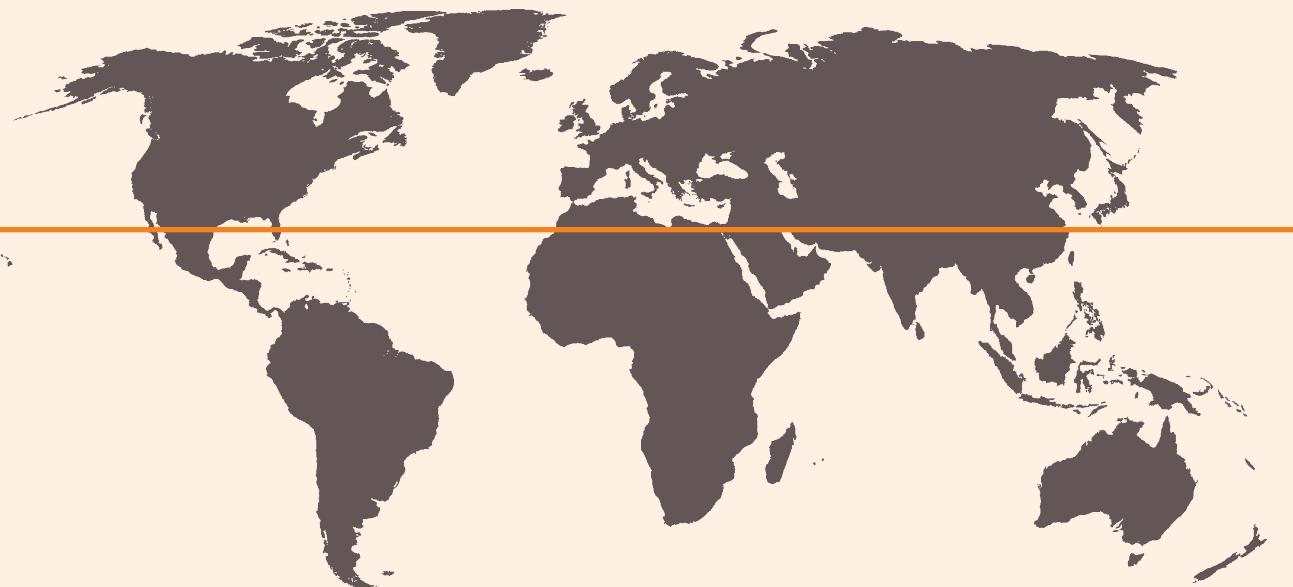
Our goal in this study is to determine whether the core technical components of the MFS ecosystem interact well with one another and to identify friction points and legal and regulatory issues. For example, use of smartphones as the perceived next step in MFS access beyond basic and feature phones may not be the imminent panacea for access and improved user experience (UX). The study found that 3G coverage needed to power the rich media used in smartphones is lacking, and that many smartphone handsets are substandard, and even counterfeit.

This report investigates the following selected components of and issues within

EXHIBIT 1

Typology of MFS in the Northern and Southern Hemispheres

Northern Hemisphere
> More physical bank branches
> Higher bank account use
> Higher smartphone penetration
> 2G–5G network speeds
> Mainly Near Field Communication

Bank Branches

Southern Hemisphere
> Fewer physical bank branches
> Lower bank account use
> Higher feature phone penetration
> 2G network speed; some 3–4G
> Mainly USSD, STK and WAP connections

Bank Branches

The southern hemisphere is characterized by transformational access and services, with non-banks providing financial services to BoP customers. Mobile devices are primarily basic and feature phones types, and national 3G coverage is generally scarce.

Source Leon Perlman, 2010

While smartphones are often perceived as the next imminent step in MFS access, this study found that the 3G coverage needed to power their rich media is lacking, and that many are substandard, even counterfeit.

the MFS ecosystem from the perspective of customers, MNOs, MFS providers, MFS platform vendors and regulators, all with special attention to financial inclusion:

> Use and impact of Signaling System 7 (SS7) technology as the core data transport methodology in mobile networks and MFS

> Use and effect of remote access mechanisms for MFS, such as IVR (Interactive Voice Response), USSD, SMS, GRPS/EDGE, 3G, 4G, and sound

> Use and effect of user interfaces (UIs) for MFS, such as USSD, STK, SMS, Java applications used on some feature phones, OTT MFS smartphone applications, Wireless Application Protocol (WAP), and encrypted sound

> Survey of basic phones, feature phones, smartphones and new hybrid smart feature phones

> Relative penetration of basic phones, feature phones and smartphones and the effect on the user experience and regulatory policy

> Technical components of handsets, such as processors, battery technology, displays and memory

> Phone operating systems

> Mapping handset features with the ability to support MFS

> Degree of low-speed 2G-type and high-speed 3G or 4G mobile coverage across MFS areas, and the effect of the provision of smartphone-based MFS services

> Magnitude and impact of stolen and counterfeit mobile phones and components on customers

> Magnitude and impact of security vulnerabilities in MNO and MFS systems and the legal implications

> Competition issues relating to entry to access networks and payment networks

This report starts with a primer on the ecosystem of technologies necessary to access MFS, then discusses access to these technologies particularly in remote areas. It goes on to compare basic, feature and smartphone access, use and connectivity, and the implications for MFS. It concludes with discussions on two important trends to consider: security of MFS and the competitive environment.

Study Methodology

To facilitate this study, we conducted *in situ* research in Bangladesh, Colombia, El Salvador, Fiji, Jordan, India, Indonesia, Malawi, Mozambique, Rwanda, South Africa, Tanzania and Uganda.

We purchased, examined and used MFS, putting the handsets and services through a series of tests. We also interviewed and consulted with MNOs, service providers, industry associations, banks, technical service providers, standard setting bodies, regulators and domain experts to gather insights and potential solutions to issues highlighted in this study.

Among the tests we applied were the following:

> To investigate the prevalence and quality of phone types, we visited informal street vendors and stores selling phones. We purchased and/or tested these devices *in situ*, and we checked the features and specifications against those outlined on the retail packaging. We noted and compared the prevalence of regional phone brands, and we also compared local mobile data and MFS charges and applicable taxes.

> Where phones were sold without retail packaging, we checked them for complete IMEI serial numbers using the universal *#06# phone command for displaying the IMEI number to determine whether fake or stolen phones were being sold. We also matched the displayed numbers against the IMEI number of the factory-installed model and serial number stickers (if available) placed inside the phone.

> We opened MFS accounts where necessary to determine ease of the process, the time allowed for input of USSD commands and responses, and for later testing of quality of access to services.

> We tested mobile network operator 2G-type and 3G (and higher 4G; both where available) mobile data availability and speeds using two smartphones and a feature phone in urban, peri-urban, rural areas, and along national roads and their periphery. We checked data speeds using our test smartphones using the free Android application *Speedtest.net*.

> We initiated MFS sessions via USSD in rural areas to verify the ability to initiate and sustain USSD sessions and to send and receive SMSs. SMSs acted as a proxy for SIM Application Toolkit-type (STK) SMS where STK was not offered by the local MFS provider. We used local SIM cards for testing the local MNOs' general and mobile data coverage. Where necessary, we locked phones into either only 2G-type or 3G (or higher 4G speeds, where available) modes to ensure that we could check the availability and quality of the required signals. Where MFS agents were found, we noted *in situ* the strength and type of mobile coverage.

> We procured a thin SIM and stuck it onto a hard SIM to check for ease of installation and use, as well as the effect of multiple removal and insertions between various phones on its physical longevity.

> To check for version compatibility for Java applets on feature phones, we downloaded available MFS applets from the provider's WAP or website. We attempted installation using a Bluetooth sideloading technique, as well as direct installation through WAP download. For MFS Android apps, we tested the ability of new and older Android phones running various versions of Android to install and fully use all the features of these apps.

1 Technologies That Enable Access to Mobile Financial Services

The seamless availability and variety of technologies on mobile networks has been the key to the growth of MFS in developing markets (see Annex A on the types of technologies each generation encompasses). To understand the technologies on which MFS is based, it helps to sort them by generation, from earlier and slower to more recent and faster. Each technology involves specific technologies for data transport—or "bearers"—and these bearers play a key role in shaping MFS.[5]

> 2G technology comprises a set of narrowband or low-speed technologies. The most prevalent of these are those based on GSM. The data transport mechanisms associated with 2G GSM technology include USSD and SMS (SS7-based technologies) and later, GPRS and EDGE (Internet Protocol [IP]-based technologies) as so-called 2G+ technologies.[6] These technologies were developed in the 1980s and 1990s. In this study we refer to them in aggregate as "2G-type" technologies.

> 3G technologies are higher-speed and IP-based, using Wideband Code Division Multiple Access (W-CDMA) technology manifested in variations of Universal Mobile Telecommunications System (UMTS) and its successor, High Speed Packet Access (HSPA).[7] They were developed in the 1990s and evolved from GSM.

> 4G technology represents a new set of mobile technologies that manifests commercially as Long Term Evolution (LTE). Its newest (and emerging) incarnations are LTE-A (LTE-Advanced), LTE-M (LTE-Machine), and the LTE-U (Unlicensed) family that includes LTE-LAA (Licensed Assisted Access) that will allow MNOs to augment their high-speed mobile data access provision and coverage using WiFi-type frequencies.[8]

Added to these technologies for moving data are technologies that create access "gateways" and user interfaces (UI) that allow customers to transact. Among the most important UI technologies and their technology bearers currently used in MFS are:

> Mobile Originated Unstructured Supplementary Service Data (MO-USSD)
> Network Initiated USSD (NI-USSD)
> SMS encrypted via SIM Application Toolkit (STK)[9]
> SMS encrypted via Java-based applets
> SMS—cleartext (unencrypted)
> Internet Protocol (IP)-based over-the-top (OTT) mobile phone applications, usually through smartphones
> IP-based Wireless Application Protocol (WAP)
> Voice channel—Interactive Voice Response (IVR)[10]
> Voice channel—acoustic or Near Sound Data Transfer (NSDT) for encrypted transaction authentication

In some cases, the UI and the remote access bearer technology are the same thing, as is the case with USSD and SMS. Combinations of these remote access bearers may be used for technical reasons or for transaction confirmation, regulatory requirements, user experience, competition, or simply for cost reasons. Service providers generally try to provide remote access methods that recognize and serve most of the access devices and reflect the technical literacy of their customers.[11]

Today, by far the most prevalent gateway systems for MFS are USSD and the SMS-based STK—both of which work on almost all GSM-based handsets.[12] Developed long before MFS using national currencies and e-money emerged, they were initially

conceived for MNO airtime recharges and for providing a ubiquitous mechanism to pay for "infotainment" using the MNO's airtime wallet acting as a non-redeemable "virtual currency." They are essentially "bolt-ons" to the basic telecommunications function, tied to the specific type of bearer in use.[13] This prevalence goes hand in hand with the dominance of basic and feature phones (rather than smartphones) in today's frontier and developing markets. These phone and access technologies together provide access to person-to-person transactions, cash-in/cash-out transactions, balance and transaction inquiries, airtime recharge, and some bill payments (see Exhibit 10 for types of MFS activities and the devices they rely on).

Other MFS remote access mechanisms—IVR, cleartext SMS, IP-based WAP, and NI-USSD—are seen as secondary access mechanisms, and used for additional levels of authentication or similar purpose.[14] Similarly, NSDT is a sound-based technology that is used primarily for merchant payments and transaction authentication.

Near Field Communication (NFC) is a proximity or "contactless" payment technology used in a few MFS implementations, primarily in merchant point-of-sale devices or in fare capture systems in transit applications.[15] MFS-oriented over-the-top (OTT) apps on smartphones are emerging, but are not yet in mainstream use in most MFS markets. For example, of the 300,000 MFS clients of Bank South Pacific, only 3,000 use smartphones to access services.

Unstructured Supplementary Service Data (USSD): The Accidental Hero of MFS

When USSD first arose in the 1980s, it was not intended for customers. Rather, USSD was created as an unobtrusive maintenance and testing feature allowing MNO engineers to send and receive messages over GSM networks without interrupting customer calls. It gained commercial application in the mid-1990s when the first prepaid airtime systems were launched around the world. Customers began to use USSD's distinctive combinations of star (*), pound (#),[16] and numbers to recharge prepaid mobile airtime balances with vouchers and check their airtime and account balances.[17]

As noted above, USSD is both a GSM bearer technology and a MFS user interface. Moreover, customers do not need to download or install anything in order to use it, and it requires no Internet connection. USSD is the unsung hero of MFS, providing nearly universal access to MFS platforms worldwide across the full range of GSM-based mobile phones—so much so that USSD has been termed "the third universal app," used on basic, feature and smartphones.[18] USSD is the most-used technology in MFS deployments around the world, including Econet Zimbabwe, Zain Jordan, Orange Jordan, TNM Malawi, Tigo Tanzania, Airtel Tanzania, Vodacom Tanzania, bKash Bangladesh, Wing Cambodia, and EasyPaisa Pakistan.

A major advantage of USSD is that it can be easily adapted as a provider's suite of product offerings evolves. The menus to support new or revised services can be created at very little cost with relatively simple coding and menu design. USSD menus are dynamic, meaning that as the provider's service range expands, USSD menu tree structures can be created and served in real time.[19]

However, USSD is not without drawbacks. Since its adaptation for MFS use, USSD's technical limitations have increased, leading to growing menu complexities and increased transaction failures. Frequent timeouts on USSD sessions are a main source of user frustration. Timeouts often occur when mobile signals are poor or when users are too slow to input data. Users who may be technophobic or functionally illiterate may not feel comfortable navigating menus or inputting long data strings, such as account numbers. This has led in part to an increase in over-the-counter (OTC) transactions, where customers gravitate to agents—the perceived safe haven of human-assisted transactions.[20] Reliance on OTC reduces users' active use of MFS accounts, both as a store of value and as a transactional base, and it limits the ability of service providers to build user profiles that ultimately provide users with richer services such as credit, as well as having an impact on anti-money laundering efforts. Some regulators, in response, are restricting the seamless use of OTC.
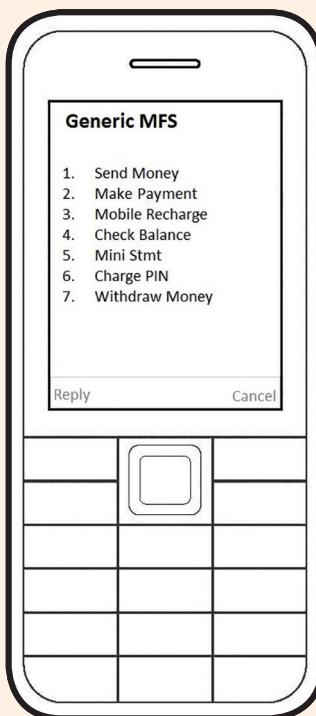
EXHIBIT 2

A Primer on USSD for Mobile Financial Services

As with SMS, USSD uses the mobile signaling channel inherent in SS7 networks. However, instead of a store-and-forward functionality as with SMS, USSD is session-based, meaning that when a user accesses a USSD service, a session is established and the radio connection stays open until the user, service provider system or time-out ends it.

There are two types of USSD: Mobile-Originated USSD (MO USSD) and Network-Initiated USSD (NI-USSD, also known as "push USSD"). In MO USSD, a user—such as a MFS customer or agent—initiates the USSD session to conduct a transaction or inquiry.

A typical USSD session is executed in increments of 20 seconds lasting up to 2 minutes. During that time, the handset cannot make or receive any voice calls, creating a potential revenue loss for the MNO, given that voice calls usually cost more than non-premium-rated USSD sessions. In NI USSD though, the USSD session is initiated by a provider or MNO, usually in circumstances in which some secondary authentication is required while the user is on a call or for use in providing value-added services. A call center agent at a bank for example may initiate a USSD session and ask the user to input their PIN code when prompted by a session menu, obviating the need for the user to reveal their PIN to the call center agent.

In South Africa, small stores are using a combination of NFC and NI-USSD offered by technology provider Boloro. A customer walks to the checkout point and indicates they want to pay via NFC. The cashier presents a NFC reader to the customer who taps the Boloro NFC sticker on the NFC reader. The Boloro platform triggers a NI-USSD session. The customer receives a NI-USSD message requesting them to respond with their PIN on their mobile phone. As soon as the correct PIN is entered, the NI-USSD session closes.[21] In both cases, data is provided to a user interface dynamically, with relatively fast access and response times.

Generic MFS

1. Send Money
2. Make Payment
3. Mobile Recharge
4. Check Balance
5. Mini Stmt
6. Charge PIN
7. Withdraw Money

Reply   Cancel

In summary, USSD has been an effective basis for the spread of MFS so far, but it does have drawbacks.

Advantages of USSD
- Works on all GSM handsets, regardless of the manufacturer
- Menus are simple and familiar to regular customers
- Does not require customer installation
- Data can be updated dynamically
- Menus can be reconfigured and updated dynamically
- Does not require an Internet connection
- Relatively fast access and response times

Disadvantages of USSD
- Text-based—no graphics
- Total session times are limited
- Users have limited time to input data strings and answer menu prompts
- Tree structure menus are limited
- Not secure, because it is based on SS7
- No data is stored on handset, so users may need to input credentials for every session
- Sessions may not initiate or complete if a MNO signal is poor. Frequent dropping of sessions can erode customer confidence in the overall MFS ecosystem.
- USSD access may potentially be blocked, throttled or made prohibitively expensive by MNOs due to bottlenecks created for competitive reasons, although thin SIM technology has been used to circumvent these bottlenecks.

STK Applications: Potential for Global Use

SIM Application Toolkit (STK) is an SMS-based remote access and user interface introduced in the 1990s and used where basic and feature phones predominate and smartphone penetration is low. In contrast to USSD, STK technology is embedded on the SIM card and menus are stored on the SIM card or phone.[22] MFS providers using STK include M-PESA Kenya, Equitel Kenya and Airtel Malawi.

