# Role of the Telecommunications Regulator in Digital Financial Services

Leon Perlman[1]

**ABSTRACT[2]**

The mobile phone has evolved from its basic telecommunications utility to take on a new enhanced role as a ubiquitous payment and value transfer instrument in the economies of developing countries. These facilities, now mostly known as Digital Financial Services (DFS), involve complex interplays of telecommunications, financial services and related components, necessitating reassessment by a range of affected national regulators on whether and how to apply or adapt their sector-specific regulatory precepts to DFS and its providers.

For telecommunications regulators in particular - which we call National Telecommunications Authorities (NTA) – the introduction of DFS may require reassessment and even expansion beyond their traditional remit over telecommunications-type services.

Overall, the purpose of the paper is to provide a fresh perspective on the role of the NTA in relation to the success and growth of DFS and to systemize the understanding of the role of NTAs within the context of DFS. Due to the multi-sectoral and cross-cutting nature and increasing complexity of DFS, we argue for increased cooperation between implicated regulators and agencies as well as increased capacity building for NTAs. This study examines then the specific and evolving roles the NTA may have in regulating DFS and similar value transfer and payment mechanisms, whilst ensuring stability of national telecommunications infrastructure and service provision.

This study is part of a series on the role of the primary regulators in the DFS ecosystem, intended to simply systemize each of their roles.[3] For NTAs, there are a number of direct impacts on DFS provision that the NTA have remit over, *inter alia,* security of mobile networks; access to critical gateways and pricing thereof; agent exclusivity; service quality; mobile coverage; handset fraud and in some cases, licensing of DFS providers. It is also important for NTAs to find internal capacity to understand DFS markets so as to to ensure telecommunication services can effectively serve provision of DFS. Similarly, to determine how telecommunications services markets are affected by DFS since lock-in feedback loop network effects can have an impact on this market.

With this tight nexus, NTA's role must constantly evolve to keep pace with rapid innovations introduced by DFS, placing pressure on the NTA's capacity to respond as needed whilst fulfilling commitments to national goals of financial inclusion. The NTA's role may include responses to emerging security and fraud challenges; application of regulatory tools to ensure market stability, quality of services, fair competition, and service expansion; their assessment on ubiquitous provision of DFS from the effect of their policies on mobile coverage and mobile technologies; and the need for the NTA to ensure regulatory coordination with other authorities.

An important component of properly regulating the DFS ecosystem is the importance of collaboration between central banks, NTAs and competition authorities for them to understand each other's markets and their feedback loop effects which should include exchanges of data and analysis where allowed.

---

[1] Leon Perlman Ph.D.; Head: Digital Financial Services Observatory, Columbia Institute for Tele-information, Columbia University, New York.

[2] This research was funded through a grant from the Bill and Melinda Gates Foundation, which facilitated the creation of the Digital Financial Services Observatory, a DFS policy and regulatory research project of the Columbia Institute for Tele-information at Columbia University in New York. See www.dfsobservatory.com

[3] See thereto, Perlman, L (2018a) *The Role of Regulators in Competition-Related Matters in Digital Financial Services*, available at www.dfsobservatory.com; Perlman, L (2018b) *The Role of the Central Bank in DFS*, available at www.dfsobservatory.com. These studies all have common introductory sections.

## CONTENTS

## ABBREVIATIONS

| | |
|---|---|
| **2G** | Second Generation Mobile |
| **3G** | Third Generation Mobile |
| **4G** | Fourth Generation Mobile |
| **5G** | Fifth Generation Mobile |
| **AML** | Anti-Money Laundering |
| **AMR** | Adaptive Multirate |
| **AWS** | Advanced Wireless Services |
| **BOP** | Bottom of the Pyramid |
| **BTS** | Base Transceiver Station |
| **CAPEX** | Capital Expenditures |
| **CB** | Central Bank |
| **CBK** | Central Bank of Kenya |
| **CCK** | Communications Commission of Kenya |
| **CDMA** | Code Division Multiple Access |
| **CFT** | Countering the Financing of Terrorism |
| **CGAP** | Consultative Group to Assist the Poor |
| **CICO** | Cash In / Cash Out |
| **CIV** | Customer Identification and Verification |
| **COLT** | Cell on Light Truck |
| **COW** | Cell on Wheels |
| **DCB** | Direct Carrier Billing |
| **DD** | Due Diligence |
| **DFI** | Digital Financial Inclusion |
| **DFS** | Digital Financial Services |
| **DFS** | Mobile Financial Services |
| **DFSP** | Digital Financial Services Provider |
| **ECLAC** | Economic Commission for Latin America and the Caribbean |
| **EDGE** | Enhanced Data for Global Evolution |
| **ETSI** | European Telecommunications Standards Institute |
| **FCC** | Federal Communication Commission |
| **FRAND** | Fair, Reasonable and Non-Discriminatory |
| **G2P** | Government To Person |
| **GHz** | Gigahertz |
| **GPRS** | General Packet Radio Services |
| **GSM** | Global System for Mobile Communications |
| **GSMA** | GSM Association |
| **HSDPA** | High Speed Downlink Packet Access |
| **HSPA** | High Speed Packet Access |
| **HSUPA** | High Speed Uplink Packet Access |
| **Hz** | Hertz |

| | |
|---|---|
| **ICT** | Information and Communication Technology |
| **ID** | Identification |
| **IEEE** | Institute of Electrical and Electronics Engineers |
| **IFSC** | Indian Financial System Code |
| **IMEI** | International Mobile Equipment Identity |
| **IMT** | International Mobile Communications |
| **IP** | Internet Protocol |
| **ITU** | International Telecommunications Union |
| **IVR** | Interactive Voice Response |
| **Kbps** | Kilo Bits Per Second |
| **kHz** | Kilohertz |
| **KYC** | Know Your Customer |
| **LDC** | Least Developed Countries |
| **LEO** | Low Earth Orbit |
| **LONO** | Letter of No Objection |
| **LTE** | Long Term Evolution |
| **LTE-A** | LTE Advanced |
| **MB** | Megabytes |
| **Mbps** | Megabits Per Second |
| **MHz** | Megahertz |
| **MIMO** | Multiple Input Multiple Output |
| **MNO** | MNO |
| **MO** | Mobile Originated |
| **MVNO** | Mobile Virtual Network Operator |
| **NGO** | Non-Governmental Organization |
| **NI** | Network Initiated |
| **NSDT** | Near Sound Data Transfer |
| **NTA** | National Telecommunications Authority |
| **NTFA** | National Table for Frequency Allocation |
| **OECD** | Organisation for Economic Co-operation and Development |
| **OPEX** | Operational Expenditures |
| **OTA** | Over the Air |
| **OTC** | Over the Counter |
| **OTT** | Over the Top |
| **P2P** | Person to Person |
| **POS** | Point of Sale |
| **PPP** | Public Private Partnership |
| **QOS** | Quality of Service |
| **RAN** | Radio Access Network |
| **RF** | Radio Frequency |
| **SAR** | Specific Absorption Ratio |
| **SMP** | Significant Market Power |
| **SMS** | Short Message Service |

| | |
|---|---|
| **SMSC** | Short Message Service Centre |
| **SOC** | System on a Chip |
| **SP** | Service Provider |
| **SRA** | Sector Regulatory Authority |
| **SS7** | Signaling System 7 |
| **SSB** | Standard Setting Body |
| **STK** | SIM Toolkit |
| **SWN** | Single Wholesale Network |
| **TIP** | Telecom Infra Project |
| **Towerco** | Tower Companies |
| **TRAI** | Telecom Regulatory Authority of India |
| **TSP** | Technical Service Provider |
| **UCC** | Uganda Communications Commission |
| **UHF** | Ultra High Frequency |
| **UI** | User Interface |
| **UMTS** | Universal Mobile Telecommunications System |
| **US** | United States |
| **USAF** | Universal Service Access Fund |
| **USF** | Universal Service Fund |
| **USSD** | Unstructured Supplementary Service Data |
| **UX** | User Experience |
| **VAS** | Value Added Services |
| **VAT/GST** | Value Added Tax / Goods and Services Tax |
| **VHF** | Very High Frequency |
| **VLEO** | Very Low Earth Orbit |
| **VoLTE** | Voice over Long Term Evolution |
| **WAP** | Wireless Access Protocol |
| **WASP** | Wireless Application Service Provider |
| **WCDMA** | Wideband Code Division Multiple Access |
| **WIB** | Wireless in Browser |
| **WOAN** | Open Access Network |
| **WOAN** | Wholesale Open Access Network |
| **WRC** | World Radio Congress |

# 1 INTRODUCTION[4]

## 1.1 Overview[5]

Digital Financial Services (DFS)[6] are rapidly becoming a ubiquitous and affordable platform to increase overall levels of financial inclusion[7] by facilitating affordable and relatively easy to access basic financial services for those at the Bottom of the Pyramid (BOP).[8]

DFS is often enabled by regulatory and technological innovations that allow non-banks to provide basic financial services similar to those traditionally offered by banks but, hitherto, have been unavailable to those at the BOP who are typically 'un-banked.'[9] DFS are offered primarily by banks, non-bank third

---

[4] Information in this paper is drawn substantially from writings and presentations by the author. See Perlman, L (2003) *Mobile Commerce*, *Payments Conference, Cape Town;* Perlman, L (2010) *Mobile Money*, *Mobile Money Conference at Columbia Business School*; Perlman, L (2012) LLD *Thesis: Legal and Regulatory Aspects of Mobile financial Services,* available at https://bit.ly/2KGfC8k; Perlman, L (2017) *Technology Inequality: Opportunities And Challenges For Mobile Financial Service*s, available at https://bit.Ly/2r7nzny; Gurung, N & Perlman, L (2018) *Role of DFS in Humanitarian Crises Responses,* available at https://www.dfsobservatory.com; Perlman, L & Weschler, M (2018) *Mobile Coverage and Its Impact on DFS*, available at https://www.dfsobservatory.com; Perlman, L (2018) *The Regulators of DFS*, available at www.dfsobservatory.com

[5] **Study Scope Note for Readers:** The study uses an evidence-based approach to ventilate issues of concern and interest for entities and national regulators in the DFS ecosystem around the world. It also explores how these issues have been addressed – or not, as the case may be – either through market dynamics and/or regulatory intervention. This includes a description of the impact of regulatory overreach or forbearance. Given then the evidence-based nature of this study, the study does ***not*** look beyond the 'basics' of telecommunications law and policy and related issues. Similarly, it will not address any analytical questions on telecommunications law and policy as to whether a National Telecommunications Authority (NTA) indeed has a role in DFS. This extension would be beyond the scope of the evidence-focused nature of this study. The footnotes in this study though refer the reader to more comprehensive studies that provide a deeper understanding of telecommunications law and policy, regulation and enforcement, and related issues. The author notes too that some prominent industry participants we canvassed even questioned the need for a study of whether the NTA had a role in DFS: they believe the NTA has no role. This study we believe highlights the impact NTAs have on DFS, directly or indirectly.