STK is implemented in three layers:

1. A software application (also called an "applet") provided by a MNO, service provider or bank

2. A STK application programming interface (API) service offered by a MNO (which includes encryption keys)[23]

3. A user interface and STK translator through the STK application on the SIM card used on the handset

A SIM and STK-compatible phone is required to host the STK application. Usually, the STK will use (encrypted) SMS as a bearer for communication with a host.[24] On a basic phone, the STK menu may appear as one menu item when scrolling through the phone menus. On a feature phone or smartphone, the STK usually appears as an icon on the home screen. The handset receives instructions from the SIM card to perform specific functions, which are then communicated to an application server. STK user interface applications are usually protected by the SIM PIN, the phone lock PIN, or both. At both ends of a communication—the handset application on the user end and the STK server on the provider end—messages that contain user credentials and transaction data are encrypted. The server decrypts communications for action by the service provider.

While more secure and less vulnerable to interception of transaction data than USSD, STK is more expensive for a non-MNO MFS provider to operate since multiple SMSs (and accompanying MNO charges) may be required, even for simple balance inquiries. Moreover, because menus sit on SIM cards, it is harder and more expensive for providers to update them. Some service providers obtain better STK pricing through use of so-called thin SIM technology. STK is unavailable on some Android-based smartphones due to operating system restrictions.[25]

In summary, STK has potential for global use, except on smartphones.

Advantages of STK

- Works on most basic and feature phones
- Does not require customer Internet access
- SMS-based technology works relatively well in poor mobile coverage areas
- Most communications have end-to-end encryption between the SIM card and the MNO or service provider
- Customers can easily find STK menus on their mobile phones

Disadvantages of STK

- Centralized control of pricing and issuance for SIMs with STK capabilities. Service providers may need to implement thin SIM technology to overcome competition-related centralized STK gateway and pricing issues.
- Can be relatively expensive, as multiple SMSs are usually required to update menus on the handset and multiple messages are required for transactions
- Encryption and decryption may slow the transaction process, leading to transaction drop-off
- Does not work on some smartphones using newer versions of the Android operating system

EXHIBIT 3

STK-Based Menu on Safaricom Kenya's M-PESA[26]

Photo credit IC4D Blog
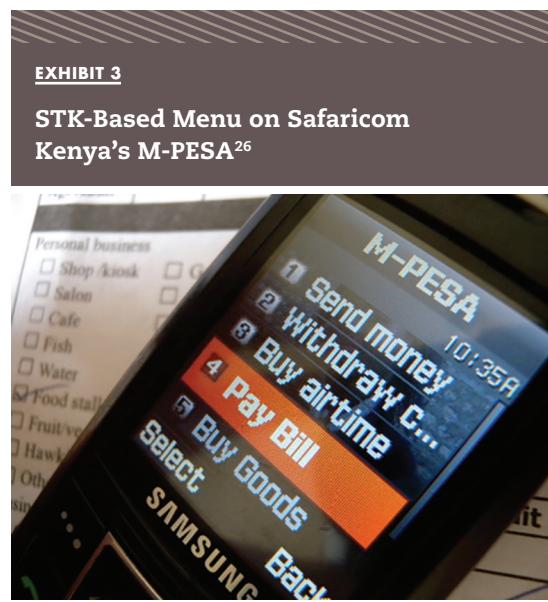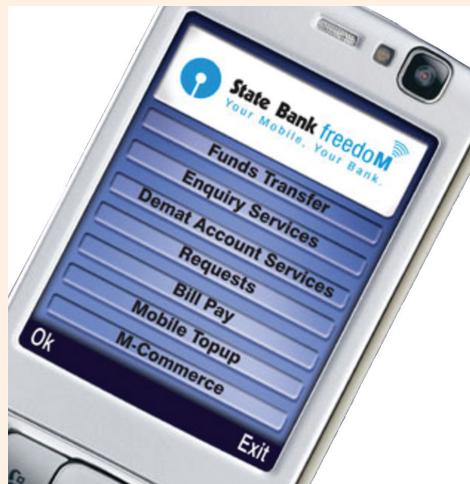
EXHIBIT 4

State Bank of India Java App

State Bank of India's use of a secure Java-based application on a feature phone to send/receive encrypted SMS-based transaction and update messages.[27]

Photo credit Afternoon Dispatch and Courier

Java-Based Feature Phone Applications: Cheaper and Quicker Than USSD

Java-based applications represent a growing alternative access method for MFS using feature phones. The menus are relatively easy to use, with an icon-based user interface that makes it easier for semi-literate or illiterate users to navigate service menus.

Unlike STK applets, MNOs do not need to enable Java applications to operate on their networks, and users can interact and transact with their service provider even without mobile data.[28] Users can install a small application for MFS access onto a phone either through Bluetooth or over the air using WAP.[29] The Bluetooth loading method known as "sideloading" requires the customer to have a Bluetooth-enabled phone and access to a MFS agent, who loads the Java application onto the phone through Bluetooth transfer—a simple transfer of information between two devices.[30] In the over-the-air method, the service provider sends the user a WAP download link for the Java application through a simple SMS or through a technique known as "WAP Push." The Java app is installed onto the feature phone once the link is clicked, and this removes the need for the user to travel to an agent. The small amount of data required for the applet download can be provided at no cost to the customer by a MNO or service provider.[31]

Usually only one mobile-originated SMS and one mobile-terminated SMS is required per transaction.[32] The compartmentalized design of many of these Java applets and applications means that a minimal amount of data (i.e., SMSs) is sent per transaction compared to the stream of SMSs characteristic of STK access. Similarly, application updates require fewer SMSs than STK. Java applet-based transactions are also secure, using encrypted SMS communications methods to enable end-to-end security.

In summary, Java-based methods of access may be less costly for consumers and service providers and quicker than USSD sessions or mobile data packages in most markets, since revenue-rich voice channels are not blocked as with USSD-based services.

Advantages of Java-based Apps
- Uses bank-grade security
- End-to-end security of transactions between the handset and the service provider, switch or bank—as different from the cleartext characteristic of remote access through USSD
- Consent of the MNO is not required to enable the application to operate on its network—unlike USSD and STK applets
- The user can complete transactions with the service provider even without mobile data[33]
- Because the amount of data required to set up the service is small, MNOs or service providers can potentially offer customers the download for free

- Icon-based menus are relatively easy to use—compared to the text-based USSD access—especially for semi-literate users
- Only one mobile-originated SMS and one mobile-terminated SMS is typically required per transaction
- Lower transaction costs for both consumers and service providers (generally)

Disadvantages of Java-based Apps
- There are fewer Java-based systems available for MFS on the market
- These apps do not work on most basic phones and they may not work on all feature phones
- Systems require an integration point to the transaction engine through a vendor's proprietary server to a core banking system or a switch
- The entire system may be dependent upon a single technology vendor for both the transaction server and the Java application. Depending on the agreement reached with the vendor, each of the existing service providers and banks may need to agree to implement the same application from the same vendor

Sound-Based Access: Universally Compatible and Secure, But Somewhat Convenient and Relatively Expensive

Acoustic-based access technology—also known as sound-based or Near Sound Data Transfer (NSDT)—is an alternative remote access technology that aims to be MNO-independent.[34] With this technology, the microphone of any basic phone, feature phone, or smartphone can be used for data capture, with the standard MNO voice channel acting as the data transporter. Thus, it can be used on all phone types. Transaction data is encrypted through the phone's audio channel using cryptosounds.[35]

This technology is particularly well-suited for merchant or agent use, either through a POS device or the merchant's own handset. During the transaction, the merchant enters an amount on the POS terminal or handset on the customer's behalf. The customer enters his or her phone number and PIN. The acoustic platform then calls the customer's phone. The customer answers the call, places the phone next to the terminal or agent's handset, and a one-time encrypted password is exchanged through the non-audible cryptosound between the two devices, completing the transaction. A similar process exists for person-to-person transfers, as long as the parties hold their phones close to each other.

This technology is used by Yes Bank (India), Pepele Mobile (Democratic Republic of Congo), Netcash (Zimbabwe), MoboMoney (India), UltraCash (India) and Alipay (China). The system may be especially well-suited to merchants in India, where there are more than 20 million merchants but only one million POS machines.[36]

Advantages and Disadvantages of Sound-Based Access:
- Well-suited for merchant payments
- Can be used on all types of phones
- Crytpo-based calls can be a more secure method of doing additional (so-called two-factor) transaction and ID authentication than the inherently insecure SS7-based SMS or NI-USSD
- Cost per call for transaction authorization may be prohibitive for merchants and customers, relative to smaller data sessions
- Not dependent on MNO gateway permissions
- Access may be dependent on a single vendor's proprietary solution
- Proprietary POS devices may be required

2

Effect of MNO Coverage on the Spread of Mobile Financial Services

High quality and ubiquitous MNO coverage provides the lifeblood for MFS success and evolution. Complete geographic coverage has strong momentum. In many or most countries competitive forces push MNOs toward nationwide coverage, and regulators add further impetus through universal service obligations.[37] However, nationwide coverage does not necessarily equal nationwide quality of service. For example, MFS delivered through USSD are particularly vulnerable to poor connections: if the signal is not strong and steady, sessions are often terminated midstream, forcing users to start over. By contrast, STK is mostly a store-and-forward communications technique based on SMS technology, which although sensitive to a poor signal, will in many cases, automatically re-send a transaction message when the mobile signal is stronger.[38]

Successful MFS provision requires either high quality on low-speed networks (i.e., for USSD-based systems) or higher-speed networks, coupled with suitable user interface and access technologies. The gap in mobile data coverage provided by MNOs in many MFS markets in the developing world manifests itself as a concentration of high-speed mobile data coverage primarily in urban and more densely populated areas and along national roads. Outlying and rural areas have just low-speed 2G-type access. This may deter users without high-speed access from migrating to smartphones, and even customers with smartphones may not use smartphone-based apps, which rely on higher mobile data speeds to provide an optimal user experience. Smartphones, on the whole, do not operate efficiently with narrowband 2G-type GPRS and EDGE bearer technologies (see Annex A).
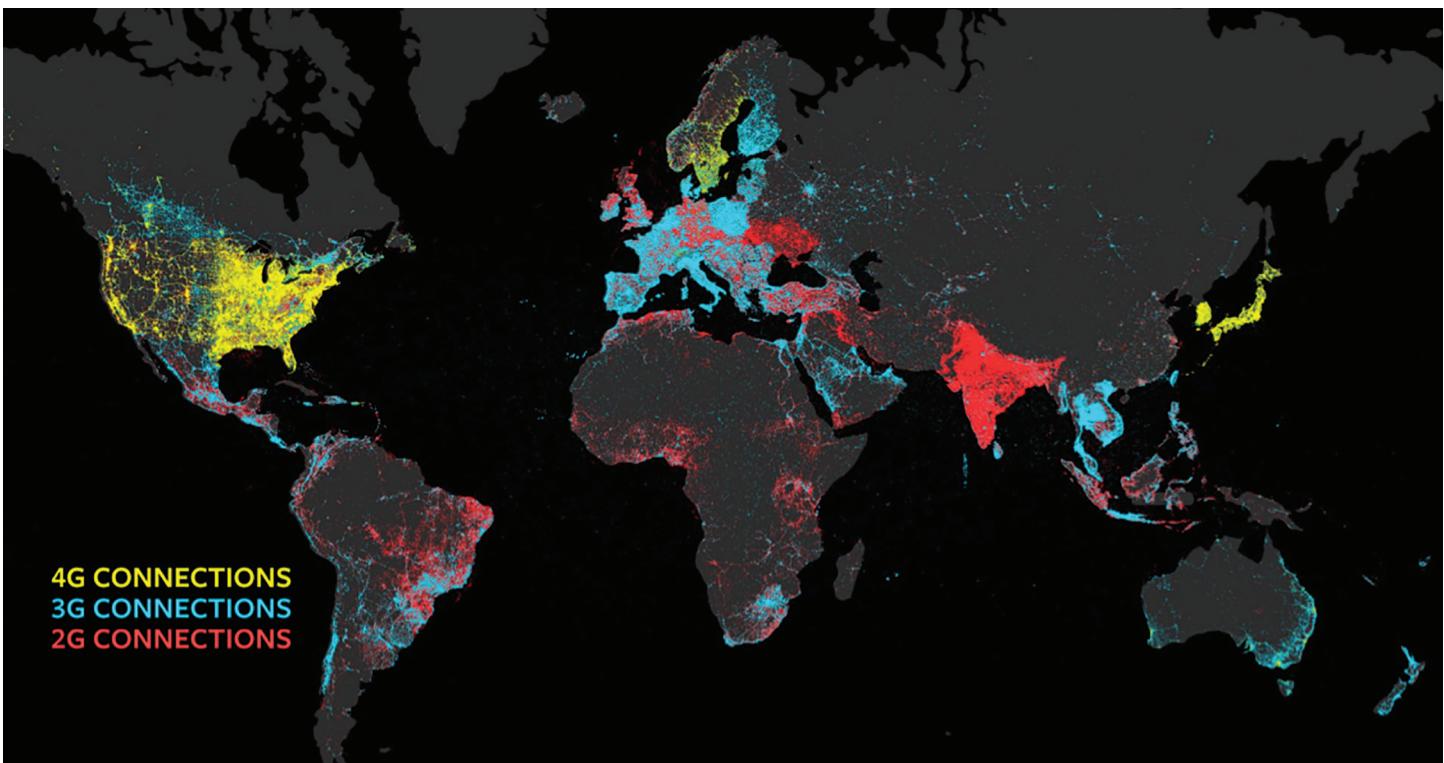
While much is made of the falling costs and rapid adoption of smartphones across the developing world, the current paucity of nationally available higher mobile data speeds remains a bottleneck. That is, while 2G-type mobile date coverage may be relatively ubiquitous, high-speed 3G and higher 4G mobile data coverage is not a given,[39] and a gap in 3G/4G coverage is characteristic of many MFS markets in the developing world.[40] The scope of 4G connections as compared to 3G and 2G connections is limited primarily to high income economies, as shown in Exhibit 5. Coverage is concentrated in urban and densely populated areas, and coverage gaps show the extent of geographic inequality of access.[41]

The coverage gap, generally, is due in part to high infrastructure and spectrum costs for 3G and 4G in many parts of the world. Part of the problem is physics: in short, the higher the frequency the MNO base station operates on, the shorter its range. Hence, the 2100 MHz frequency range used in most 3G deployments has a smaller coverage area than 900 MHz signals used for 2G-type coverage and therefore needs far more base stations per area than the 2G-type systems operating at 900 MHz. And while 3G signals can operate at 900 MHz, not all smartphones have 900 MHz 3G capabilities: the norm for GSM-based handsets generally is 900 MHz for 2G use and 2100 MHz for 3G use.[42] Coverage gaps also affects phone battery life: the further away the base station is from the handset, the more the handset must search for it, which then drains the battery much faster. This effort is especially true with smartphones trying to connect to 3G base stations operating at the poor coverage 2100 MHz frequency range (the norm)—the phone always needs to be searching for a nearby base station.

While much is made of the falling costs and rapid adoption of smartphones across the developing world, the current paucity of nationally available higher mobile data speeds remains a bottleneck.

Global Connectivity Speed[43]

4G CONNECTIONS
3G CONNECTIONS
2G CONNECTIONS

Source Facebook, 2016

Without a shift to reliable 3G coverage, users will remain unable to fully utilize the media-rich features of smartphones. Therefore, for the next several years, vendors and MNOs should cater to feature phones and USSD.

Implementing 3G (and 4G) nationwide becomes a major infrastructure capital cost for MNOs, which may accordingly concentrate 3G (and 4G) coverage mainly in densely populated urban areas where they ostensibly get a better a return on investment. National high-speed mobile data coverage may improve over time, especially if the new 700 MHz frequency bands are made available by regulators, as these have better range than the current 2100 MHz coverage, or if MNOs are mandated to implement 3G coverage by national regulators as part of national universal service obligations.[44]

Indeed, the next arms race for MNOs and other new entrants is at the 700 MHz and 800 MHz frequency ranges, which allow mobile broadband services to be offered at far greater coverage areas than the current 900, 1800, 2100 MHz frequency ranges.[45] The new spectrum is part of what the International Telecommunication Union (ITU) calls the "digital dividend"—the amount of spectrum in the frequency band of 470–862 MHz to be released (or "refarmed") as a result of the global switchover from analog to digital TV.[46] Lower frequencies generally mean there is more coverage per base station, fewer base stations to cover a specific area, and therefore lower capital costs overall to provide higher-speed mobile data. The propagation characteristics of these frequency bands can facilitate improved mobile broadband coverage in rural areas for MFS, as well as better indoor coverage in more densely populated areas.

If regulators make these new frequency bands available, or if they mandate implementation of 3G coverage (as a minimum) as part of universal service obligations, higher-speed mobile data coverage will improve over time.[47] MNOs may, however, lack the appetite to provide services on these new bands if spectrum auctions or mobile licenses costs are too high.

A potential, but partial, solution to the paucity of high-speed mobile data coverage and associated spectrum may be the use of LTE-U (unlicensed) mobile data technology, which allows an MNO to provide high-speed LTE coverage in unlicensed—that is, free for all to use—spectrum. However because of the (high) frequencies it could operate on, LTE-U coverage is likely to be poor, while mass-market availability of handsets that support LTE-U is still a while away.

The limited availability of high-quality, high-speed coverage, especially in rural areas, has profound implications for financial inclusion policy. For the next several years, vendors and MNOs should cater to feature phones and USSD. Without a shift to reliable 3G coverage, users will remain unable to fully utilize the media-rich features of smartphones.[48] This time frame may differ from market to market, but within much of Sub-Saharan Africa, the Indian subcontinent and Latin America, USSD is likely to dominate until at least 2020. Until provision gaps in high-speed mobile data are filled, basic and feature phones are likely to predominate in outlying areas, resulting in less availability of richer MFS products, such as credit.