[6] These mobile-based financial services are also variously also known in the developing world as 'mobile money' and 'Mobile Financial Services (MFS).' The GSM Association uses the term 'mobile money' to describe 'a service in which the mobile phone is used to access financial services.' See GSAM (2012) *Mobile Money*, available at https://bit.ly/2JyiTqg

[7] Many countries have developed financial inclusion strategies. A World Bank database shows 30 countries have National Financial Inclusion Strategies; 5 countries have National Financial Sector Strategies Addressing Financial Inclusion: 5 countries; while 2 countries have financial inclusion laws. See World Bank (2018) *National Financial Inclusion Strategies Resource Center*, available at https://bit.ly/2D2ur4l

[8] The bottom of the pyramid (BOP) refers to the bottom of the wealth pyramid or the bottom of the income pyramid is the largest, but poorest socio-economic group. The term BOP was introduced sometime in 1999 by Prahalad and Hart to describe what they observed were 'Four Consumer Tiers.' At the very top of the world economic pyramid, they said were 75 to 100 million affluent Tier 1 consumers from around the world, comprising a cosmopolitan group of middle- and upper-income people in developed countries and the few rich elites from the developing world. In the middle of the pyramid, in Tiers 2 and 3, are poor customers in developed nations and the rising middle classes in developing countries, the targets of past emerging-market strategies. Tier 4, they indicated, were the 4 billion people at the bottom of the pyramid who had an annual per capita income — based on purchasing power parity in US dollars — is less than USD 1,500, the minimum considered necessary to sustain a decent life. For well over a billion people — roughly one-sixth of humanity — per capita income is less than USD 1 per day. See Prahalad, C & Hart. S (1999) *Strategies for the Bottom of the Pyramid: Creating Sustainable Development*, available at https://bit.ly/2OdTYsV. For an analysis of the BOP concept years later with revised figures, see Kolk, A, Rivera-Santos, M & Rufin, C (2012) *Reviewing a Decade of Research on the 'Base/Bottom of the Pyramid' (BOP) Concept*, available at https://ssrn.com/abstract=2193938. In global terms, this is the three billion people who live on less than USD 2.50 per day. London, T (2008) *The Base-Of-The-Pyramid Perspective: A New Approach To Poverty Alleviation*, available at https://bit.ly/2KUAAjX

[9] This is a generic term to indicate that they have not had access to a bank account, or are underserved by lack of ready access to a financial services facility. For a discussion of these terms, see Lyman, T & Kate Lauer (2015) *What is Digital Financial Inclusion and Why Does it Matter?*, available at https://bit.ly/1GX1xdJ; and Evans, O (2016) *Determinants of Financial*

party Service Providers (SPs) and Mobile Network Operators (MNOs).[10] These services include person-to-person payments (P2P), cash-in/cash-out (CICO) 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. 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 DFS.

The general convergence of purpose where MNOs provide a full range of services from voice, data and multimedia applications accessible from mobile handsets and a full range of end-user devices has resulted in countries around the world to update their licensing and regulatory frameworks to address the increasing reality of this convergence.[11]

DFS, in particular, requires additional competencies from a National Telecommunications Authority (NTA) beyond its 'traditional competencies' relating telecommunications services. Invariably in relation to DFS, the NTA will have co-jurisdiction or (more probable) will closely cooperate with other regulators or government departments and agencies - for example on consumer protection, aspects of competition, and network security – and often mediated by a Memorandum of Understanding (MOU) between them.[12]

## 1.2 Methodology and Approach

The information contained within this study is based on research performed between November 2017 and July 2018. The author undertook *inter alia*, desktop research; sending of electronic surveys of technologies and policies employed NTAs in a number of countries where DFS is prevalent; interviews and conversations with personnel from NTAs and the DFS and telecommunications ecosystems; and selected location visits to investigate the nature of any problems and solutions.

The author also undertook capacity building with some NTAs through the Digital Financial Services Observatory (DFSO) series of webinars on DFS, of which there was a nominal testing component.[13] Background studies by other authors that survey the DFS ecosystem are included. Because of the scope and scale of our study, we have rely on external sources and previous internal studies undertaken by the author and others.

Overall, the objective of this study is to systemize the understanding of the role of NTAs within the context of DFS and, due to the multi-sectoral and cross-cutting nature of DFS, highlight the additional capacity required of the NTA as well as argue for increased cooperation between implicated regulators and

---

*Inclusion in Africa: A Dynamic Panel Data Approach,* available at https://bit.ly/2sEiD0V; and Sahay, R, Čihák, M, N'Diaye, P, *et al.* (2015) *Rethinking Financial Deepening: Stability and Growth in Emerging Markets*, available at https://bit.ly/1K4Gb3d

[10] In most cases and for reasons of brevity, this paper will mostly conflate third party service providers (SPs) - which may include banks - with MNOs, to mean entities providing DFS. Where the context necessitates it, SPs will be differentiated from MNOs: for example, in relation to competition issues and MNO mobile data coverage.

[11] International Telecommunication Union (2004) *Trends in Telecommunication Reform 2004/05: Licensing in an Era of Convergence: Summary*, available at http://goo.gl/aU3MP

[12] Perlman, L (2018) *Model MOU Between a central Bank and National Telecommunications Authority For Digital Financial Services Regulation*, available at www.dfsobservatory.com

[13] For more information about the DFS Observatory webinar archive, visit the DFSO website at www.dfsobservatory.com

agencies. We do not endorse nor specifically recommend any particular proposed solution which may be contained herein.

Organizationally, the study is split into two parts: Part 1 (**Section 1** to **Section 5)** introduces fundamental commercial, usability, technical, regulatory, policy and service components of the telecommunications and DFS ecosystems. Part 2 (**Section 6 to Section 13)** offers discussions on the role of the NTA in specific issues relating to telecommunications and provision of DFS.

To start, **Section 2** looks at the evolving role of the mobile phone as a new and pivotal mechanism in undertaking financial transactions, and in financial inclusion. It discusses the progenitor systems such as Direct Carrier Billing (DCB) using mobile airtime wallets to the emergence of basic 'DFS 1.0' transactional services, and then to the better user interfaces and richer services offered by 'DFS 2.0.'

**Section 3** introduces the regulators of DFS, and focuses on the role of the NTA in telecommunications provision and DFS, noting the evolution of its role and capacity building requirements and initiatives.

**Section 4** is an overview of the telecommunications-related technologies used in DFS, including the mobile infrastructure, the mobile handsets; user interfaces available to access DFS. This includes an important discussion on the types of mobile technologies

**Section 5** looks at the policies and mechanisms around licensing, allocations and service Authorisations and the role of spectrum provision in the evolution from basic 'DFS 1.0' transactional services to better user interfaces and richer 'DFS 2.0' services.

**Section 6** begins the paper's discussion on the role of the NTA in specific issues relating to DFS. This section looks at the role of the Customer Identify And Verification (CIV).

**Section 7** looks at the role of the NTA in pricing of telecommunications and DFS.

**Section 8** looks at the role of the NTA in competition issues relating to telecommunications and DFS.

**Section 9** looks at the role of the NTA in ensuring quality of service relating to telecommunications and DFS.

**Section 10** looks at the role of the NTA in ensuring that telecommunications and DFS systems remain secure.

**Section 11** looks at the role of the NTA in ensuring in privacy in use of telecommunications and DFS systems.

**Section 12** looks at the role of the NTA in consumer protection in telecommunications and DFS systems.

**Section 13** looks at the role of the NTA in taxation of MNOs, DFS service providers and customers of DFS.

**Section 14** offers conclusions to the issues raised in the study.

## 2 THE EVOLVING ROLE OF THE MOBILE PHONE AS A PAYMENT INSTRUMENT

### 2.1 Overview

The lack of access to formal banking and credit facilities and a latent demand for digital payments in emerging markets has led to the emergence of a number of innovative new payment facilities operated by non-banks that use features of low-cost mobile phones for ubiquitous and low-cost means of access. The key to their genesis was using the mobile phone as the primary means of access services. Core to this nexus is that, while 1.7 billion adults do not have a bank account, more than 1 billion of these unbanked adults have a mobile phone.[14] And while around 230 million unbanked[15] adults work for businesses and get paid in cash, 78% of these people own a mobile phone.[16]

The mobile phone soon evolved from its basic telecommunications utility to take on a new enhanced role as a ubiquitous payment and P2P transfer instrument in emerging economies manifesting in 'walled garden' payment systems controlled by MNOs now known as Direct Carrier Billing (DCB), followed by a more general purpose mobile-based financial ecosystem now known as Digital Financial Services. Differences between DCB and DFS is shown in **Exhibit 1** and in the sections that follow.

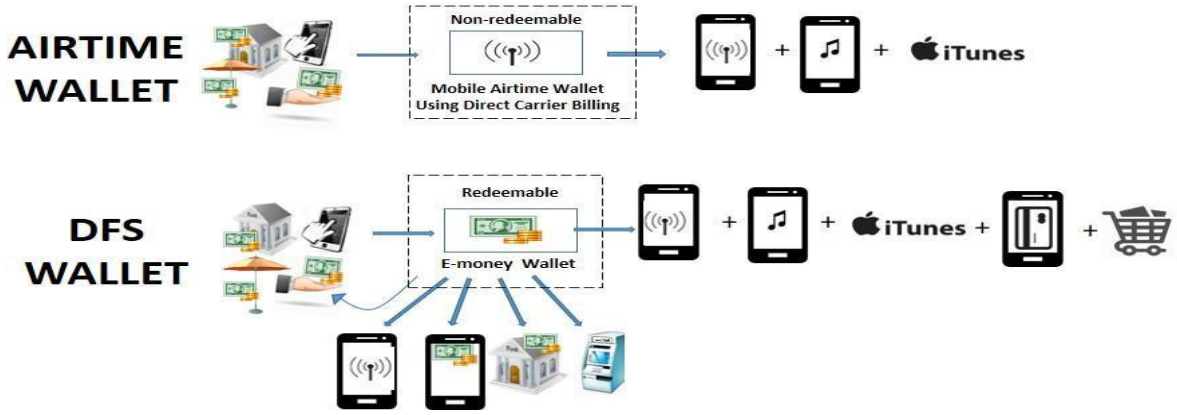



**Exhibit 1:** Transactional DCB and DFS ecosystems operated by a MNO. DCB (**top**) emerged in the late 1990's and uses mobile airtime electronic value stored in a mobile airtime (value) wallet by a MNO, and allows users to pay for digital goods and services and to do person-to-person (P2P) mobile airtime-only transfers. Customers usually buy these services through third party value added services (VAS) providers connected to the MNO. The value in the airtime wallet is non-redeemable. Later, DFS (**bottom**) – also known as 'mobile money' and 'mobile financial services' – emerged in the early 2000s and is characterized by an e-money wallet comprising fiat value, and which is usable for paying for digital and physical goods and services as well as to undertake, *inter alia,* P2P fiat-based transfers. The value in the e-money DFS wallet is redeemable on demand and on par, usually at DFS agents.

[14] Gallup (2018) *Global Findex: Technology Can Bridge Financial Inclusion Gap*, available at https://bit.ly/2IhCoVE

[15] For a discussion of these terms, see Lyman, T & Kate Lauer (2015) *What is Digital Financial Inclusion and Why Does it Matter?*, available at https://bit.ly/1GX1xdJ; and Evans, O (2016) *Determinants of Financial Inclusion in Africa: A Dynamic Panel Data Approach,* available at https://bit.ly/2sEiD0V; and Sahay, R, Čihák, M, N'Diaye, P, *et al.* (2015) *Rethinking Financial Deepening: Stability and Growth in Emerging Markets*, available at https://bit.ly/1K4Gb3d

[16] Some 100 million 'unbanked' adults worldwide receive government payments (G2P) in cash, including 67 million who have a mobile phone. Gallup (2018) *ibid.*

## 2.2 Progenitor Mobile-based Payment Services

Progenitor ecosystems where the mobile phones were first used as a payment instrument emerged in the late 1990s using prepaid mobile airtime and post-paid mobile phone bills and the store of value. Now known as Direct Carrier Billing (DCB), these ecosystems allowed effortless purchased of almost exclusively incorporeal digital goods and services. MNOs and wireless application service providers (WASPs) provided services. NTA could have oversight over the use of shortcodes, VAS or 'content' licenses.[17] In many cases the Central Bank has, together with the NTA, undertaken oversight over what type of digital services could be purchased through DCB.