Which Phone for Which Purpose?

Basic and Feature Phones Still Dominate the MFS Market

Most BoP users in MFS markets use basic and feature phones. These models constitute about 70 percent of the phones used in the developing world.[49]

Product evolution over the past few years has blurred the hard distinctions between these devices, but in general, basic phones—low-end phones—have limited features, no factory-installed or user-installable third-party applications, and very limited data connectivity (if any).[50] Users can, for the most part, access MFS platforms through basic USSD and STK technologies. Users' quality of service may be reduced due to poor power output and antenna design in some of these devices.

Feature phones represent a midway design point, characterized by limited functionality and proprietary operating systems designed either by the phone manufacturer, or as part of an operating system designed by the primary component maker. They are by far the most common device type worldwide. In India, industry data shows that despite a surge in shipments of smartphones, around 60 percent of mobile subscribers use feature phones.[51]

Some MFS markets show glacial increases in smartphone penetration. Adoption within the East African Community is 17 percent and within the Southern African Development Community it is 24 percent.[52] Smartphone penetration rates though are generally higher in parts of Asia.[53]

The expiration of earlier mobile-related patents is fueling growth and reducing costs. Many of the initial patents on basic mobile phone technology have expired, allowing

Basic and Feature Phones At-A-Glance

Basic Phone Characteristics
Photo by: Ian Fuller
- Low price (range below US$6)
- Small screen (1.1 to 1.3 inch)
- Monochrome or low-resolution color screens
- Up to 1 week battery life while in standby mode
- Cannot use third party applications
- USSD version 2 and SMS for connectivity
- Some ability to use STK
- Cannot use Java-based MFS applications
- GPRS or EDGE as connectivity or no IP-based connectivity at all
- No Bluetooth
- No WiFi

Feature Phone Characteristics
Photo by: InDIa7 Network
- Slightly larger screen size larger (median of 2.7 inches)
- Low quality and low resolution screens
- Long battery life, 1-3 weeks in standby mode
- Factory-installed social media applications
- External connectivity options such as 2G-type GPRS/EDGE+, and sometimes also WiFi and Bluetooth
- WAP capabilities
- Dual SIM capabilities[54]
- VGA-quality camera
- Minimal memory storage (Micro SD card slots for memory expansion)
- Slower memory
- Incompatibility between feature phone chipsets and no universal Java MFS application support
- Few implementations of 3G or 4G mobile data support

EXHIBIT 6

Basic and Feature Phone Use

Percentage of connections, excluding machine-to-machine

Legend:
- Sub-Saharan Africa
- MENA
- Asia Pacific
- Latin America and Caribbean
- North America
- Europe

Source GSMA, 2016

EXHIBIT 7

Penetration of MFS Technologies on Tigo Network, 2014

Percentage of connections by device type

Legend:
- Basic phone
- Feature phone
- Smartphone
- Modem

Use of basic phones, feature phones, smartphones and data/Internet of things modem devices on Tigo networks during 2014 in selected African countries (Ghana, Senegal, Democratic Republic of Congo, Tanzania, Rwanda, and Chad)

Source Tigo, 2014

EXHIBIT 8

Emerging Phone Brands and Their Regional Penetration[55]

manufacturers to add 'smart features' to enable feature phones to resemble smartphones. Subsequently, mobile phone manufacturers no longer have to pay licensing fees to former patent holders. (Devices can involve thousands of patents, for example, royalties related to internal memory storage and RAM.)[56] This, coupled with improvements in component manufacture of all-in-one system-on-a-chip (SOC) technology (see Exhibit 15), has led to a flood of phones and tablets entering the market from newer manufacturers that are rapidly displacing the established brands that dominated the early days of modern GSM mobile communications.[57]

The first SOC-based mobile phones appeared in 2005–06, primarily from Chinese and Indian phone manufacturers, who now represent six of the global top ten smartphone manufacturers (the top brands at the end of 2016 were Alcatel, Apple, Coolpad, Gionee,

Huawei, Lenovo, LG, Oppo, Samsung, Tecno, Vivo, Xiaomi and ZTE).[58] Some other newer brands that now have significant global market presence include AG, Blu, Doogee, Hisense, Itel, Maxwest, Meizu, Micromax, M-Phone, Nubia, Oneplus, Oppo, Plum, Prestigio, Symphony, TC, Tecno, Torque, Viettel, Vivo and Yezz. In many cases, these devices may derive from the same factory, with some customization of the user interface or some technical specification for a particular brand. This manufacturing, branding and distribution arrangement is typical for many electronic devices made in China.

The average selling price for smartphones across Sub-Saharan Africa was US$160 in 2015, down from around US$230 in 2012.[59] An analysis of smartphone pricing in first quarter of 2017 indicates that prices have dropped even further, with some entry-level Android-based smartphones priced at around US$30 or even less.[60]

EXHIBIT 9

Billboard for Oppo Smartphones in Bali, Indonesia[61]

Photo credit Leon Perlman

Devices are catered to specific market segments. MFS platform vendors and service providers cater their products and services towards the access mechanisms characteristic of their respective markets. Thus, while users in the developed world use mobile payment and banking apps for 3G/4G smartphones, users in the developing world use slower (narrowband) 2G-type access mechanisms, primarily text-based user interfaces such as USSD, STK, and to some extent, WAP. Some MNOs are now offering Internet-based apps for smartphones in the developing world, even though in many cases there is no national 3G/4G mobile data coverage and the smartphones in use have below-average specifications. For example, some lack high-speed 3G mobile data capabilities; touch-screen sizes are small and of low resolution; there is a lag in executing touch screen commands which may induce 'fat finger' data input mistakes by users (in which an error is caused by accidentally pressing the wrong key); processors are relatively slow; internal storage memory and RAM memory are minimal; and battery life is limited.[62]

Basic Phones: Still Widely Used

There is a large base of basic phones installed worldwide, with new models released regularly. The GSMA estimates that while basic and feature phones currently represent 50 percent of the market, by 2020, the percentage will drop to 30 percent.[63] Considering this, MNOs, vendors and service providers need to continue to support basic phones via USSD and STK for MFS access for the foreseeable future.[64]

Basic phones provide primarily only voice and SMS, and feature small (1.1 to 1.3-inch) monochrome or low-resolution color screens. They may or may not use (at least) GPRS or EDGE bearer services. A basic phone cannot load any applications such as Java applications.

Basic phones are typically characterized by:
> Low price (range below US$6)
> Small (1.1 to 1.3 inch) monochrome or low-resolution color screens
> Usually up to 1 week standby time (battery life while in standby mode), which is ideal for places with limited electricity. Some models launched in 2017 claim up to a month standby.
> Cannot use third party applications
> USSD version 2 and SMS for connectivity
> Some ability to use STK
> Cannot use Java-based MFS applications
> GPRS or EDGE as connectivity or no IP-based connectivity at all
> No Bluetooth
> No WiFi

Feature Phones: Growing More Popular and Getting Smarter

Feature phones are perennially popular and remain the primary means of access for most MFS-based systems in the world.[65] Since they operate primarily with 2G-type connectivity, they can be used in a wide range of geographies where high-speed 3G/4G mobile data coverage is not yet available.

Feature phones are usually low-specification devices, with many lacking 3G/4G access or touch screens. However, most feature phones produced since 2008 have Bluetooth, WAP-based phone browsers, an ability to install and run Java applications, and a camera. In addition to USSD, feature phones can usually run STK-based applications that provide secure access to MFS platforms, such as M-PESA in Kenya.

EXHIBIT 10

Characteristics of Phone Types Needed for Various MFS Services

The first four services are fundamental MFS activities.

MFS ACTIVITY	BASIC	FEATURE	SMART
Check balances	Y	Y	Y
Person-to-person transfer	Y	Y	Y
Cash in/cash out	Y	Y	Y
Pay bills	Y	Y	Y
Secure transactions	Y	Y	Y
Electronic Know Your Customer verification with camera	N	Y	Y
Agent location	N	Y	Y
Interactive assistance	N	N	Y
Change profile	N	N	Y
Easily add beneficiaries	N	N	Y
Online shopping	N	N	Y
Spending dashboard	N	N	Y
Transaction dashboard	N	N	Y
Add funds via Visa/MasterCard	N	N	Y
Agent rating system	N	Y	Y
One-touch transaction dispute query	N	N	Y
NFC payment[66]	N	Y	Y

EXHIBIT 11

Basic Nokia Phone[67]

Photo credit Ian Fuller

EXHIBIT 12

Nokia 220 Feature Phone[68]

Note the Facebook and Twitter applications.

Photo credit InDIa7 Network

Many Chinese and Indian manufacturers produce basic feature phones, and they are sold in markets, small stores and online markets within unsubsidized price ranges of US$7 to $30, depending on the particular features.

Feature phones are typically characterized by:
- Dual SIM capabilities[69] (when dual SIM phones are lacking many people purchase two phones)
- VGA-quality camera
- Micro SD card slots for memory expansion
- External connectivity options such as 2G-type GPRS/EDGE+, and sometimes also WiFi and Bluetooth
- Factory-installed social media applications
- Long battery life—up to one week or even more of standby time—which is well-suited for MFS. Models launched in 2017 claim up to three weeks of battery life.
- WAP capabilities
- Screen size between 1.4–4 inches, with a median of 2.7 inches

Drawbacks include:
- Minimal memory storage
- Slower memory
- Lower-quality and low resolution screens
- Incompatibility between feature phone chipsets means that there is no universal Java MFS application support, so that service providers must cater to both non-Java and Java-compatible feature phones.
- Few implementations of 3G or 4G mobile data support

Feature phones sometimes operate on proprietary operating systems or mass-market operating systems, predominantly from chip manufacturers Mediatek and Spreadtrum. Despite this, not all feature phones support third party software. However, if they do, they run applications on Java or similar software or are made for the proprietary operating systems of the feature phone.[70] Indeed, the most common Java "application" platform across feature phones is the Java 2 Platform, Micro Edition (J2ME) software environment.[71] However, this is not universal, since some phone chipsets support application development alternatives such as Mediatek's MAUI Runtime Environment (MRE).[72] Many feature phones already incorporate popular factory-installed social networking facilities such as Twitter and Facebook, but do not offer many other applications for customer installation. An influx of "smarter" feature phones, e.g., supporting NFC and 3G and sold as part of a larger phone portfolio by some manufacturers, is emerging.

Due to low manufacturing costs, feature phones are affordable for low-end to mid-range customers who cannot afford smartphones. Like basic phones, there is a large base of feature phones installed worldwide, with new models constantly being released. All stakeholders—MNOs, service providers, policymakers and regulators—must take note of the feature phone's widespread prevalence, affordability, popularity and suitability for MFS, and therefore continue to support USSD and STK for MFS access for the foreseeable future.

Smartphones: Developing Markets Are Slowly Embracing Them

As the data show, smartphones are increasingly used on mobile networks around the world.[73] The prices of these devices have dropped considerably; a low-end entry smartphone now costs around US$30 or even less.[74] Smartphone penetration will significantly increase as new brands worldwide sell cheaper devices using a new breed of all-in-one SOC chipsets. From a competitive policy perspective, an advantage of smartphones is that their use of over-the-top (OTT) Internet-based, customer-installed MFS apps can circumvent competitive restrictions related to USSD and STK access (though net neutrality issues may yet emerge).[75]

Smartphones provide the most promising alternative for enhanced service offerings and integration into merchant and payment infrastructures. Most smartphones use a variant of Google's Android operating system,[76] and the devices allow OTT apps to be installed for MFS and mobile banking, and NFC-based payments to merchants. Smartphones can accommodate a range of enhanced features from agent location mapping, to identity capture and user authentication using built-in biometrics, which may prevent many users from accessing many basic and government services.

All stakeholders—MNOs, service providers, policymakers and regulators—must take note of the feature phone's widespread prevalence, affordability, popularity and suitability for MFS, and therefore continue to support USSD and STK for MFS access for the foreseeable future.

Moreover, with the advance of smartphones, MFS customers are in for significant user experience and user interface improvements, especially when compared to the fixed-menu text designs of USSD and STK.[77] Large touch-screen displays allow for more interesting, informative and interactive customer interfaces. Smartphones are likely to be the choice of mostly urban MFS users, where devices can easily be recharged and high-speed mobile data access is readily available.
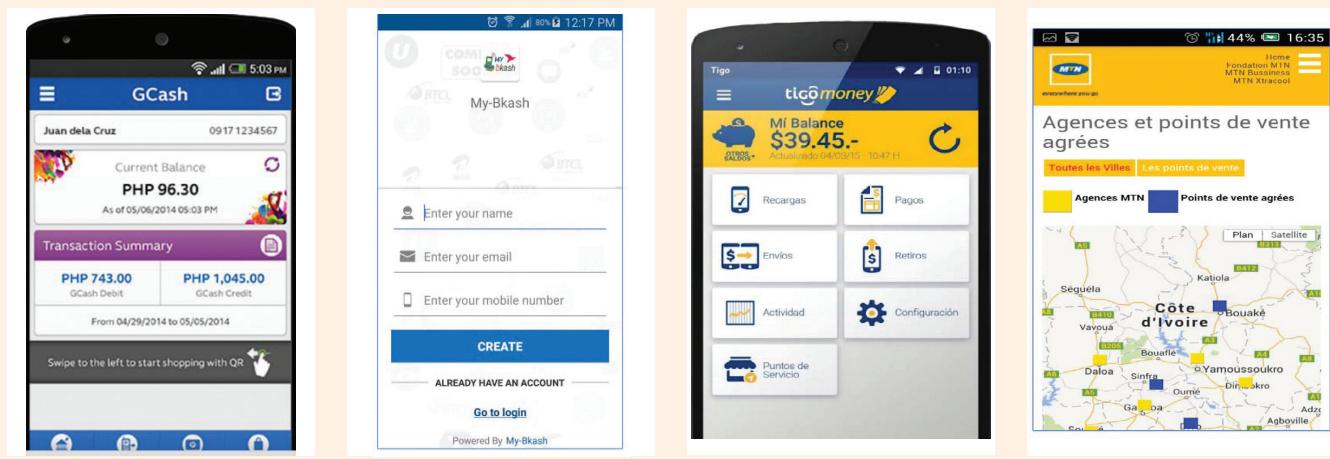
Some challenges, however, may help explain the relatively slow pace of smartphone adoption in many emerging markets. Many smartphones in MFS markets are of low specification, which may impede user uptake:

> Sizes of the newest MFS apps touch the upper limit of available storage space on devices whose RAM—the amount of phone memory available—is sufficient to run only a few applications efficiently and whose internal storage can only contain a few applications.

> Poor battery life is incompatible with the always-on functionality of MFS.

> Touch screens are low resolution and relatively fragile, causing frequent 'fat finger' mistakes.

> Although the UI and UX are enhanced, users in some markets may be intimidated by the complexity.[78] When such problems are detected, service providers should provide training for their agents and customers on the use of these apps or simplify the apps.[79]

> Not all smartphones sold in developing markets have 3G (or higher) capabilities, often because the manufacturer wants to save on 3G chipset licensing costs in price-sensitive markets.[80] One royalty calculation—based on total announced rates for mobile-related royalties—estimates this cost at about 5 percent per smartphone.[81] Lack of 3G coverage, as previously explored, may lead to a sub-standard UX and drive customers away since most MFS and mobile banking applications use rich media and require higher-speed connectivity to operate.[82]

> Not all apps are usable across all Android versions. Design changes across the various Android versions are not necessarily backwards-compatible to previous versions, so the latest version of OTT Android-based MFS app may not work on an older Android phone.[83] For example, smartphones using the older Android 2.3 operating system released December 2010 are no longer supported by many app makers today.

> Updates to apps or to the Android system itself may be problematic. Many smartphones lack the internal memory capacity to be able to upgrade to the latest operating system version.[84] Moreover, because they are large files, Android updates and MFS apps are expensive to download. Customers frequently bear the associated data costs, although some service providers and MNOs provide their MFS app download for free.

EXHIBIT 13

Smartphone OTT MFS Applications: GCash, Bkash, Tigo and MTN

Tests during the course of 2016 and 2017 indicate that the latest versions of these MFS-oriented Android smartphone over-the-top (OTT) apps available on the Android Play Store from GCash, Bkash, Tigo and MTN were not compatible with a Huawei/Vodafone 858 released in 2012, nor a Samsung GT-S6500 Galaxy Mini 2 released in 2013. Most of the apps on the Android Play store checked in March 2017 required Android version 2.3 or higher and required more than 2MB of available storage space on the device to download and install.

Source Google Play Store, 2017

Hybrid "Smart Feature Phones:" An Emerging Trend

A curious trend during the course of late 2016 is the emergence of a new hybrid phone market segment straddling in between feature phones and smartphones. These, what we term "smart feature phones," usually have small non-touch, low-resolution displays; small memory capacity; a phone keypad characteristic of basic and feature phones; support 3G/4G; and use the latest Android operating system. The 3G-only versions of these hybrid phones sell for under US$25. Exhibit 14 shows one of the first of these new hybrid phones.

EXHIBIT 14

Example Hybrid Smart Feature Phone

A new market segment of hybrid "smart feature phones" is emerging in the developing world. The Wellstec F18 smart feature phone shown here has 4G, 256 MB storage memory, a small 2.4 inch non-touch display, and uses Android 6.0 OS.[85]

Photo credit Leon Perlman

Mobile Phone Components and Their Impact on MFS

4

Mobile phone prices have dropped significantly with the expiration of key patents as well as the emergence of system-on-a-chip components that integrate most of the critical mobile phone features onto a single chip. The user experience is also enhanced by improvements in phone display size and resolution, as well as enhanced battery technologies. These improvements allow customers to sustain their ability to access mobile networks and MFS products and funds. While most basic and feature phones are robust, many of the smartphones introduced into developing markets by new device manufacturers are of relatively low quality compared to the developed world models, but designed to facilitate an affordable price entry point. In particular, their touch screens are power-hungry and reduce battery life; they are fragile; and there is often a lag time on the touch screens. These shortcomings limit access to MFS, cause mistakes in entry, and lead to costs for users due to breakage. The message that we have emphasized repeatedly is again underlined here: MFS based on feature phones are a strong alternative for the present, while smartphones have some distance to travel before they will be cost-effective and robust enough to support MFS for lower-end users.

One important development with MFS implications that speaks for smartphones is display and camera technology that can be used for biometric-based identity capture and authorization, which can allow for the easier onboarding of MFS customers and increased access to government and other social services.

System-on-a-Chip (SOC) Technology Revolutionizes Phone Design

The emergence of the system-on-a-chip (SOC) concept, which incorporates a number of individual but complex mobile phone components onto a single silicon chip, has spurred the emergence of new mobile phone brands that use these chipsets to produce cheap basic, feature and smartphones (see Exhibit 15).[86] SOC technology has dramatically lowered phone production costs while improving performance. In addition, the newest processors are faster and allow for multitasking, and they extend battery life because they use less power.

At the 'core' of the SOC is the central processing unit, which mediates the efficiency, feature, and performance of the device. The more cores on a SOC, the faster they can split up the power needed to operate multiple
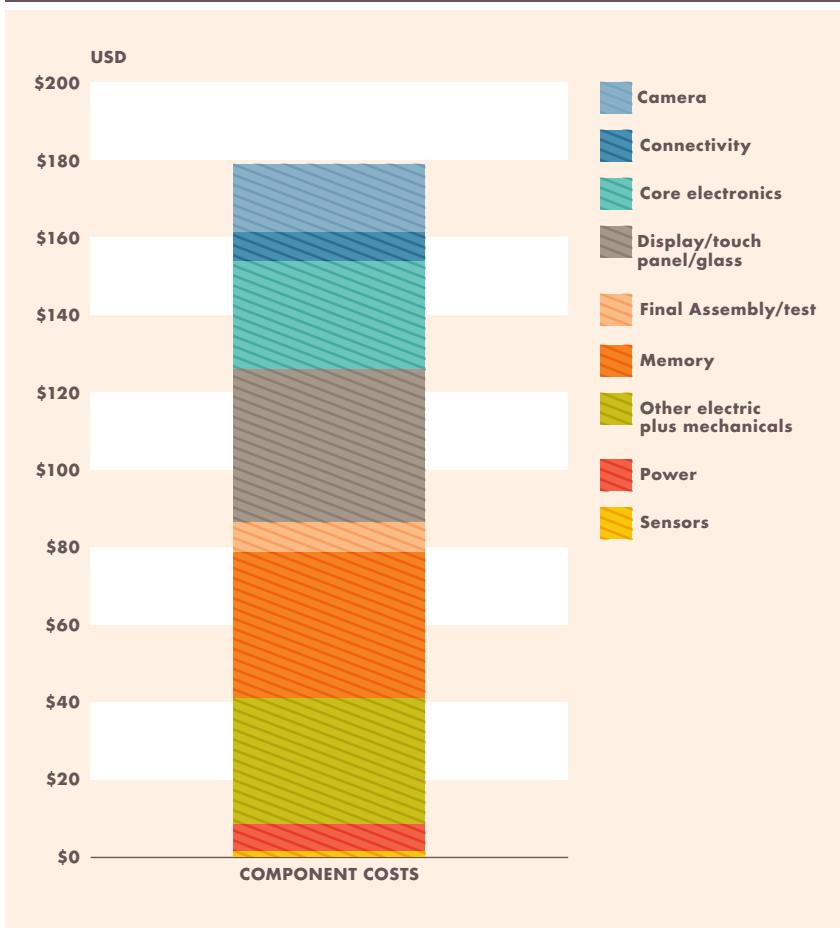
Mobile phones released since 2006 use system-on-a-chip (SOC) chips, which integrate most of the critical mobile phone components onto a single component. A SOC can contain the central processing unit (CPU), some memory for processing applications, graphic processing unit (GPU), and the mobile radio system (2G/3G/4G, or WiFi, GPS/GLONASS or Bluetooth).[87]

Because a single SOC is much cheaper to produce than its individual components, this has led to a surge in manufacturing, particularly for basic and feature phones with enhanced capabilities.

Among the relatively new SOC manufacturers, Mediatek and Spreadtrum dominate the market for feature phones.[88] For smartphones, the predominant manufacturers are Apple, Qualcomm, Texas Instruments, Intel, Samsung, ARM and Mediatek.
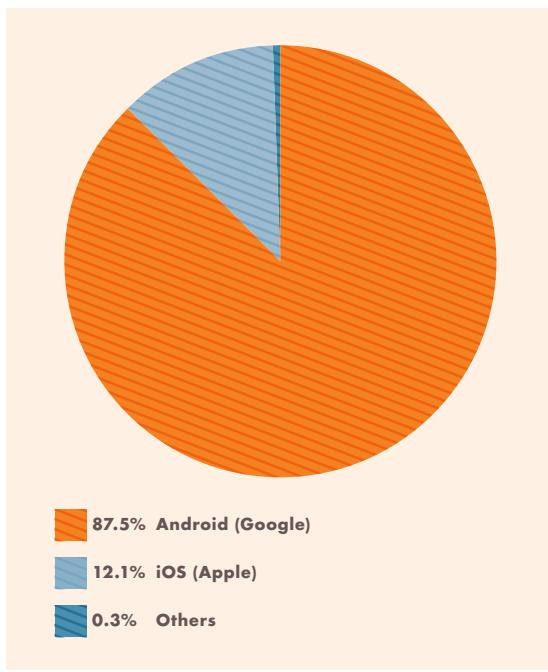
It appears that some Mediatek feature phone SOCs will not run standard Java applications used in MFS, requiring bifurcation of application development for use on feature phones.

EXHIBIT 16

## Relative Costs of Components to Build a Mid-Range Smartphone[89]

Legend:
- Camera
- Connectivity
- Core electronics
- Display/touch panel/glass
- Final Assembly/test
- Memory
- Other electric plus mechanicals
- Power
- Sensors

Y-axis: USD ($0–$200)
X-axis: COMPONENT COSTS

EXHIBIT 17

Worldwide Smartphone Sales by Operating System in Third Quarter of 2016[90]

- 87.5% Android (Google)
- 12.1% iOS (Apple)
- 0.3% Others

applications and processes on a device, and hence, the better the performance of the device.[91] While feature phones usually only have one core, smartphones can have dual-cores, quad-cores, hexa-cores, and even octa-cores.[92] The more cores, the more the features and increase in processing power.

The SOC and other critical components make up the bulk of the phone cost. Exhibit 16 provides a breakdown, for example, of the costs associated with the manufacture of a mid-range smartphone: the three most costly aspects of a handset are the electronic (mainly memory) components (at around 20 percent), the display (20 percent), and the SOC (25 percent) (note that the battery is not very expensive).[93]

Mobile Phone Operating Systems

The evolution of mobile phone operating systems has allowed feature phones to add additional (albeit limited) functionality, and for smartphones, to extend the utility of these devices beyond just telecommunications and related features. For feature phones, operating systems have been developed based on the remnants of the venerable Nokia mobile phone empire, as well as proprietary yet customizable operating systems from SOC manufacturers Spreadtrum and Mediatek. Most feature phone operating systems are proprietary, and do not allow for the installation of third party apps. New hybrid smart feature phones using Android OS may however alter that paradigm.

Mediatek's MRE and Series 30+ operating systems, for example, are based on the chipsets incorporated into the majority of feature phones released since 2010.[94] Some have built-in apps. Twitter and Facebook, for example, have factory-installed their applications in phones running MRE.[95]

Nokia operating systems remain from Nokia's halcyon days when its Symbian feature phone operating systems powered most phones around the world.[96] There will certainly be user defections from phones using these OSs as a result of instant messaging giant WhatsApp having discontinued support for the Nokia S40 and Nokia Symbian S60 operating systems at the end of 2016.[97] There is, however, support for WhatsApp on Java-based phones.[98]

For smartphones, Google's Android operating system dominates over Apple's iOS, Microsoft's Windows Phone, the BlackBerry operating system, Samsung's Tinzen, and another Nokia-derived operating system remnant, Sailfish.[99] However, apps written for newer Android versions may not be compatible with older Android phones.

Mobile Phone Memory Capacity Constraints

Mobile devices have two memory types: 'flash' memory for storage of user information and applications, and random access memory (RAM) to facilitate the execution of apps.[100] Some cheaper smartphones have just 512 MB of available storage and 512 MB of RAM, not enough to store MFS and user-selected apps.

Skimpy RAM capacity is detrimental to MFS because low RAM can result in an inferior user experience and an inability to run critical apps, while low internal storage may prevent the installation of some MFS-oriented apps and over-the air upgrades of some phones.

For example, Airtel Money Uganda requires 1.5 MB storage space; Tigo Pesa Bolivia requires 7.6 MB; GCash Philippines requires 6.4 MB; bKash Bangladesh requires 2 MB and Android 3.0; MTN Money Cote d'Ivoire requires 2 MB; while Zain Jordan's app requires 4.7 MB. These (and other) apps have to compete for storage space with factory-installed "bloatware"—superfluous third party apps, which the manufacturer is paid to install.

Battery Technology Affects Sustained MFS Use

An important factor for MFS is the need for devices to have sustained access to the mobile network operator. This requires batteries with the ability to provide reliable and long-lived power. Poor battery life may cut off user access to MFS systems and funds when they are most needed. Entry-level smartphones introduced into many markets have very poor battery capacity and poor usage times.

Longevity of battery life is not just measured in standby time and milliamp hour (mAh) storage capacity, but also through the batteries' ability to withstand real-life conditions such as heat and constant non-standard recharge cycles.[101] Feature phones and basic phones, with small screens and 2G-type technology, often have standby and usage times of multiple days and weeks, while smartphone usage time is, at best, usually less than 48 hours. Poor battery performance may be mitigated somewhat by the use by customers of a second, charged battery, which some manufacturers include in the box. The trend however—especially in the mid-and higher-end—is towards handsets with non-removable batteries. Fake batteries, also a factor in these markets, pose a health hazard: they have been known to explode.[102]

To keep prices low, many feature phones have battery power as low as 400 mAh.[103] For a smartphone to last at least a day with moderate use, it needs battery power of at least 2300 mAh. Low-end smartphones at prices below US$35 with 4-inch displays, however, tend to have a battery capacity below 1300 mAh, giving them a theoretical standby time around 48 hours, which in practice may be far less. When a user deliberately downgrades a smartphone's 3G mobile data access to 2G-type technology, the battery life of the device increases substantially.[104] The awareness and technical literacy to alter these settings, however, is not always available.[105]

Improvements in battery life occur very slowly. Usage improvements are more likely to come from more power-efficient SOC chips and more power-efficient displays.

Display and Camera Technology

While manufacturing innovations are improving the performance of mobile phone displays, tradeoffs remain between performance, cost and battery life. Predictably, for low-end smartphones, performance is often sacrificed to cost—with direct implications for MFS.

Depending on phone type and sophistication, one of several basic types of display technologies may be used (see Exhibit 18).[106] Some displays may use less sensitive first generation capacitive touch technology, rather

Battery Technologies Used in Mobile Phones

Most feature phones and low/mid-range smartphones use lithium ion (Li-Ion) batteries.[107] Higher-end smartphones tend to use newer high-capacity lithium-polymer batteries.

Lithium ion

This technology allows for very high charge capacity relative to the size and weight of the battery. These batteries first appeared in mobile phones in the late 1990s and have advanced for use in smartphones with higher capacities. These higher capacities, however, make lithium ion more fragile and thus require a protection circuit to maintain safe operation, which in turn results in lower battery capacity when used in feature and basic phones. Self-discharge is less than half compared to nickel-based batteries, but they tend to discharge more if used in temperatures above 15 degrees Celsius.[108]

Lithium polymer

Lithium polymer (LiPo) batteries are the most advanced batteries available on the market, with up to 40 percent greater use capacity than nickel-based batteries. They are usually cased in plastic, making them thinner and lighter than other battery types. They also do not suffer from memory effect, a battery chemistry artefact which reduces performance.

than the newer 'in-cell' and 'on-cell' technology where the touch sensors are embedded inside the display rather than in a separate touch sensor layer on top of the display.[109] This again may create a poor user experience.

Overall, lower manufacturing costs allow for lower-cost, higher-resolution mobile phone displays with lower power consumption and hence better standby and usage times. However, entry-level smartphones introduced into MFS markets use cheaper display components that consume more battery power and are easily damaged. These cheaper models may bring further user annoyances (and impediments to uptake), such as 'fat finger' input errors due to small screens and prohibitive costs for simple repairs to cracked phone screens.

One of the positive developments for MFS in this area is the advent of technology for biometric ID capture and authentication. Technologies are emerging that will allow

mobile phone displays to have biometric capture and authentication technologies built-in, allowing fingerprints to be captured for e-KYC purposes and authenticated for transaction purposes by simply pressing on the display glass. These techniques may avoid complications in capture characteristic of tactile-type fingerprint capture components on phones that are usually caused by environmental factors.

Phones with iris scanners using high-resolution built-in cameras are also emerging: the LYF Earth 2 Smartphone as well as the (now discontinued) Samsung Galaxy Note 7 both have iris scan features, with many others emerging during the course of 2017. Recognizing the trend, the Universal Identification Authority of India—the entity that controls the successful Aadhaar biometric-capture ID system—is providing application programming interfaces (APIs)—seamless technology interfaces—to allow these and other iris-enabled mobile phones to capture and verify users.

Manufacturing data for feature phones shows a steady demand in shipments, suggesting strongly that the projected pivot to a majority smartphone presence in MFS markets has not occurred. Exhibit 20 shows display panel manufacturing statistics for 2015, indicating steady demand for the shipment of display panels smaller than three inches—characteristic of feature phones—over the course of 2015 due to increasing demand in the feature phone market. This appears to correlate with findings of previous studies and *in situ* market investigations showing the dominance of feature phones in the developing world.

While this may reflect a general increase in market size for all devices due to general growth and a need for replacement feature phones, these manufacturing statistics do not support market projections that have smartphones overtaking feature phones in MFS markets by 2020.[110] Data showing feature phone distribution during the course of 2016 bolsters the view, with feature phones still showing robust sales. Indeed, Nokia (as part of its new brand licensing agreement with HMD Global) in February 2017 released a feature phone version of its venerated Nokia 3310 basic phone that was first seen 2000, and now sporting a color display and camera.

EXHIBIT 19

Display Types and Specifications Used in Mobile Phones

LCD is the predominant technology used in basic phones, and newer types use less power. LCD is used now mostly in monochrome or low color saturation displays in basic phones.
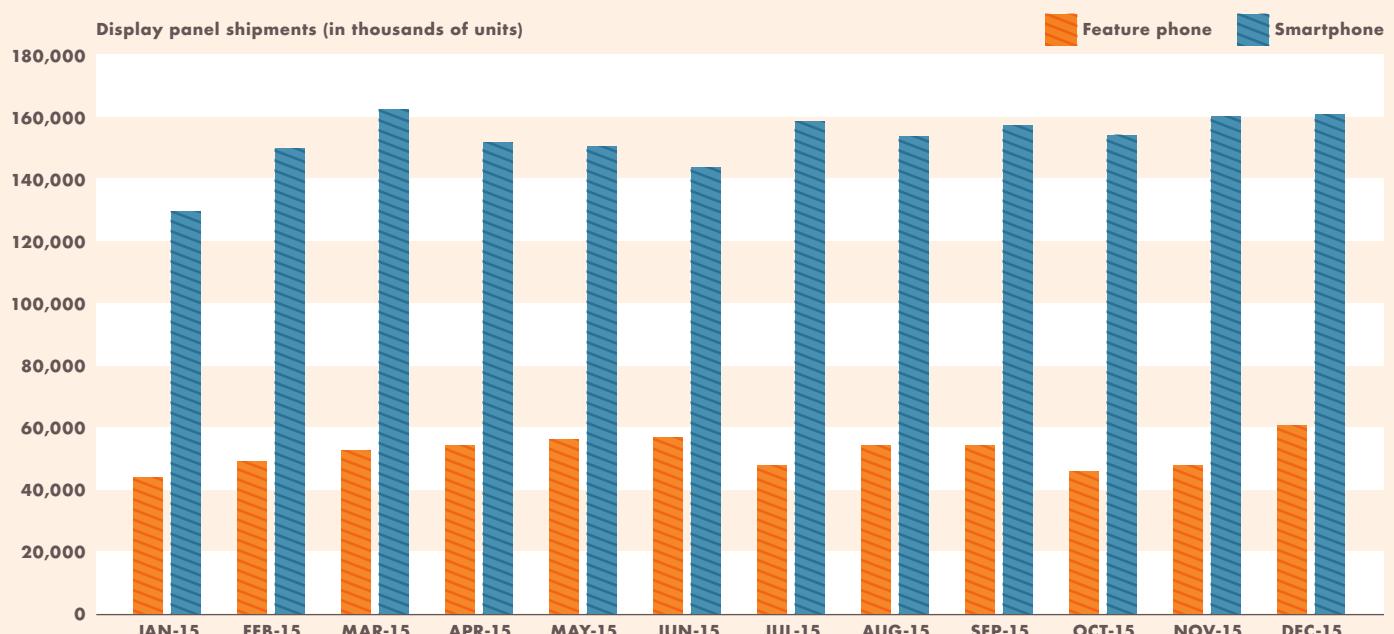
TFT-LCD is an active-matrix LCD found on low-end smartphones, basic phones and feature phones.[111] Each pixel on a TFT-LCD has its own transistor on the glass itself, offering more control over the images and colors. However, TFT-LCDs offer relatively poor viewing angles, and consume more power than other display types.