A progenitor e-wallet micro-payment system emerged through the use of prepaid airtime wallets, usually through the provision of VAS services. Here, the MNO's airtime wallet provide a digital liquidity to purchase VAS. Now known as Direct Carrier Billing, the DCB-based wallet is based on mobile airtime, and allows for mainly digital goods and purchases. The value is non-redeemable. The DFS wallet allows for additional services to be provided, and the value is redeemable. The NTA leads the process of regulating this use, since the source of airtime value is from a licensed MNO. The central bank provides supporting guidance for the ability or not to use mobile airtime value in the broader (physical) economy.[18]

## 2.3 The DFS Ecosystem

The early 2000's saw the emergence of a low-cost financial and transactional ecosystem - known then as 'mobile money' and 'mobile financial services' - but now more formally as DFS. It is characterized by the use of a fiat-based, redeemable on demand e-wallet, demonstrating a salient transformational evolution from DCB, by allowing mobile phones to be used as general purpose payment instruments using 'e-money' stored for the user in a DFS wallet operated by a non-bank DFS provider (DFSP).

User value - or 'digital liquidity' - is stored in an e-money mobile wallet hosted by DFSPs. This value is primarily based on the national (fiat) currency and can be redeemed on demand and at par.[19] Liquidity within the DFS ecosystem is usually facilitated by electronic-human combinations, primarily using agents, who provide what are known as 'cash in/cash-out' services by swapping cash for e-money and vice versa.

Service bouquets for DFS, in particular across the world have grown, in many cases, resembling basic transactional features of a bank account but with primarily non-credit, transactional services at their core.[20] These basic transactional capabilities – initially called 'mobile money' - are coined 'DFS 1.0' by this study. The current iteration as 'DFS 2.0' is characterized by more sophisticated service offerings. Exhibit

---

[17] Perlman, L (2012) LLD *Thesis: Legal and Regulatory Aspects of Mobile financial Services,* available at https://bit.ly/2KGfC8k

[18] Perlman, L (2018) *The Regulators of DFS*, available at www.dfsobservatory.com; Perlman, L (2018) *The Role of the Central Bank in DFS*, available at www.dfsobservatory.com

[19] These are often termed e-money, a pecuniary construct usually derived from a regulatory process. MNOs may also offer users an alternate wallet where the store of value is based on mobile airtime acting as a virtual currency. Indeed, many of the services available through what is now known as DFS evolved from the modalities and systems involved in the initial use of the MNOs airtime wallet to pay for infotainment-type VAS.

[20] Unlike the value in most bank accounts, no interest is provided on e-wallet account balances in most DFS implementations. ITU (2016) *Digital Financial Services: Regulating For Financial Inclusion – An ICT Perspective*, available at https://bit.ly/2w8ryfT

3 shows the evolutionary split between DFS 1.0 and DFS 2.0-based services and the mobile instrument (more specifically the type of mobile phone) required to access the full range of each type of service.

The first service to recognize the potential nexus between broad access to fiat-based financial services and mobile phones was Smart Money, launched in 2001 in the Philippines by MNO Smart communications, which used the network as the communications channel for facilitating mobile payments and remittances using SMS-based SIM Toolkit as the UI.[21] At its most basic iteration, customer accounts would be operated and controlled by Smart, now also acting as a financial service provider, in additional to its role as a MNO. Agents contracted to the Smart Money provided cash-handling and account sign-up facilities and covert cash to electronic money ('e-money') which could be used to send to other Smart Money customers and buy a limited range of goods and services.

**Exhibit 2:** The Genesis of DFS

Depending on the jurisdiction, generally four broad types[22] of DFS operational models have evolved through regulation and policy. These include:

- Operating licenses or consent for non-banks to provide DFS[23]
- Mandated partnerships where non-banks must use banks to provide DFS[24]
- Bank-only provision of DFS with non-banks only providing technical support and/or agent services
- Bank-only provision of DFS[25]

Each of these models have their own complexities and challenges and varying success and efficacy for financial inclusion. Globally, the non-bank-only DFS models[26] have been the most successful because they want to and are able to serve the 'unbanked' population in (rural) areas that banks were unwilling to do. MNOs in particular could use their airtime and SIM-sale agents for DFS provision. While the first DFS incarnations were launched in Asia in the early 2000's, it was MNO Safaricom's M-PESA DFS system launch in 2007 in Kenya[27] that propelled DFS into the global spotlight. Its subsequent phenomenal growth has provided the prospect of a model financial ecosystem for the unbanked that catalyzes and accelerates financial inclusion.[28] As of May 2018, there were 276 DFS offerings live in 90 countries.[29] They provide DFS to over 690 million people, many of whom live in rural areas.[30]

[21] GSMA (2009) *Mobile Money in the Philippines – The Market, the Models and Regulation*, available at https://bit.ly/2I9EXG7 G-Cash started commercial operations in the Philippines in October 2004. Globe Telecom (2004) *Annual Report 2004*, available at https://bit.ly/2w9i2cj

[22] There may be slight variations in a particular jurisdiction because of the political economy of the country.

[23] M-PESA Kenya was initially provided with a 'Letter of No Objection' (LONO) to operate DFS by the Central Bank of Kenya. This was later grandfathered into a (DFS) license. See Perlman, L (2012) LLD *Thesis: Legal and Regulatory Aspects of Mobile financial Services,* available at https://bit.ly/2KGfC8k

[24] In Bangladesh, DFSP b-Kash is part-owned by a bank. MNOs cannot provide stand-alone DFS.