IPS-LCD is a variant of TFT-LCD, offering thinner displays and better viewing angles. It requires a more powerful backlight, which while delivering more accurate colors and allowing the screen to be viewed from a wider angle, consumes more power.[112]

AMOLED is a new technology that uses organic materials to allow for faster and more precise control of the image needed for higher definition smartphone displays with a lot of pixels.[113] Many of the newer smartphones use a next-generation version: Super AMOLED.

Display sizes range from 1 to 1.3 inches for basic phones, from 1.4 to 4 inches for feature phones, and from 3 inches to 'phablet' sizes of 7 inches or higher for smartphones.

Display resolutions range from QQVGA (160x120) and QVGA (240x320 pixels) resolution for basic phones, HVGA (320x480 pixels) resolution or less for feature phones, to WVGA (800x480 pixels) or FWVGA (854x480 pixels) resolution for low-end smartphones, and QHD (1440x2560 pixels) resolution or higher for higher-end smartphones.

EXHIBIT 20

Feature Phone and Smartphone Component Shipments, 2015

Display panel shipments (in thousands of units) ■ Feature phone ■ Smartphone

Here, feature phones refer to those with displays of three or more inches. As evidenced in the above chart, feature phones are holding their own, despite earlier projections that smartphone growth would drive out feature phones.[114]

Source David Hsieh, 2016

Technology Fraud and Security

An emerging but relatively under-appreciated trend in MFS is the growing problem of counterfeit phones and components, such as displays and batteries. A closely related problem is the illegal resetting of identifying characteristics of stolen phones to allow for their resale. Unwitting users who buy fake or stolen phones may find that MFS do not work on the devices they have paid for. The effects of fake phones on MFS customers include:

> Inability to receive over-the-air updates from MNOs or service providers to set up the phone with correct mobile network settings

> Performance degradation, including a high percentage of dropped calls, failure to access the network, handover problems and low reliability

> Failed warranty and technical support

> Blocking of the handset by a regulator/industry blacklist, preventing access to MFS-based funds

> Potential hazards such as battery explosions and exposure to high levels of radiation[116]

> Increased incidences of malware, spyware and viruses[117]

EXHIBIT 21

Unique International Mobile Equipment Identity (IMEI) Verification

IMEI
35721582 5023328

OK

IMEI
0000000000000000

OK

At the top, a genuine IMEI number found on a sticker inside a feature phone. Inputting the discovery code ***#06#** will show that the original IMEI number has been replaced with a set of zeros (on the bottom). These changes hide the phone's true identity.[115]

Photo credit Leon Perlman

There are two types of phone technology fraud. First, bad actors can reset a phone's 15-digit unique International Mobile Equipment Identity (IMEI) number—a type of serial number—to a set of zeros or a random 15-digit number.[118] The IMEI is used to check information such as the phone's country of origin, manufacturer and model number. Second, counterfeiters, particularly in Asia, manufacture phones that on the exterior have the look and feel of popular and expensive brands, but do not run the brand's operating system.[119]

The problem is growing: these phones—often called *Shanzhai*, or "bandit" phones—have been estimated to make up 15 to 20 percent of the global market in terms of units sold.[120] The Mobile Manufacturers Forum—a consortium of companies that

make mobile devices—reported that there were almost 150 million counterfeit phones sold globally in 2013.[121] The Organization for Economic Co-operation and Development (OECD) estimated that the total value of internationally traded counterfeit and pirated products has increased significantly: in 2013 it reached a value of US$461 billion, equivalent to the GDP of Austria.[122]

A phone always broadcasts its IMEI number to an MNO when it connects to that network, which is checked and stored in the MNO's Equipment Identity Register (EIR). Knowing the IMEI number allows a MNO to remotely configure the phone with correct network access settings. If an MNO cannot properly identify the phone and model, that customer may not be able to obtain network access and configuration settings generally and for MFS such that the phone may not work properly on that network.

The only way to determine a phone's authenticity is to run an inquiry of the IMEI number through a national or international database of stolen or fake phones, usually administered by the national telecommunications authority or through the GSMA's international IMEI database. For users, the IMEI number is revealed by typing the sequence *#06# on the handset. This number can be provided to the police or insurance companies if the phone is lost or stolen so that it can either be traced or blacklisted. MNOs can block a phone from use on its network if IMEI number is associated with a phone that has been reported lost or stolen or if the IMEI number appears suspicious.[123]

Suspicious IMEI numbers appear because bad actors try to circumvent potential blacklisting of a stolen or lost phone—which effectively makes their bounty unsellable—by using off-the-shelf technology to easily reset the IMEI and replace it with a fake one. Tigo, which has MNO properties in many developing countries, estimates that nearly 10 percent of the device types on its networks are unidentifiable, mostly within Chad (63 percent) and Senegal (15 percent).[124] This is often a game of cat and mouse: MNOs will check their EIR database and oftentimes thousands of phones on their network will have identical 15 digital IMEI numbers, usually indicating the work of

EXHIBIT 22

IMEI Command

Use of the *#06# code to discover a handset's IMEI number

a syndicate operating in a country. If a trend emerges with thousands of these identical IMEI numbers appearing, or if specific IMEI numbers associated with stolen or lost phones are identified, the MNO may then blacklist (prevent use) or graylist (monitor use) these phones depending on their internal policies or instructions from a national authority.

The impact on MFS is this: if a MFS customer's phone is blacklisted without notice, access to stored funds may be cut off. This has happened in a number of countries following instructions from national authorities to MNOs to turn off en masse phones with identical or zeroed IMEI numbers (See Annex B for country examples). When this happens, customers lose the value of their blocked phone, and must then purchase a new phone and place their SIM card in the new phone to re-access their MFS accounts.

Vulnerabilities to Bad Actors

A number of vulnerabilities to bad actors can potentially disrupt systems and cause data and financial loss to MNOs, service providers and their customers.[125] These vulnerabilities occur at both the MNO and customer levels. MNO-level vulnerabilities include Signaling System 7 (SS7)-based and USSD-based exploits and man-in-the-middle attacks using "IMSI catcher" hacking devices. Customer-level vulnerabilities include MFS application tampering and phone number spoofing.

How the Signaling System 7 (SS7) Vulnerabilities Are Made Possible

Most attacks on SS7 are based on designs inherent in modern mobile networks that enable customer mobility (i.e., roaming). To facilitate roaming, a seamless exchange of customer information between MNOs is required, and this is achieved with SS7 messages exchanged between the networks.[126]

However, this means that attackers with SS7 access anywhere in the world can use inter-MNO SS7 communications to send fraudulent SS7 messages that give them access to the core network functions of the attacked MNO, exposing consumer information and facilitating potentially fraudulent financial transactions.

When SS7 was introduced in 1975, it was not designed with security in mind, as the only participants in international SS7 interactions at the time were trusted (mainly state-owned) fixed-line telecommunication operators.[127] It was thought that these trusted operators would not cause or allow security breaches. Use of SS7 by bad actors today are therefore not "hacks" *per se*, but exploitations of SS7's inherent lack of security.

System-wide SS7-derived vulnerabilities at the MNO-level can affect multiple mobile and MFS customers, and individual customers can also be targeted directly, compromising their SIM cards, handsets and MFS accounts. Customers can also introduce vulnerabilities by downloading various apps. Threats can arise from poor app design, resulting in the exposure of customer data, or from apps embedded with malware that is used to extract user data and/ or steal balances. In addition, threats can come from viruses inadvertently downloaded from websites. Similarly, bad actors can emulate a trusted caller ID and call the MFS customer to attempt to extract personal MFS and bank credentials, often resulting in financial loss.

It is difficult to surmise how often such risks will actually be exploited and how much financial harm will result. Nevertheless,

ventilating these risks should provide an impetus toward appropriate planning and risk mitigation. Indeed, there are often ways at both the SS7 and handset levels to mitigate many of these vulnerabilities.

Vulnerabilities in Signaling System 7 (SS7). As noted earlier, SS7 forms the connective tissue of most telecommunication systems, allowing mobile and fixed line networks across the globe to seamlessly interact and, crucially, to allow effortless mobile roaming across MNOs.[128] The need to facilitate roaming however creates vulnerabilities within these networks and affects the core network and base stations at the extremities of the networks. SS7 vulnerabilities can be exploited through Mobile Application Part (MAP), a core mobile phone network interface component that uses SS7 and which powers USSD as one of the primary customer user interfaces for MFS access.

MNOs must allow for the receipt of SS7 messages from external networks when a mobile customer wants to roam and the foreign MNO needs to acquire consent from the home MNO. The constant business need of MNOs to interact with external SS7 networks makes filtering SS7 messages networks difficult, but not impossible.

Many MNOs now use filtering hardware and software to block unnecessary and potentially rogue SS7 requests from external sources. Common characteristics of SS7 attacks include:

> Attacks are based on legitimate SS7 messages, for example, by hijacking requests to allow customers to roam. When networks filter SS7 messages to block intruders, this poses a business revenue risk and may negatively impact the overall quality of service.

> An attacker does not need sophisticated equipment: a Linux-based computer and publicly available software for generating SS7-based packets suffice.

> After an initial attack using SS7 commands, the attacker can execute additional attacks using the same methods.[129]

Intrusion Vulnerabilities and Exploits in MFS and Mobile Networks[130]

Percentage of successful SS7 attacks, as performed by a group of security experts

(Bar chart showing percentages by type of exploit:)
- OBTAINING BALANCE DATA: ~92
- STEALING SUBSCRIBER DATA: ~90
- HIGHJACKING INCOMING SMS: ~89
- TRACKING LOCATIONS: ~58
- EAVESDROPPING ON CONVERSATION: ~50

Y-axis: 0 to 100 (in increments of 10)

TYPE OF SS7 AND/OR USSD EXPLOIT

The percentages indicate the most prevalent types of exploits of SS7 and USSD that have been reported globally via the ITU.

Source Dmitry Kurbatov, 2016

Insofar as it may affect MFS, this SS7-derived vulnerability is a general problem for all USSD-based mobile access systems since bad actors with relatively basic telecommunications skills have the potential to perform intrusive attacks that can lead to customer financial loss, data leakage or disruption of communication services. The majority of intrusions actually perpetrated appear to involve theft of customer login credentials, interception of customer records, and monitoring of customer calls, SMS and data.

Using SS7 requests, a bad actor can also pose as a SMS center—the MNO core network component that acts as a post office for SMS messages—to obtain the international mobile subscriber identity (IMSI) and even location of the target customer.[131] The bad actor can also gain access via SS7 to all SS7 traffic relating to that particular IMSI and can intercept a customer's SMS messages and request the customer's account balance. The attacker can even initiate a transfer of funds from the target MFS customer's account to the attacker's MFS account. While this risk could be mitigated through two-factor authentication via a one-time password (OTP) sent via cleartext SMS in parallel with a USSD-based MFS or banking session, even an OTP intended for a customer under attack may never reach the intended customer, or may be intercepted by an attacker *en route*.[132]

Because of these SS7 vulnerabilities, the U.S. National Institutes of Standards and Technology has recommended that SMS not be used for any authentication purposes for financial transactions. Its recent briefing calls SMS "usable, but regarded as obsolete and best avoided."[133]

MNOs and service providers need to implement risk management frameworks to anticipate, prevent, resolve and mitigate the effect of any intrusions into their systems, and regulators need to revise and update their rules to ensure clarity about roles and responsibilities.

Fake Mobile Base Stations Undertake Man-in-the-Middle Attacks

Bad actors can use fake MNO base stations called "IMSI catchers" (also known as "stingrays") to extract customer data over the air at the edge of a mobile network. The IMSI catcher allows a bad actor to impersonate an MNO, connecting to the customer's handset and capturing all data sent to and from the handset. These relatively easy-to-build devices take advantage of SS7 vulnerabilities and exploit the fact that the GSM A5 encryption technologies designed to keep information safe over GSM networks have largely all been compromised.[134]

In most countries, special permissions are required to import and operate IMSI catchers as they are ostensibly only to be used for law enforcement purposes. In South Africa, for example, the devices fall under a category of equipment designated for national security interests and can only be bought with presidential authorization.[135] Despite these ostensible precautions, commercial IMSI catchers have made their way into the wild. While originally intended for law enforcement, advances in technology now allow anyone to build an IMSI catcher for less than US$1,400. A classic man-in-the-middle-attack can lead to loss of customer data and can compromise an MNO's systems.

There are currently only a few ways to detect the presence and use of IMSI catchers.[136] A number of providers have developed so-called "IMSI catcher catchers" that can determine whether a mobile base station is suspicious.[137] An MNO, regulatory authority or national intelligence network can operate a mobile ICC placed in a surveillance truck. Alternatively, a MNO or telecommunications regulator can utilize a network of stationary measurement units installed on rooftops in a specified geographical area to constantly scan frequency bands for cell announcements and detect any mobile network parameters that arouse suspicion. Another emerging method of detecting fake base stations is to check for signs ("fingerprinting") of IMSI catcher activity at the MNO level.[138]

Unsecure Mobile Applications May Compromise User Funds

MFS applications and user interfaces on feature phones or smartphones are the primary means by which customers interact with the MFS ecosystem.[139] Handsets and applications may however have design deficiencies that attackers can exploit, which may compromise access control and authentication, data confidentiality, privacy and integrity, and service availability.

Some applications are vulnerable due to the lack of PIN authentication prior to sensitive operations, such as checking one's balance or paying bills online. Bad actors can tamper with these transaction details, ultimately calling into question who performed the transaction. Applications that do not support digital signatures cannot provide non-repudiation guarantees when transactions are performed.[140] And incorrect use of key encryption techniques by an application as it communicates with other elements of the MFS

ecosystem can provide an attacker with the means to break weak cryptography and expose sensitive information.[141]

Within applications, lack of access control amongst some applications provides an avenue for bad actors to modify financial data. Application availability is a measure of application design quality and security and if an app does not perform robust input validation, then a bad actor can potentially perform attacks that may crash the application.[142]

Java-based MFS Apps Are More Secure

MFS transaction security can be solidified through the use of small feature phone-based "applets" using the Java programming language. Transaction and maintenance SMS messages are sent via SMS, which are encrypted with unique sets of encryption keys. The applets mostly use bank-grade security, using encryption up to and exceeding Payment Card Industry Data Security Standard.[143]

MNOs and service providers need to implement risk management frameworks to anticipate, prevent, resolve and mitigate the effect of any intrusions into their systems, and regulators need to revise and update their rules to ensure clarity about roles and responsibilities. Specifically, MNOs and service providers should assess the potential for the stealth theft of funds or other financial implications due to external SS7 vulnerabilities, and should deploy hardware and software solutions that can filter rogue SS7 messages. All parties—MNOs, service providers, commercial banks and regulators—should collaborate in assessing and mitigating risks,

especially deploying IMSI catcher catchers and base station fingerprinting to identify fake base stations. Developers should check apps for data leakage and potential for intrusion, and where market conditions allow, Java-based applications should be used more often as they are more intuitive and secure than USSD menus.

One of the most important issues concerns fixed liability when fraud occurs, which providers now usually make consumers accept in their terms of conditions (T&Cs) as a binary precondition for using MFS. The T&Cs usually assign all liability to the consumer, and in case of dispute, may raise the evidential burden of proof that customers need to clear to prove that they were not at fault in relation to loss of their funds. For most MFS customers, and especially in the absence of neutral dispute mechanisms, this is an impossible burden. This usual asymmetry in an MNO or service provider's T&Cs may however be affected and needs to be revised to reflect the fact that since exploits at an infrastructure and local base station level are known to exist, it cannot be taken as a given then that any MFS losses should fasten totally onto the customer.

Since it cannot be proven conclusively at this stage that providers are effectively impenetrable to intrusions that may lead to customer loss, changes to T&Cs should instead reflect the relative responsibilities in cases of technically-caused loss of MFS customer funds. Similarly, any neutral dispute resolution procedures and bodies should take this into account when apportioning blame in case of financial loss in MFS.

6

Competition Aspects of MFS Technology Access and Use

As the MFS ecosystem grows, key market participants—MNOs, non-banks, technical aggregators and switches, agents and banks—may have particular technology-related competition concerns relating to access and pricing for access channel services, interoperability between MFS systems, quality of service and access to big data sets. While these issues may not actually breach national anti-competition laws or regulations, the ultimate effect may be more limited customer access to a growing array of MFS services at attractive prices. In all, the *de facto* curtailing of access and effective use of critical infrastructure degrades global efforts towards the achievement of full financial inclusion.

Access to core MFS facilities, key bearer access channels and payment infrastructure is often shadowed by competition-related issues, due to the fact that access gatekeepers may be controlled by entities that are often in direct competition with the entities seeking access. In particular, even if access is made available to the necessary market participants, the business case for MFS can be made unfeasible because of variable or uneconomical wholesale access costs—a situation often referred to as foreclosure.[144]

For third party service providers relying on MNO communications channels, this gatekeeping or foreclosure often relates to the technical access methods such as for USSD and STK, the primary bearer services used for MFS access. A service provider's inability to secure one or more of these components could render its ability to provide a service using USSD or STK unobtainable or untenable, including an inability to access USSD and STK-based short codes. There may also be quality

of service issues relating to provision of these services, which could negatively impact user perceptions of service providers.

For non-banks seeking to offer MFS, there may be a competition bottleneck involving access to payment infrastructures such as payment switches. Access to the payments infrastructure may also be rendered uneconomical due to discriminatory pricing (e.g., access to automated clearing houses that facilitate interoperable transactions between banks and non-banks or access to the national ATM network).