[25] In some cases, some banks may form a new bank-light entity to provide low-cost services which do not include credit provision.

[26] The majority of the non-banks providing DFS are MNOs.

[27] Vodafone (2018) *M-PESA*, available http://www.vodafone.com/content/index/what/m-pesa.html

[28] The e-money in the DFS wallet is fiat-based and is fungible, meaning that the e-money can be 'bought' using cash and be cashed-out back into cash, or transferred to another fiat-based e-money DFS wallet. Such fungibility is currently restricted in most jurisdictions using DCB ecosystems although this is slowly changing.

[29] GSMA (2018) *2017 State of the Industry Report on Mobile Money*, available at https://bit.ly/2CKPLqF

[30] *ibid*

| | DFS Activity | Basic | Feature | Smartphone |
|---|---|---|---|---|
| **DFS 1.0** | *Check balances* | Y | Y | Y |
| | *P2P transfer* | Y | Y | Y |
| | *Cash In/Cash Out* | Y | Y | Y |
| | *Pay Bills* | Y | Y | Y |
| **DFS 2.0** | **Secure transactions** | N | Y | **Y** |
| | **e-KYC[31] with camera** | N | Y | **Y** |
| | **Agent liquidity** | N | N | **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** |
| | **Universal search facility for Bill Pay Bank codes** | 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** | N[32] | Y[NS][33] | **Y[NS]** |

**Exhibit 3:** Characteristics of DFS Phone Types. Characteristics of phone types needed for different type of DFS services. The services in italics at the top of the table are the foundational DFS 1.0 activities in DFS markets. The services shaded indicate the next level of DFS – DFS 2.0 - some of which are provided today in a limited number of countries.

The ability of DFSPs to make these services ubiquitous is enabled by:

- Improvements in mobile network technology and coverage
- Greater reliability and sophistication of mobile handsets
- Better mechanisms to identify and authenticate users[34]
- Increasing acceptance by merchants of electronic payment instruments
- New vendor platforms that allow non-banks to safely store both fiat-backed and airtime-based user value
- The leveraging of features of Global System for Mobile Communications ('GSM') mobile technology[35] that allow them to act as both an access mechanism and a seamless user interface (UI) for navigating DFS service options.

[31] Know Your Customer (KYC)
[32] If not included or non-standard (NS), made possible with NFC 'stickers' placed on the back of non-NFC phones.
[33] *ibid*
[34] ITU DFS FG (2017) *Identity and Authentication,* available at https://bit.ly/2KistMX
[35] These include features such as voice, Short Message Services (SMS) and Unstructured Supplementary Service data (USSD).

These services depend on specific access and UI technologies,[36] all with varying degrees of ease of access, ease of use, efficacy, cost, security and reliability.[37] Most DFS technologies use the GSM[38] mobile infrastructure as the standard for mobile technology starting in the early 1990s. In the majority of countries where DFS is provided, low-speed (narrowband) second generation (2G) technologies still prevail with third generation (3G) and higher technologies[39] mostly only available in urban and peri-urban areas. And over 60% of users in these DFS countries still[40] use mobile phones, which are now termed 'basic' or 'feature' phones. [41]

With basic and feature phones dominating most DFS markets, SPs mostly facilitate access to DFS systems primarily via text-based USSD and the SMS-based SIM Toolkit (STK) – both of which work on almost all GSM-based handsets.[42] Smartphones in these countries are usually only found in the urban and peri-urban areas, which match the 3G and higher mobile phone coverage available in those locations.[43]

# 3 THE REGULATORS OF DFS

## 3.1 Overview

Laws, regulations, supervision and oversight have traditionally followed an institutional approach, whereby specific regulators have had supervisory oversight and rule-making capacity over institutions within their regulatory domain. Thus, for example, banks have traditionally been regulated by the national banking regulator and telecommunications entities by the national telecommunications regulator.

But with non-bank entities, such as telecommunications companies and service providers offering banking-like financial and transactional services through DFS for purposes of financial inclusion, there has been disruption of traditional categorizations and supervisory and oversight roles. The first primarily transactional iterations of DFS by banks and non-banks alike around the world have shown that the core regulatory authorities required to provide an enabling environment for the establishment of DFS involve

[36] See Section 4.5 on UIs

[37] Other technologies – such as QR codes; Bluetooth Low Energy and Magnetic Secure Transmission – were considered, but were found not to be suitable, for now, for mass use in DFS-focused countries.

[38] Originally Groupe Spécial Mobile. It is a standard developed in the 1980s by the European Telecommunications Standards Institute (ETSI) to describe the protocols for second-generation (2G) digital cellular networks used by mobile phones. The first GSM implementation was in Finland in 1991 on a network built by Telenokia and Siemens and operated by Radiolinja. In 1992, the first Short Messaging Service (SMS) message was sent; Vodafone UK and Telecom Finland signed the first international GSM roaming agreement. See GSMA (2016a) *History*, available at https://bit.ly/1sHjxSC. These digital technologies have since evolved to include second generation (2G) mobile technologies that include technologies such as Unstructured Supplementary Service Data (USSD), Short Message Service (SMS) and various low data speed capabilities. together constituting the enabling infrastructure for basic DFS provision.

[39] Broadband includes 3G and higher technologies, such as 4G (fourth generation) and 5G (fifth generation) technologies.

[40] See *inter alia,* GSMA (2018) *2017 State of the Industry Report on Mobile Money*, available at https://bit.ly/2CKPLqF; GSMA Intelligence (2018*) Blog: Why Is Bangladesh Experiencing Tepid 4G Uptake?,* available at https://bit.ly/2Iqtcvh; Perlman, L (2017) *Technology Inequality: Opportunities And Challenges For Mobile Financial Service*s, available at https://bit.Ly/2r7nzny

[41] Feature phones include most of the features of basic phones, augmented by features such as Bluetooth, MMS, WAP capabilities, and in some cases 3G and 4G capabilities.

[42] Excluding some smartphones.

[43] A number of 'contactless' facilities such as Near Field Communication (NFC)) and linkages of fiat-backed DFS accounts to companion debit cards are also spurring the growth of merchant payments

three entities – a country's central bank, its telecommunications regulator and the financial intelligence authority.[44] An enabling environment requires regulators to strike a balance between financial inclusion goals and financial integrity imperatives. This balance allows for the introduction of new services and innovation by new participants whilst protecting consumers and the integrity of the financial system as a whole.

As DFS evolves beyond basic transactional accounts to more complex services such as credit provision and merchant payments, additional regulatory authorities may assert supervision and oversight over components of the ecosystem. This also means that domain-specific laws and regulations may need to be modified to avoid a situation where multiple laws applicable to DFS participants create inconsistent and conflicting results, which is a common cause of regulatory arbitrage.

Capacity building within regulatory authorities and coordination between policy makers is also required to ensure consistency and predictability in laws, regulations and their application whilst allowing innovation to foster. The better each regulator understands the risks and benefits of DFS as perceived by the others, the more likely that their engagement will reflect a proportionate approach to regulation and supervision of the relevant actors and products.[45]

DFS is an emerging and evolving ecosystem. In developing countries where DFS is primarily found, the extent to which legislative framework exists and has been updated to address dynamic changes over time varies greatly. At its most basic transactional enabling of person-to-person transfers, a DFS ecosystem will have as direct regulatory overseers the central bank, the telecommunications regulator and, if they separately exist, AML, competition and consumer protection regulators. Indirectly and by default, an identity authority, tax authorities and those overseeing commercial entities will also have some degree of oversight or will provide essential enabling frameworks.

The core DFS 1.0-related regulators will include the central bank, telecommunications regulators and financial intelligence units. The variety of DFS 2.0 regulators will increase as service offerings and competition-based complexities increase. While their regulatory roles are usually similar, their exact names, boundaries of remits, and existence on the list of national regulators will vary between jurisdictions.[46]

Generally, for DFS, the central bank is the lead regulator and the telecommunications regulators have, up to now, acted in a supporting role, to some degree, with their jurisdiction mostly limited to issues related to the telecommunications channel.

[44] There are of course specialized laws and regulators who may have an omnibus remit over an entity, no matter the institution and service offered. For example, financial intelligence agencies, competition regulators, tax authorities, financial services regulators, privacy and data protection regulators, trade and industry regulators, and consumer protection regulators.

[45] GPFI-CGAP (2012) *Global Standard-Setting Bodies and Financial Inclusion for the Poor Toward Proportionate Standards and Guidance,* available at https://bit.ly/2LcdaXt

[46] For the cross-jurisdictional aspects of DFS, see Perlman, L (2018) *The Regulators of DFS*, available at www.dfsobservatory.com

## 3.2 The Role of the NTA

### 3.2.1 Overview

Much of the telecommunications industry globally was, until the 1980s, characterized by public monopolies[47] with postal mail, telegraph and telephone services (PTT) provided by a single government agency.[48] Thus, separate regulators were not needed.[49] Since the beginning of 1980s, liberalization has seen the establishment of separate postal and telecommunication operators and opening competition.[50]

These restructuring initiatives were first seen in the United States when the Telecommunications Act of 1996 lowered barriers to entry,[51] opening up the market for other players and required interconnection and access to infrastructures.[52] Similarly, in the UK, liberalization followed the separation of postal and telephone services in 1981 and the privatization of British Telecom in 1984.[53] Such developments in the US and UK preceded similar restructuring and liberalization initiatives in other countries.[54] Whereas in the early 1990s only nine countries had a separate regulator for telecommunications,[55] within the next two decades this increased to 158.[56]

The evolving nature of information and communications technology (ICT) based services and the introduction of financial services has affected and tested the ability of NTAs to understand, respond to and develop new policies and/or regulations thereto. NTAs' tasks are usually very challenged by first, a lack of qualified personnel and second, continued threats of or actual legal action against them by dissenting licensees or those wanting licenses. As a result, their licensing and rule-making procedures may often take years, be very rigid and normative and, sadly, largely inchoate.

---

[47] International Labour Organization (1998) *Structural and Regulatory Changes In Globalization In Postal And Telecommunications Services: The Human Resources Dimension*, available at https://bit.ly/2IchG6

[48] Davids, M (1995) *The Relationship Between the State Enterprise for Postal, Telegraph, and Telephone Service and the State in the Netherlands in Historical Perspective,* available at https://bit.ly/2KhWMUf; Huurdeman, A (2003) *The Worldwide History of Telecommunications,* available at https://bit.ly/2I8nDW9

[49] Technofunc (2018) *History of Telecommunications Industry,* available at https://bit.ly/2L7G1wa

[50] International Labour Organization (1998) *Structural and Regulatory Changes In Globalization In Postal And Telecommunications Services: The Human Resources Dimension*, available at https://bit.ly/2IchG6

[51] Technofunc (2018) *History of Telecommunications Industry,* available at https://bit.ly/2L7G1wa

[52] *ibid*

[53] Rodine-Hardy, K (2015) *Globalization, International Organizations, and Telecommunications,* available at https://bit.ly/2rLXSkl

[54] *ibid*

[55] Schwarz, T & Satola, D (2000) *Telecommunications Legislation in Transitional and Developing Economies,* available at https://bit.ly/2Ihg0Zk