Thin SIMs

While access to payment infrastructures requires coordination with multiple parties, some market participants are using new methods to circumvent restricted or unfavorable STK and USSD access. Banks and non-banks have used "thin SIMs" (also known as SIM overlay technology or "sticky SIMS") which are paper-thin plastic sheets embedded with a number of sticky contact points and a chip layered on top of a standard SIM card.[145]

Despite their appearance, thin SIMs are full-featured SIMs which, when placed over a larger SIM, convert the handset into a dual-SIM phone, meaning that users can access services on both networks without physically switching the cards.[146] Users can switch between networks either manually through the accompanying menu, or by inputting a specific short code to perform the selection. The thin SIM listens for a specific short code, and if the short code belongs to a network supported by the thin SIM, the traffic will be directed to the alternate network which can provide MFS access at cheaper USSD and

Since feature phones are likely to dominate MFS access for the foreseeable future, regulators should continue developing and maintaining policies on access to USSD and STK gateways at fair, reasonable and non-discriminatory terms.

STK rates. Thin SIMs work with basic phones, feature phones and smartphones. They are also MNO-agnostic, so they can work with any MNO operator independent of the underlying SIM card.[147] Thin SIM technology is now used in a number of countries for MFS, but they are not yet widespread due to the relatively high cost of thin SIMs.[148] For example:

> Kenya's Equity Bank uses thin SIM technology for cheaper bearer services from the MNO Airtel for USSD and SMS access for the customers of its mobile virtual operator subsidiary, Equitel.[149]

> Yes Bank, India's fifth largest private sector bank, launched a thin SIM payments solution for feature phones that installs a STK-based app linked to a prepaid wallet.[150]

> Chinese service provider F-road used thin SIM technology to expand access for over 15 million users from 1,300 banks in 27 provinces.[151]

There is anecdotal evidence to suggest that some regulators have applied regulatory forbearance over universal USSD access and pricing based on the narrative that smartphone apps and 3G/4G technologies will overtake USSD and other narrowband access technologies. However, as emphasized here, feature phones are likely to dominate MFS access for the foreseeable future, using USSD, encrypted SMS and WAP. Regulators should continue developing and maintaining policies on access to USSD and STK gateways at fair, reasonable and non-discriminatory terms.

EXHIBIT 25

Taisys-Manufactured Thin SIM

A thin SIM is placed over the SIM from another MNO. Taisys manufactures thin SIMs for Equitel and all of Equitel's MFS-related STK activity runs over MNO Airtel.[152]

Photo credit Taisys

A

Summary of Mobile Technologies and Their Use in MFS

TECHNOLOGY TYPE	MOBILE TECHNOLOGY GENERATION	MOBILE DATA SPEEDS	PRIMARY PHONES USED	TYPICAL NETWORK COVERAGE	TYPICAL PHONE SCREEN SIZES
GSM, CSD	2G	9.6 kbps	Basic	National	Small
GSM GPRS	2.5G	< 115 kbps	Basic; feature	National	Small; medium
GSM EDGE	2.75G	< 237 kbps	Basic; feature	National	Small; medium
GSM EDGE-Evolution	2.75G+	< 1.6 Mbps	Basic; feature	National	Small; medium
UMTS W-CDMA	3G	< 0.4 Mbps	Smart	Mostly urban, national roads	Large
UMTS HSPA	3.5G	< 14.4 Mbps	Smart	Mostly urban, national roads	Large
HSPA+	3.75G	< 67.2 Mbps	Smart	Mostly urban	Large
LTE	4G	< 300 Mbps	Smart	Mostly urban	Large
LTE Advanced	4G+	< 1000 Mbps	Smart	Mostly urban	Large

GSM—Global System for Communication
CSD—Circuit-Switched Data
GPRS—General Packet Radio Service

EDGE—Enhanced Data Rates
UMTS—Universal Mobile Telecommunications System
W-CDMA—Wideband Code-Division Multiple Access

HSPA—High Speed Packet Access
HSPA+—Evolved High Speed Packet Access
LTE—Long-Term Evolution

Source Leon Perlman, 2012

Summary of Mobile Technologies and Their Use in MFS (continued)

TECHNOLOGY TYPE	RELATIVE USE IN MFS	PRIMARY MFS USER INTERFACE	ACCESS COST	PHONE BATTERY USE	TECHNICAL LITERACY REQUIRED
GSM, CSD	Majority	USSD; STK	$-$$	Low	Low
GSM GPRS	Majority	USSD; STK; WAP; Java	$-$$	Low	Medium
GSM EDGE	Majority	USSD; STK; WAP; Java	$-$$	Low	Medium
GSM EDGE-Evolution	Majority	USSD; STK; WAP; Java	$-$$	Low	Medium
UMTS W-CDMA	Significant	Apps	$$$	High	Medium
UMTS HSPA	Significant	Apps	$$$	High	Medium
HSPA+	Growing significant	Apps	$$$	High	Medium
LTE	Limited	Apps	$$$	Very high	Medium
LTE Advanced	Scarce	Apps	$$$	Very high	Medium

GSM—Global System for Communication
CSD—Circuit-Switched Data
GPRS—General Packet Radio Service

EDGE—Enhanced Data Rates
UMTS—Universal Mobile Telecommunications System
W-CDMA—Wideband Code-Division Multiple Access

HSPA—High Speed Packet Access
HSPA+—Evolved High Speed Packet Access
LTE—Long-Term Evolution

Source Leon Perlman, 2012

Example Market-Level Regulatory and Industry Initiatives to Combat Fraudulent Devices

Asian, Middle Eastern, and African authorities are acting against fake devices and devices with reset IMEI numbers.[153]

Azerbaijan: The Ministry of Communication and Information Technologies has operated its mobile devices registration system based on the IMEI database since 2013, aimed at preventing the use of illegally imported phones, phones with fake IMEI codes and lost or stolen phones. All imported mobile devices must be registered within the first 30 days. Over 13 million devices have been registered.[154]

Bangladesh: The government plans to shut down illegally imported and counterfeit mobile phones following the completion of SIM registration under the new biometric SIM registration system.[155]

Colombia: In 2011, the Ministry of Information and Communication Technologies issued Decree 1630 to control the marketing and sale of new and used devices and create two centralized databases—a registry with the IMEI numbers of devices reported stolen or lost and a registry with a record of IMEI numbers of devices legally imported or manufactured in the country, associated with the ID number of the subscriber.[156]

Egypt: In 2010, the National Telecommunication Regulatory Authority established the Central Equipment Identity Register to curb fake and illegal handsets, combat handset theft and address health and safety. As of December 2014, there were 3.5 million handsets with the fake IMEI code 13579024681122, 250,000 with cloned IMEIs, 500,000 with fake IMEIs, 350,000 with an all-zero IMEI, and 100,000 without proper IMEI codes.[157]

Kenya: In 2011, the Communications Authority (CA) issued a notice to all MNOs to phase out counterfeit handsets on their networks.[158] Some 1.9 million counterfeit mobile phones were phased out after September 30, 2012. A handset verification system was established by the CA to enable subscribers to verify the validity of their phones through submitted IMEI numbers.[159] In early 2017, the CA procured specialized equipment to trace and automatically block *inter alia* counterfeit and stolen phones.[160] The CA will work with the country's Anti-Counterfeit Agency and Kenya Bureau of Standards and the National Police Service to ensure national implementation.[161]

Malaysia: Syndicates selling fake Galaxy Note 5, S7 and Galaxy Tabs have been shut down.[162]

Nepal: The Nepal Telecommunications Authority established a register of IMEI numbers of mobile devices, integrated into MNO databases. It has also blocked unregistered numbers that fail to comply with the new regulations within the mandated timeframe.[163]

Nigeria: The Nigerian Telecommunications Commission indicates that about 250 million fake or reset phones were sold in the country in 2014.[164] Nearly 10 percent of the phones in the country are counterfeit or have been reset.[165] In 2016, the Standards Organisation of Nigeria (SON) began prosecuting individuals who sold fake and substandard mobile phones and accessories. Any phone not registered with the SON will be confiscated and offenders will be prosecuted.[166]

Oman: The Telecommunications Regulatory Authority launched an automated program enabling consumers to identify fake mobile devices. Buyers can send the 15-digit IMEI number on the product's box to the number 80566, and the system will verify if the phone is registered in the GSMA database.[167]
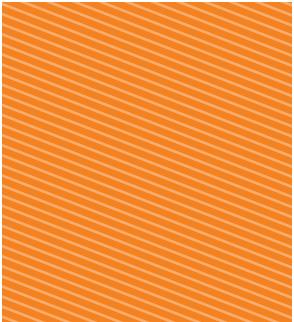
Pakistan: The Pakistan Telecommunication Authority (PTA) implemented a complex procedure for importers to get a no-objection certificate from the PTA to import Chinese-made handsets. This has perversely led to an increase in fake handsets, while decreasing the import of Chinese-made handsets by 40 percent.[168]

Tanzania: As of June 2016, the Tanzania Communication Regulatory Authority reported 630,000 blocked counterfeit phones using a GSMA database of fake IMEI numbers with an estimate of nearly 2 million more to be blocked by the end of the year.[169]
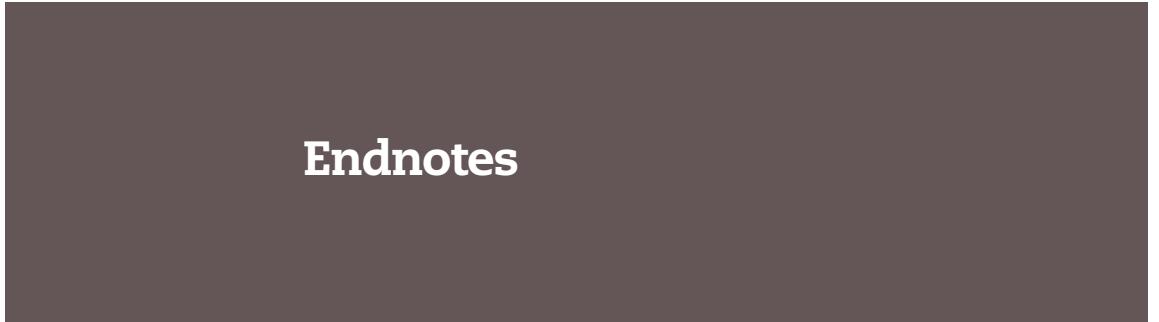
UAE: Dubai police seized over 60,000 counterfeit iPhones, Samsung Galaxy and other phones in a two-week period in 2014. To evade detection, the phones were smuggled into the UAE in pieces before being assembled. Each component is imported separately, even brand stickers.[170] More broadly, authorities have seized a large number of counterfeit mobile phones, mainly fake BlackBerrys.[171]

Uganda: A study by the Uganda Communications Commission has estimated that about 30 percent of Uganda's approximately 17 million mobile phones are Chinese-made counterfeits. The government loses about 15 billion Ugandan shillings (about US$4.1 million) in tax revenue to counterfeit mobile phones.[172]

Supranational initiatives: There are initiatives to create a global system for the exchange of unique telecommunication and ICT device identifiers (in line with the International Telecommunications Union's TDC-14 Resolution 79 and PP-14 Resolution COM 5/4).[173] The GSMA also maintains an international IMEI database which is accessible to network operators, device manufacturers and qualified industry parties.[174]

Endnotes

1 GSM Association (GSMA), *State of the Industry Report on Mobile Money, Decade Edition: 2006–2016 (Executive Summary)*, GSMA, 2017, www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/02/GSMA_Executive_Summary_PRINT-READY-VERSION.pdf.

2 GSM Association (GSMA), *State of the Industry Report on Mobile Money*.

3 Other technologies—such as QR codes, Bluetooth Low Energy, and magnetic secure transmission—were considered, but were found not to be suitable at present for mass use in MFS-focused countries.

4 See GSM Association, "History," www.gsma.com/aboutus/history. See also, Leon Perlman, "Legal and Regulatory Aspects of Mobile Financial Services," 2012; Leon Perlman, "Aspects of Legal and Regulatory Issues in Mobile Financial Services in the Developing World," Proceedings of Mobile Money Conference at the Columbia Institute for Tele-Information, Columbia Business School, November 5, 2010.

5 A bearer service—or just bearer—is a telecommunications term describing a service that allows transmission of information signals between network interfaces. USSD, SMS, and 3G networks can be considered bearer technologies used in mobile financial services.

6 Internet protocol (IP) is the principal communications protocol in the Internet protocol suite for relaying data. IP delivers packets from the source host to the destination host solely based on the IP addresses in the packet headers.

7 High speed packet access (HSPA) is an amalgamation of two mobile protocols—high speed downlink packet access (HSDPA) and high speed uplink packet access (HSUPA)—that extends and improves the performance of 3G mobile networks utilizing the WCDMA protocols. A further improved 3rd Generation Partnership Project (3GPP) standard—evolved high speed packet access (also known as HSPA+)—was released late in 2008, with worldwide adoption beginning in 2010.

8 LTE is based in part on UMTS/HSPA network technologies. It increases the capacity and speed over UMTS/HSPA by using a different radio interface together with core network improvements. LTE was developed by the 3GPP and is specified in its Release 8 document series.

9 STK allows MNOs and others to store easily-discoverable menus on SIM cards as the user interface for MFS access.

10 IVR technology allows a computer to interact with humans through the use of voice and DTMF tones input via keypad.

11 On the effects of technical literacy on MFS use, see Grameen Foundation, *Use of Mobile Financial Services Among Poor Women in Rural India and the Philippines*, 2013, www.gsma.com/mobilefordevelopment/wp-content/uploads/2014/07/Use-of-Mobile-Financial-Services-Among-Poor-Women-in-Rural-India-and-the-Philippines.pdf.

12 Feature phones include most of the features of basic phones, augmented by features such as Bluetooth, MMS, WAP capabilities, and in some cases 3G capabilities.

13 Depending on the context and jurisdiction, a service provider could be a third party provider such as a bank, a non-bank entity, a MFI, or a MNO.

14 Cleartext means that the SMS data is unencrypted when transferred. SMSs using STK and Java technologies are encrypted.

15 Contactless payment systems are credit cards and debit cards, key fobs, smart cards, or other devices, including smartphones and other mobile devices that use radio frequency identification or NFC technology for making payments. Bluetooth is another emerging proximity communications method, but does not yet have significant use in MFS.

16 "Pound" is also known as "hash" in some markets.

17 USSD is now in version 2 (v2). USSD version 1 (v1)—which is no longer in primary use, but still supported by MNOs—has limited features compared to v2, although handsets first issued in the 1990s that use USSD v1 only have long since been discontinued or have reached their useable lifespan, and are unlikely to be used. Supplementary (or 'quick') codes using USSD allow users to undertake basic programming of their MNO services and features, for example, allowing them to forward a call to a number and toggle Caller Line ID (CLI) e.g., # 31 #.

18 Trevor Perrier, Brian DeRenzi, and Richard Anderson, "USSD: The Third Universal App," Proceedings of the 2015 ACM Symposium on Computing and Development (ACM DEV 2015), 2015, http://bderenzi.com/Papers/perrier-dev2015.pdf.

19 This means that calculations for transaction costs can be dynamically generated per transaction—for example, as a percentage of revenue. Other methods such as STK or Java applets, which are store-and-forward technologies, may not necessarily have those capabilities built in.

20 Grameen Foundation, *Use of Mobile Financial Services*.

21 USSD may sometimes be the secondary authentication mechanism in MFS. In some cases, the primary authentication mechanism will be through an over-the-top (OTT) smartphone application, using encrypted STK or cleartext (unencrypted) SMS-based access to a server, with network-initiated (push) USSD serving as the second-factor authenticator; this requires the user to input the answer to a challenge question whose answer only they would know.

22 These commands are standard for all mobile equipment and defined by the European Telecommunications Standards Institute and 3GPP specifications.

23 This is a simple machine code that converts the raw messages from the software to application-level message. This requires a special STK gateway at the MNO.

24 STK as a technology can use USSD as a bearer, but some handset manufacturers have not adequately implemented STK support for USSD. In practice, STK will almost always use SMS as a bearer.

25 Many new smartphones do not have the STK 'translator' installed, meaning that services using STK-based menu items will not appear. This may impact those using remote airtime transfer as a form of foreign remittance. For example, see the NoSTK Android smartphone app, which caters to smartphones lacking STK functionality (https://play.google.com/store/apps/details?id=appinventor.ai_tborja.NO_STK).

26 Photo credit: Information and Communications for Development (IC4D) Blog, http://blogs.worldbank.org/ic4d/mobile-services-game-changer-greater-good.

27 Photo credit: Afternoon Dispatch and Courier, http://afternoondc.in/userfiles/13-9-11-SBI-MOBILE-BANKING-POSTER---Eng.jpg.

28 Except if using a WAP link for application download, which requires mobile data.

29 This method is similar in principle to a smartphone app, but it runs on a less sophisticated type of handset operating system. The minimum feature phone requirement for Java applications is Mobile Information Device Profile 2.0 and Connected Limited Device Configuration 1.1 specification, 1 MB of RAM memory, and 600 kb of phone storage. Many feature phones will have sufficient storage for this. MIDP is a specification published for the use of Java on embedded devices such as mobile phones and PDAs. CLDC is a set of standards, libraries, and virtual-machine features that serve as the basis for APIs targeted at devices with very limited resources. A large number of feature phones, as well as some embedded systems, fall under this category of device. See Techopedia, "Connected Limited Device Configuration (CLDC)," *Techopedia*, www.techopedia.com/definition/3340/connected-limited-device-configuration-cldc-java.

30 As with the sideloading installation method, on installation and on use, the application on the handset will undertake internal 'fingerprinting,' a self-check to ensure that the application has not been tampered with and is not 'leaking' data to fraudsters. A similar fingerprinting confirmation is done with the server on every transaction.

31 Zero-rating of the data cost of an application download and/or its use on a mobile network is an emerging trend worldwide. The small data cost can be reverse-billed, so that the MFS service provider is charged by the MNO for the data required for the customer's download. See Anne Morris, "Report: 45% of operators now offer at least one zero-rated app," *FierceWireless*, July 15, 2014, www.fiercewireless.com/europe/story/report-45-operators-now-offer-least-one-zero-rated-app/2014-07-15.

32 For example, a biller can be added to the applet menu by sending just one encrypted SMS to the handset instead of multiple SMSs to update the entire applet.

33 Except if using a WAP link for application download, which requires data.

34 Of course, this locks the service provider using the acoustic technology into the vendor platform. NSDT is the trade name for the acoustic access service offered by Tagpay. For more information, visit www.tagpay.fr.

35 Cong Wang, et al., "PriWhisper: Enabling Keyless Secure Acoustic Communication for Smartphones," *IEEE Internet of Things Journal*, 2013, https://eprint.iacr.org/2013/581.pdf.

36 Rian Boden, "Ultracash launches sound-based mobile payment service in Bangalore," *NFC World*, October 13, 2015, www.nfcworld.com/2015/10/13/338639/ultracash-launches-sound-based-mobile-payment-service-in-bangalore/.

37 The underlying concept of universal service is to ensure that telecommunications services are accessible to the widest number of people (and communities) at affordable prices. For global universal service obligations, see International Telecommunications Union (ITU), *Universal Service Fund and Digital Inclusion for All Study*, June 2013, www.itu.int/en/ITU-D/Conferences/GSR/Documents/ITU%20USF%20Final%20Report.pdf.

38 Cartesian, "Mobile Platform Access for USSD-based Applications (MPA-USSD) (Market Assessment)," January 30, 2015, www.ucc.co.ug/files/downloads/SMP_Report_Mobile_Platform_Access_USSD_April%202015.pdf.

39 3G will refer to representative coverage providing broadband speeds, including (but not technically) HSPA and 4G LTE. See Annex A for mobile phone technologies.

40 Ubiquitous 3G and/or 4G coverage in the developed world is of course also not a given.

41 Smartphone coverage is usually associated with urban areas, where there may be more disposable income for the purchase of smartphones and affordability for data plans.

42 Although 900 and 2100 MHz are the plurality of GSM-based system frequency use, they differ in North America and parts of Latin America and the Caribbean.

43 Facebook, *State of Connectivity*, 2016.

44 Again, this coverage may be limited if spectrum costs are too high. Spectrum frequencies may be allocated through a so-called 'beauty contest,' or through a spectrum auction facilitated by the government and/or national regulator.

45 Regulators around the world are beginning to auction off or sell the released former analog TV frequencies, including the 700 MHz, 800 MHz, and 2,600 MHz ranges. South Africa is auctioning off the 700 MHz, 800 MHz and 2,600 MHz spectra. See Natasha Odendaal, "Icasa opens auction for long-awaited spectrum," *Engineering News*, July 15, 2016, www.engineeringnews.co.za/article/icasa-opens-auction-for-long-awaited-spectrum-2016-07-15. In India, the regulator tried to auction off the 700 MHz spectrum, but had no bidders because the reserve price was considered too high. See Sunil Jain, "Trai's arbitrary, and inexplicable, pricing to blame for failure of 700MHz auction," *The Financial Express*, October 3, 2016, www.financialexpress.com/economy/trais-arbitrary-and-inexplicable-pricing-to-blame-for-failure-of-700mhz-auction/403649/. Similar auctions are also taking place in East Africa.

46 Some markets already have phones compatible with the 450 MHz frequency spectrum. The 450 MHz frequency band is being used by some 115 operators in 60 countries, primarily in Latin America and the Caribbean and with CDMA networks. See Steve Costello, "LTE 450 MHz: taking the road less travelled," *Mobile World Live*, April 27, 2015, www.mobileworldlive.com/featured-content/home-banner/lte-450mhz-taking-road-less-travelled.

47 Again, this coverage may be limited if spectrum costs are too high. Spectrum frequencies may be allocated through a beauty contest, or through a spectrum auction facilitated by the government and/or national regulator. In some circumstances, the new LTE-U specification may assist in augmenting LTE 4G coverage.

48 For example, the National Payments Corporation of India has planned for feature phones and USSD to be the primary access mechanisms to MFS. See Chaitanya Gudipaty, "Move to cashless society to be driven by feature phones: Hota," *Moneycontrol.com*, December 4, 2016, www.moneycontrol.com/news/economy/move-to-cashless-society-to-be-driven-by-feature-phones-hota_8056361.html.

49 Gu Zhang, "From feature phones to smartphones, the road ahead," *GSMA Intelligence*, July 30, 2015, www.gsmaintelligence.com/research/2015/01/from-feature-phones-to-smartphones-the-road-ahead/456/. Similarly, in Africa, nearly 70 percent of identified users use feature phones (Millicom, in discussion with the author, 2015).

50 The basic or low-end appellation is a throwback to the early days of the emergence of GSM mobile technology, where only basic functionality—such as call functions, SMS, USSD version 1 functionality, and a phonebook—were needed (and available) to communicate. Some basic devices though could receive value added services such as ringtones via over-the-air installation.

51 The Hindu Business Line, "Feature phones may see price rise on supply concerns," *The Hindu Business Line*, July 3, 2016, www.thehindubusinessline.com/info-tech/feature-phones-may-see-price-rise-on-supply-concerns/article8803900.ece; Chaitanya Gudipaty, "Move to cashless society."

52 Gu Zhang, "From feature phones to smartphones."

53 See Jacob Poushter, "Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies," *Pew Research Center*, February 22, 2016, www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/.

54 That is, devices have two SIM card slots.

55 In Sub-Saharan Africa and the Middle East: Tecno, Itel, Mi-Phone, Torque, Gionee, Prestigio, Xiaomi, Viettel. Hisense, AG; in Asia: Torque, Gionee, Viettel. Hisense, Symphony, Prestigio, Micromax, Yezz, Oneplus, Plum, TC, Oppo, Vivo, Meizu, Doogee; in Latin America and the Caribbean: Blu, Xiaomi, Prestigio, Doogee, Maxwest.

56 It has been estimated that there are over 250,000 active patents involved in the manufacture of a single smartphone. Mike Masnick, "There are 250,000 Active Patents that Impact Smartphones," *Techdirt*, October 18, 2012, www.techdirt.com/blog/innovation/articles/20121017/10480520734/there-are-250000-active-patents-that-impact-smartphones-representing-one-six-active-patents-today.shtml. In addition, as many standards-essential patents are required to have fair, reasonable and non-discriminatory licensing, there is an arms race to license and purchase evolving smartphone technology patents. See Juro Osawa, "China Smartphone Makers Snap Up Patents in Fight for Market Dominance," *Wall Street Journal*, June 20, 2016, www.wsj.com/articles/china-smartphone-makers-enlisting-patents-in-fight-for-market-dominance-1466428889.

57 For example, Nokia, Siemens, BlackBerry, NEC, Haier, Alcatel, Sagem, Samsung, LG, and Sony-Ericsson. Many of these brands still exist to some extent, but usually only through the licensing of the brand names by Asian mobile phone manufacturers. Alcatel, for example, is manufactured by TCL.

58 See Statista, "Smartphone shipments' share worldwide by vendor from 1Q'15 to 4Q'16," *Statista*, 2017, www.statista.com/statistics/632249/global-smartphone-market-share-by-vendor/. See also Tim Green, "10 Chinese Phone Makers Transforming the Industry," *Hot Topics*, 2015, www.hottopics.ht/stories/consumer/10-chinese-phone-makers-to-your-pocket/.

59 Darryl Linington, "Smartphone adoption is accelerating as device costs decline in Africa," *IT News Africa*, October 8, 2015, www.itnewsafrica.com/2015/10/smartphone-adoption-is-accelerating-as-device-costs-decline-in-africa/; GSM Association (GSMA), "History."

60 The promise, however, of carrier subsidies for devices, increased 3G coverage as part of universal service obligations of MNOs, and lower data costs. Prices for smartphones (and other phone types) and access may, however, be affected by the increased tendency by some regulators to tax mobile phone imports and mobile phone airtime.

61 Photo credit: Leon Perlman.

62 Random access memory is not used for data storage but for running applications. The more RAM available on a device, the more space there is to process applications, and therefore, the applications run much faster and smoother.

63 Gu Zhang, "From Feature Phones to Smartphones."

64 This time frame may differ from market to market, but within Sub-Saharan Africa, the Indian subcontinent, and Latin America and the Caribbean, USSD is likely to dominate until at least 2020.

65 See also, Gu Zhang, "From feature phones to smartphones."

66 Near Field Communication is a contactless payment and access technology available in many higher-end smartphones. Basic and feature phone use is possible with NFC 'stickers.'

67 Ian Fuller, *Nokia Mobile Phone*, Flickr, December, 30, 2005, https://flic.kr/p/83eiD.

68 IndIa7 Network, *Nokia 220*, Flickr, April 24, 2014, https://flic.kr/p/ngYWnd.

69 That is, these devices have two SIM card slots.

70 These are usually standalone applications that do not necessarily integrate with other features of the phone.

71 J2ME (Java 2 Platform, Micro Edition) is a technology developed by Oracle that allows programmers to use the Java programming language and related tools to develop programs for mobile wireless information devices, such as basic and feature phones.

72 MRE is implemented by SOC manufacturer Mediatek.

73 Gu Zhang, "From feature phones to smartphones;" Linda Sui, "Android Captures Record 88 Percent Share of Global Smartphone Shipments in Q3 2016," *Strategy Analytics*, November 2, 2016, www.strategyanalytics.com/strategy-analytics/news/strategy-analytics-press-releases/strategy-analytics-press-release/2016/11/02/strategy-analytics-android-captures-record-88-percent-share-of-global-smartphone-shipments-in-q3-2016#.WLmhNfkrJAm.

74 Author *in situ* research in Bangladesh, Colombia, El Salvador; India, Indonesia, Jordan, Malawi, South Africa, Uganda, and Tanzania; see also Ebay.com.in, Amazon.com, and Alibaba.com. Retail prices vary because of local taxes and import tariffs imposed by authorities.

75 Net neutrality relates to the non-restrictive and identical access pricing and parameters to third party over-the-top (OTT) apps by telecommunications providers, usually over IP-based networks.

76 The percentage of smartphones using Windows Mobile, iOS, BlackBerry, Tizen, and Firefox is far less than Android. Google, which owns Android OS, does not charge a licensing fee for its Android OS, but there reportedly may be other costs to manufacturers for using components of Google's software portfolio or for testing this software. See Charles Arthur and Samuel Gibbs, "The Hidden Costs of Building an Android Device," *The Guardian*, January 23, 2014, www.theguardian.com/technology/2014/jan/23/how-google-controls-androids-open-source.

77 For an excellent overview of design principles for smartphone user interfaces (UIs) that engage customers while also reducing required bandwidth for executing MFS transactions, see Gregory Chen, Alexandra Fiorillo, and Michele Hanouch, "Smartphones & Mobile Money: Principles for UI/UX Design (1.0)," *CGAP*, October 5, 2016, www.slideshare.net/CGAP/smartphones-mobile-money-principles-for-uiux-design-10.

78 Grameen Foundation, *Use of Mobile Financial Services*.

79 See Gregory Chen, Alexandra Fiorillo, and Michele Hanouch, "Smartphones & Mobile Money."

80 Ann Armstrong, Joseph J. Mueller, and Timothy D. Syrett, "The Smartphone Royalty Stack: Surveying Royalty Demands for the Components Within Modern Smartphones," 2014, www.wilmerhale.com/uploadedFiles/Shared_Content/Editorial/Publications/Documents/The-Smartphone-Royalty-Stack-Armstrong-Mueller-Syrett.pdf.

81 See Keith Mallinson, "Cumulative Mobile-SEP Royalty Payments no More than Around 5% of Mobile Handset Revenues," *IP finance*, August 19, 2015, www.ip.finance/2015/08/cumulative-mobile-sep-royalty-payments.html.

82 3G handsets invariably also require higher-capacity batteries, and larger and more power-hungry touch screen displays, another incremental cost.

83 See Android Developers, "Backwards Compatibility," 2016, https://developer.android.com/design/patterns/compatibility.html.

84 An image of the operating system is usually factory-installed on the smartphone.

85 Photo credit: Leon Perlman.

86 Bonnie Cha, "Smartphones Unlocked: Understanding processors," *CNET*, August 8, 2011, www.cnet.com/news/smartphones-unlocked-understanding-processors/.

87 Chris Smith, "How it Works: Systems on a Chip (SoC)," *Android Authority*, June 8, 2012, www.androidauthority.com/how-it-works-systems-on-a-chip-soc-93587/.

88 Mediatek is now Qualcomm's largest competitor in smartphone SOCs. As of November 2014, over 1,500 mobile models accounting for 700 million units were shipped globally in 2014, using MediaTek chips. See Tim Green, "Mediatek: cheap, super fast processors will change the smartphone market forever," *Hot Topics*, 2014, www.hottopics.ht/stories/consumer/get-ready-for-super-mid-market-smartphone-revolution/.

89 Analysis of Samsung Galaxy Smartphone production costs. Data derived from Scott Adam Gordon, "Guess how Much." Cost breakdown may be different for non-marquee brands, but are relatively the same in proportion.

90 Linda Sui, "Android Captures Record."

91 Most processors, though, are based on reference designs from Advanced RISC Machines (ARM). The new Mediatek MT6595 chip, for example, is based on the ARM 'big.LITTLE' architecture, with four high-performance Cortex-A17 and four energy efficient Cortex-A7 processors. An ARM processor is one of a family of CPUs based on the RISC (reduced instruction set computer) architecture developed by Advanced RISC Machines. RISC processors are designed to perform a smaller number of types of computer instructions so that they can operate at a higher speed, performing millions of instructions per second. See Margaret Rouse, "ARM processor," *WhatIs.com*, January 2015, http://whatis.techtarget.com/definition/ARM-processor.

92 The only dual core feature phone currently on the market is the Samsung Xcover B550H. Also, The MediaTek MT6595 SOC, for example, includes four high-performance and four energy efficient processors, LTE radios with worldwide frequencies compatibility, and a 2560 x 1600 (WQXGA) display controller and a 20-megapixel image signal-processor for high-quality smartphone digital camera applications, alongside WiFi, BLE and GPS.

93 Scott Adam Gordon, "Guess how Much it really Costs to make a Smartphone," *Android Pit*, February 20, 2015, www.androidpit.com/how-much-does-it-cost-to-make-a-smartphone.

94 This includes Mediatek's Feature Phone Runtime Environment (MRE), which allows third party apps to be installed on compatible devices. Also, Nokia Series 30+ is a feature phone operating system from MediaTek that has been used in Nokia-branded mobile devices. It, however, is not the same the older Nokia S30 or S40 platforms. S30+ does not support J2ME applications. It can use built-in applications such as the Opera Mini browser, Bing Search and Skype-like chat.

95 Spreadtrum's WRE (Windows Runtime Environment) is a middleware platform for mid-tier devices like feature phones. See Justin Springham, "Spreadtrum and Sohu.com partner for feature phone app store," *Mobile World Live*, November 4, 2011, www.mobileworldlive.com/apps/news-apps/spreadtrum-and-sohucom-partner-for-feature-phone-app-store/.

96 In June 2016, Microsoft sold the series as part of its feature phone sale to HMD Global, after which HMD discontinued the series. See BBC News, "Microsoft sells Nokia feature phones business," May 18, 2016, www.bbc.com/news/technology-36320329. Taiwanese firm Foxconn is taking ownership of a Microsoft feature phone factory in Hanoi, while Nokia has licensed the brand to another Finnish firm started by former employees.

97 It will also discontinue support for BlackBerry, Windows Phone 7.1, iPhone 3GS/iOS 6, Android 2.1 and Android 2.2. WhatsApp, "WhatsApp support for mobile devices," 2016, https://blog.whatsapp.com/10000617/WhatsApp-support-for-mobile-devices.

98 Deccan Chronicle, "WhatsApp will stop working on many phones end of 2016; which one do you have" *Deccan Chronicle*, July 14, 2016, www.deccanchronicle.com/technology/mobiles-and-tabs/140716/whatsapp-will-stop-working-on-many-phones-end-of-2016-which-one-do-you-have.html.

99 There are variants to Android, such as MIUI (Mi User Interface) from Chinese mobile phone manufacturer Xiaomi. In addition, from 2015, most BlackBerry devices use the Android operating system. The last BlackBerry OS-based device is the BlackBerry Classic, released in early 2015. It should also be noted that Tizen is a Linux-based operating system. Most of Tizen-based smartphones are manufactured by Samsung, for example, the Samsung Z1, Z2 and the Z3. In addition, the operating system is an evolved continuation of the Linux MeeGo operating system previously developed by alliance of Nokia and Intel, which itself relies on Maemo. See https://sailfishos.org/.

100 This is most often dynamic random access memory (DRAM). The flash memory can either be a removable Secure Digital (SD) memory card or an integrated component of the device.

101 Evan Dashevsky, "Why Cell Phone Batteries Sometimes Explode (And How to Avoid It)," *PC Magazine*, September 17, 2015, www.pcmag.com/article2/0,2817,2491375,00.asp.

102 Neil J. Rubenking, "Counterfeit Phones are Full of Surprising Dangers," *PC Magazine*, October 24, 2015, http://au.pcmag.com/software/39360/feature/counterfeit-phones-are-full-of-surprising-dangers; GSM Association (GSMA), "Beware of sub-standard mobile phone batteries and chargers," 2013, www.gsma.com/publicpolicy/beware-of-sub-standard-mobile-phone-batteries-and-chargers; Jeremy Blum, "'Fake' iPhone charger cited in electrocution death probe," *South China Morning Post*, June 16, 2013, www.scmp.com/news/china/article/1283818/woman-electrocuted-while-answering-iphone-may-have-been-using-fake. However, even the Samsung S7 Galaxy Note 7 battery has been known to explode, leading to a massive worldwide recall and discontinuation of the model. See Australian Broadcasting Company (ABC), "Samsung recalls Galaxy Note7 smartphones after exploding battery reports," *ABC*, September 5, 2016, www.abc.net.au/news/2016-09-06/samsung-recalls-galaxy-note7-smartphones-over-explosion-risk/7817674.

103 Higher capacity is clearly better, but given current battery technologies, may increase the phone's size.

104 This ability to change the technology access method is usually through an accessible setting in the phone's menu.

105 See, for example, a report on technical literacy in India and the Philippines, detailing why many users do not use non-voice services on handsets: Grameen Foundation, *Use of Mobile Financial Services*.

106 See generally, David Nield, "Gadget tech explained: AMOLED vs. IPS displays," *New Atlas*, September 1, 2015, http://newatlas.com/amoled-vs-ips-display-technology/39196/.

107 There are also older nickel metal hydride batteries, replacing NiCad types. They do not hold as much charge as and are not as light as lithium-based batteries, and suffer from memory effect. They are seldom found in newer phone generations.

108 They are not prone to a battery chemistry artefact known as 'memory effect,' which simply means that the battery will not lose capacity if it isn't completely discharged when used. However, they tend to be more flammable and prone to internal short-circuits, overcharging, or other malfunctions that can result in fires or explosive release of gases. Battery University, "Is Lithium-ion the Ideal Battery?," *Battery University*, http://batteryuniversity.com/learn/archive/is_lithium_ion_the_ideal_battery.

109 See further, Rasmus Larsen, "Touch technology in smartphones explained," *FlatpanelsHD*, September 19, 2012, www.flatpanelshd.com/focus.php?subaction=showfull&id=1348049303.

110 Gu Zhang, "From Feature Phones to Smartphones."

111 There is now also super LCD used in some smartphone displays. Super LCD differs from a regular LCD in that it does not have an air gap between the outer glass and the display element, which produces less glare, lower power consumption, and improved outdoor visibility. Some manufactures are using SLCD because of the expense and lack of production capacity of AMOLED displays. Super LCD has been succeeded by the newer super LCD2 displays. See MobileBurn, What is "Super LCD"?," *MobileBurn.com*, www.mobileburn.com/definition.jsp?term=S-LCD. See further, Liane Cassavoy, "What is TFT-LCD? Definition of TFT-LCD," *Lifewire*, October 31, 2016, http://cellphones.about.com/od/phoneglossary/g/What-Is-Tft-Lcd.htm.

112 Liane Cassavoy, "What is an IPS-LCD? Definition of IPS-LCD," *Lifewire*, October 31, 2016, http://cellphones.about.com/od/phoneglossary/g/What-Is-An-Ips-Lcd.htm.

113 There are variants many of AMOLED, usually named by the manufacturer. For example, there is active matrix versus passive matrix AMOLED. With passive AMOLED, a complex grid system is used to control individual pixels, where integrated circuits control a charge sent down each column or row. Super AMOLED is a term for an AMOLED display with an integrated digitizer: the layer that detects touch is integrated into the screen, rather than overlaid on top of it. This makes the screen lighter and thinner. See also OLED-Info, "Super AMOLED: Introduction and Basics," *OLED-Info*, www.oled-info.com/super-amoled.

114 Gu Zhang, "From feature phones to smartphones;" David Hsieh, "Low-End Smartphone and Feature Phone Display Shortage Driving Up Prices and Shipments," *IHS Markit*, February 3, 2016, http://blog.ihs.com/low-end-smartphone-and-feature-phone-display-shortage-driving-up-price-and-shipments.

115 Photo credit: Leon Perlman.

116 Radiation output is measured as specific absorption rates. Lower rates are better.

117 Catalin Cimpanu, "24 Chinese Android Smartphone Models Come with Pre-Installed Malware," *Softpedia*, September 4, 2015, http://news.softpedia.com/news/24-chinese-android-smartphones-models-come-with-pre-installed-malware-490930.shtml#ixzz4KAgwE0WC.

118 The IMEI code style must correspond to the code specified by the GSMA document DG06 (TW.06)–IMEI Allocation and Approval Guidelines. See GSM Association (GSMA), "IMEI Allocation and Approval Guidelines," *GSMA*, July 29, 2011, www.gsma.com/newsroom/wp-content/uploads/2012/06/TS.06-v6.0.pdf.

119 In Bangladesh, for example, a popular fraud is to encase a fake BlackBerry with an original BlackBerry casing. For further understanding on counterfeit phones see Mobile Manufacturers Forum (MMF), "Counterfeit and Substandard Mobile Phones: A Resource Guide for Governments," www.itu.int/en/ITU-T/C-I/Documents/WSHP_counterfeit/Contributions/Contribution-001-MMF.pdf.

120 Jeremy Millard, et al., *Study on internationalisation and fragmentation of value chains and security of supply*, European Commission, February 17, 2012, http://ec.europa.eu/DocsRoom/documents/393/attachments/1/translations/en/renditions/pdf.

121 Neil J. Rubenking, "Counterfeit Phones."

122 OECD/EUIPO, *Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact*, OECD, April 18, 2016, www.oecd.org/gov/risk/trade-in-counterfeit-and-pirated-goods-9789264252653-en.htm.

123 The model is specified in the IMEI number through a type allocation code (TAC), the initial eight-digit portion of the 15-digit IMEI codes used to uniquely identify phones. The TAC identifies a particular model (and often revision) of the handset. If the TAC does not correspond to the code for a specific model, then the MNO or service provider cannot determine what type of handset is being used, it may not be able to send the correct over-the-air configuration and/or update settings to the handset. It's also worth noting that with blacklisting, the MNO will block a phone on its stolen phone database from being able to operate on its network. With gray listing, the MNO will monitor the use of the phone, with a view to catching the holder of the stolen phone.

124 Data supplied by Tigo. This lacuna is largely due to the fake/reset IMEI numbers that prevent proper identification of the device characteristics.

125 For more on security aspects of mobile networks and MFS and the risks therein, see Leon Perlman, "Legal and Regulatory Aspects."

126 The ability to send SS7 messages is called global title, which is usually the purview of fixed line and mobile telecommunications licensees. However, many licensees allow third parties to use their global title, for example, to send bulk SMSs via a MNO's SMS center.

127 See Larry Loeb, "SS7 Vulnerability Isn't a Flaw–It Was Designed That Way," *SecurityIntelligence*, April 16, 2016, https://securityintelligence.com/ss7-vulnerability-isnt-a-flaw-it-was-designed-that-way/.

128 Data based on Leon Perlman, "Legal and Regulatory Aspects."

129 See further, Dmitry Kurbatov, "Statistics of Vulnerabilities in SS7 Networks and Ways to Make Them Secure," Proceedings of the ITU Workshop of "SS7 Security," *International Telecommunications Union (ITU)*, June 29, 2016, www.itu.int/en/ITU-T/Workshops-and-Seminars/201606/Documents/Abstracts_and_Presentations/S2P2_Dmitry_Kurbatov.pdf.

130 Dmitry Kurbatov, "Statistics of Vulnerabilities."

131 An IMSI is the serial number of the subscriber SIM card. The IMSI is sent as rarely as possible, to avoid it being identified and tracked. Instead, the temporary mobile subscriber identity is the identity that is most commonly sent between the mobile phone and the MNO, and is randomly assigned. An attacker, for example, would send a specific 'update location' request message directly to the customer's MNO via SS7. See Cellusys, *SS7 Vulnerabilities*, 2016, www.cellusys.com/thank-you/ss7-vulnerabilities/?source=Ibn.

132 See, for example, the massive breach of the supposedly secure instant messaging application, Telegram, by hackers. Vulnerability in Telegram's and other apps using one-time passwords via SMS lies in their use of one-time passwords via cleartext SMS text messages to activate new devices. When users want to log on to Telegram from a new phone, the company sends them authorization codes via SMS, which can be intercepted. With these codes hackers can add new devices to a person's account, enabling them to read chat histories as well as new messages. See Joseph Menn and Yeganeh Torbati, "Exclusive: Hackers accessed Telegram messaging accounts in Iran," *Reuters*, August 2, 2016, www.reuters.com/article/us-iran-cyber-telegram-exclusive-idUSKCN10D1AM. For more data on interception of messages by an attacker, see Tobias Engel, *SS7: Locate. Track. Manipulate*, 2014, http://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf.

133 See Paul A. Grassi, et al., *NIST Special Publication 800–63B Digital Identity Guidelines: Authentication and Lifecycle Management (Draft)*, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, https://pages.nist.gov/800-63-3/sp800-63b.html.

134 Jaikumar Vijayan, "Researchers use PC to crack encryption for next-gen GSM networks," *Computerworld*, January 14, 2010, www.computerworld.com/article/2522701/security0/researchers-use-pc-to-crack-encryption-for-next-gen-gsm-networks.html.

135 Shaun Swingler, "Meet The Grabber: How government and criminals can spy on you (and how to protect yourself)," *Daily Maverick*, September 1, 2016, www.dailymaverick.co.za/article/2016-09-01-meet-the-grabber-how-government-and-criminals-can-spy-on-you-and-how-to-protect-yourself/.

136 See Leon Perlman (ITU-T Focus Group on Digital Financial Services), *Competition Aspects of Digital Financial Services (Focus Group Technical Report)*, International Telecommunications Union (ITU), March 2017, www.itu.int/en/ITU-T/focusgroups/dfs/Documents/201703/ITU_FGDFS_Report-Competition-Aspects-of-DFS.pdf.

137 Dabrowski, et al., "IMSI-Catch Me If You Can: IMSI-Catcher-Catchers," Proceedings of the 2014 Annual Computer Security Applications Conference (ACSAC), www.sba-research.org/wp-content/uploads/publications/DabrowskiEtAl-IMSI-Catcher-Catcher-ACSAC2014.pdf.

138 See Kevin Butler, et al. (ITU-T Focus Group on Digital Financial Services), *Security Aspects of Digital Financial Services (DFS) (Focus Group Technical Report)*, International Telecommunications Union (ITU), January 2017, www.itu.int/en/ITU-T/studygroups/2017-2020/09/Documents/ITU_FGDFS_SecurityReport.pdf.

139 See also Lynn M. Batten, Veelasha Moonsamy, and Moutaz Alazab, "Smartphone Applications, Malware and Data Theft," *Computational Intelligence, Cyber Security and Computational Models*, December 19, 2015, https://link.springer.com/chapter/10.1007/978-981-10-0251-9_2.

140 A study of smartphone-based systems found that some applications are vulnerable due to the lack of PIN authentication prior to performing sensitive operations such as acquiring financial balance information or paying bills. On mobile banking, mobile money, and mobile payment app security, see Kyle Butler, et al., "Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World," Proceedings of the USENIX Security Symposium (SECURITY), 2015, www.cise.ufl.edu/~traynor/papers/reaves-usenix15a.pdf.

141 The GSM encryption is known to be vulnerable to attack. See GSM Association (GSMA), "Security Algorithms," *GSMA*, www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/security-algorithms.

142 Kyle Butler, et al., "Mo(bile) Money;" Kevin Butler, et al. (ITU-T Focus Group on Digital Financial Services), "Security Aspects of Digital Financial Services (DFS) (Focus Group Technical Report)."

143 Payment card industry data security standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover and JCB.

144 This could be the result, for example, of the abuse of a market participant who has what is termed significant market power. The OECD says an MNO is presumed to have significant market power if it has more than 25 percent of a telecommunications market in the geographic area in which it is allowed to operate. See OECD, "Significant Market Power (SMP)," *OECD Glossary of Statistical Terms*, https://stats.oecd.org/glossary/detail.asp?ID=6755. See also, Leon (ITU-T Focus Group on Digital Financial Services), *Competition Aspects of Digital Financial Services (Focus Group Technical Report)*.

145 The technology was developed in China by Shanghai-based tech company F-Road in 2005, primarily as a mobile phone solution to support multi-operator access, designed to avoid roaming fees. Digitech and Taisys have in recent years developed their own technology. Taisys recently prevailed in a patent suit over the technology.

146 The thin SIM supports GSMA/3GPP/ETSI standards, making it compatible with all standard devices from older feature phones to the latest smartphones.

147 It also has a patented secure, encrypted SMS technology.

148 See Michele Hanouch and Greg Chen, "Promoting Competition in Mobile Payments: The Role of USSD," CGAP, February 2015, www.cgap.org/publications/promoting-competition-mobile-payments-role-ussd.

149 In the case of Equitel in Kenya, use of the shortcode *247# will divert the session to use the Airtel network. See Equitel, "Get Activated," 2016, www.equitel.com/my-phone/get-activated.

150 Sneha Jha, "Yes Bank to launch SIM sleeve payments solution for feature phones," *ETCIO.com*, April 12, 2016, http://cio.economictimes.indiatimes.com/news/mobility/yes-bank-to-launch-sim-sleeve-payments-solution-for-feature-phones/51780748. The transactions currently offered are P2P fund transfers, person-to-account (P2A) fund transfers using NEFT and IMPS, balance checking, payments to merchant for small and large value purchases and payment of bills; top-ups, and recharges.

151 It handles more than 5 billion RMB daily transactions. See CGAP Microfinance Gateway, "Shanghai F-road Wins 1st Prize in Wall Street Journal's Financial Inclusion Challenge," *CGAP*, February 3, 2016, www.microfinancegateway.org/announcement/shanghai-f-road-wins-1st-prize-wall-street-journals-financial-inclusion-challenge.

152 Photo credit: Taisys, www.taisys.com/solution.

153 Joackim Bwana, "Sh5.2m Fake Samsung phones Seized in Mombasa," *The Standard*, July 2, 2016, www.standardmedia.co.ke/article/2000207238/sh5-2m-fake-samsung-phones-seized-in-mombasa.

154 Dmytro Protsenko, "Regulatory Procedures and Solutions for Protecting the Market Against Counterfeit/Substandard Terminal Equipment in Ukraine," Proceedings of ITU Conference on Combating Counterfeit and Substandard ICT Devices, November 17-18, 2014, www.itu.int/en/ITU-T/C-I/Documents/WSHP_counterfeit/Presentations%20and%20Abstracts/S1P1-Dmytro-Protsenko.ppt.

155 Staff Reporter, "Illegal, Fake Mobile Phones Will Be Shut Down: Tarana," *NewsBangladesh.com*, January 26, 2016, www.newsbangladesh.com/english/details/10989.

156 Dmytro Protsenko, "Regulatory Procedures."

157 Dmytro Protsenko, "Regulatory Procedures."

158 The Communications Authority was previously known as the Communications Commission of Kenya.

159 Dmytro Protsenko, "Regulatory Procedures."

160 Edwin Okoth, "Big Brother could start tapping your calls, texts from next week," *All Africa*, February 17, 2017, http://allafrica.com/stories/201702170088.html.

161 Implementation of the system was, however, halted by court order. See Rachael Mburu, "Blow to Communications Authority as court suspends deployment of 'spyware,'" *Capital News*, February 20, 2017, www.capitalfm.co.ke/news/2017/02/blow-to-communications-authority-as-court-suspends-deployment-of-spyware/.

162 Bernama, "Cops Expose Gang Selling Fake Samsung H-Phones In S'wak," *Free Malaysia Today*, June 23, 2016, www.freemalaysiatoday.com/category/nation/2016/06/23/cops-expose-gang-selling-fake-samsung-h-phones-in-swak/.

163 Prahlad Rijal, "NTA's IMEI Registration Plan Set to Face Delays," *Kathmandu Post*, May 8, 2016, http://kathmandupost.ekantipur.com/news/2016-05-08/ntas-imei-registration-plan-set-to-face-delays.html.

164 Metronaija, "250 Million Fake Phones Sold In Nigeria Yearly—NCC," *Nairaland Forum*, September 11, 2015, www.nairaland.com/2591713/250-million-fake-phones-sold.

165 Franklin Alli, "Telecom companies to switch-off fake phones from networks—SON," *Vanguard*, August 8, 2014, www.vanguardngr.com/2014/08/telecom-companies-switch-fake-phones-networks-son/.

166 Anna Okon, "SON to Prosecute Substandard Phone Sellers," *The Punch*, May 26, 2016, http://punchng.com/son-prosecute-substandard-phone-sellers/.

167 Erik Prins, "Oman launches programme for identifying fake mobile devices," *Times of Oman*, April 13, 2016, http://timesofoman.com/article/81469/Oman/Government/Oman-launches-programme-for-identifying-fake-mobile-devices.

168 Abrar Hamza, "Import of Chinese mobile phones drops by 40%," *Daily Times*, May 24, 2016, http://dailytimes.com.pk/business/24-May-16/import-of-chinese-mobile-phones-drops-by-40.

169 BBC News, *Tanzania 'Cuts Off 630,000' Fake Phones*, June 17, 2016, www.bbc.com/news/world-africa-36558056.

170 Dana Moukhallati, "60,000 Fake Phones Seized in Dubai since Start of August," *The National*, August 25, 2014, www.thenational.ae/uae/courts/60000-fake-phones-seized-in-dubai-since-start-of-august.

171 Afkar Abdullah, "Fake Mobile Market Thrives in Ajman and Sharjah," *Khaleej Times*, July 8, 2016, www.khaleejtimes.com/nation/sharjah/fake-mobile-market-thrives-in-ajman-and-sharjah.

172 Dmytro Protsenko, "Regulatory Procedures."

173 International Telecommunications Union (ITU), "Resolution 79: The role of telecommunications/information and communication technologies in combating and dealing with counterfeit telecommunication/information and communication devices," The World Telecommunication Development Conference, 2014, www.itu.int/en/ITU-T/C-I/Documents/WSHP_counterfeit/WTDC-14-RESOLUTION%2079.docx.

174 See https://imeidb.gsma.com/imei/login.jsp.