[56] ITU (2014) *World Telecommunication/ICT Indicators Database Online,* available at https://bit.ly/2k5FFtv. A number of countries regulate their telecommunications ecosystem via a ministry of communication. For a list of African telecommunication regulators, see African Telecom News (2018) *Africa Telecommunications Regulators*, available at https://bit.ly/2IxuiZn

| Telecommunications-related Competencies | |
|---|---|
| Licensing of MNOs | **Yes** |
| Authorization To provide VAS | **Yes** |
| Data Privacy | **Yes** |
| Consumer Protection | **Yes** |
| Quality of Service | **Yes** |
| Competition | **Often** |
| Anti-Money Laundering | **Yes** |
| Infrastructure Security | **Yes** |
| Taxation of airtime/SIMs | **Yes** |
| Taxation of VAS | **Yes** |
| MVNO Licensing | **Yes** |
| Infrastructure sharing | **Yes** |
| Fraud Detection | **Yes** |
| Spectrum Allocation/sale | **Yes** |
| Mobile Airtime Agent Registration | **Yes** |
| Handset Approvals/SAR/QOS | **Yes** |
| SIM card registration | **Often** |
| Universal Service Funds | **Often** |
| IMEI Database | **Often** |
| Wholesale pricing | **Yes** |
| Mobile Number Portability | **Yes** |
| Content Regulation | **Sometimes** |
| Net Neutrality | **Yes** |
| Retail price control | **Often** |
| Cybercrime | **Yes** |
| Cyber-resilience | **Often** |
| Broadband Policy | **Yes** |
| Interconnection | **Yes** |
| Spectrum Monitoring | **Yes**[57] |
| POS Type approvals | **Often** |

| DFS-related Competencies | |
|---|---|
| Authorization To provide DFS | **Often** |
| Authorization To provide DFS as VAS | **Often** |
| Taxation of DFS transactions | **Yes** |
| Taxation of VAS | **Yes** |
| DFS Transaction Data Monitoring | **Yes** |
| DFS Interoperability | **Sometimes** |
| DFS Agent Registration | **Sometimes** |
| Transaction Security Over Bearers | **Often** |
| FRAND Access to DFS Bearers | **Yes** |
| Data Privacy | **Yes** |
| Retail price control over DFS bearers | **Sometimes** |
| AML/KYC for DFS | **Sometimes** |
| Money Laundering | **Yes** |
| Cybercrime | **Yes** |
| Wholesale price control over DFS bearers | **Often** |
| Contribution to Financial Inclusion Policies | **Often** |

**Exhibit 4**: NTA remits over telecommunications and DFS-related and over mobile coverage components. DFS has expanded - by regulation and circumstance - the remit of the NTA and required additional competencies to be brought into its personnel complement. Often the NTA will share DFS-related competencies with other regulators and agencies in an MOU, most often the central bank.[58]

### 3.2.2 NTA Regulatory Evolution

The traditional remit of NTAs has been on telecommunications related issues. As the internet has permeated the technology environment, this role has evolved to ICT to provide the roadway for provision internet-based services. This has evolved to what has become known as a 'converged' regulator where,

[57] For example, the Malawian NTA signed a MOU on spectrum management with the Malawi Police Service (MPS). See MACRA (2017) *MACRA And MPS Sign Mou On Spectrum Management,* available at https://bit.ly/2rIU3vh

[58] See Annex B: MOU

inter alia, content sent over the 'pipes' over which the NTA has remit is also folded into the NTAs remit. The latest evolution, of course, is DFS.

From this rapid technology and services evolution, the NTA has had to adapt, enhance and upgrade its capacity to regulate beyond just 'basic' telecommunications-type services. This highlights key challenges for NTAs, including the need for cross- cutting skills and the importance of having adequate human resources to fulfil the regulatory mission. This is complicated though when the NTA is a multi-sector NTA handling, for example, electricity and transport besides telecommunications. The situation is even more pronounced where there is no independent NTA or components of a NTAs remit is split with a government ministry[59] or other technology regulators.[60]

As a result, many developing countries are still in the midst of their regulatory 'transition' which the ITU's Regulatory Tracker sees as involving generational shifts:[61] The first is the early stage of regulation where a government acts as policy maker, regulator and sector player, progressing towards a fully competitive environment in which regulators work with other sectors in harmonizing regulation across the entire ICT ecosystem to ensure systematic use of information and communication technologies in key sectors like health, education and trade.

In Kenya, the Kenya Communications (Amendment) Act[62] was passed to expand the opportunities presented by converged technologies; in so doing it also expanded the regulatory scope and jurisdiction of the NTA, the Communications Authority. The CA issues licenses in terms of the Kenya Communications Act,[63] the Kenya Communications (Amendment) Act of 2009[64] and the Kenya Communications Regulations.[65]

[59] See for example Angola where the NTA INCOM's activities are split with the Ministry of Telecommunications and Technologies.

[60] See for example in Colombia, where telecommunications, spectrum and broadcasting is split between the Comisión de Regulación de Comunicaciones; Ministerio de Tecnologías de la Información y las Comunicaciones (http://www.mintic.gov.co/ MinTIC); Autoriad Nacional de Televisión (http://www.antv.gov.co/ ANTV); and Agencia Nacional del Espectro (http://www.ane.gov.co/ ANE). For an updated list of NTAs, see ITU (2018) *National Telecommunication Agencies,* available at https://bit.ly/2IkOcr3

[61] The ITU refers to the 'invisible mile' (of regulatory evolution) as being a hindrance to provision of telecommunications services: policy failures, such as market concentration, troubled privatization, excessive taxation, and monopoly control over international gateways, remain the principal bottlenecks impeding broadband development in the LDCs. See ITU (2018) *Achieving Universal And Affordable Internet In The Least Developed Countries*, available at https://bit.ly/2DNWII3

[62] Parliament of Kenya (2009) *Kenya Communications (Amendment) Act 1 of 2009*, available at https://bit.ly/2Kxkko2

[63] Parliament of Kenya (2009) *Kenya Communications Act 2 of 2009*, available at https://bit.ly/2L8Y1q0

[64] For a broader perspective on how the Act possibly impacts on media freedoms and the ability to disseminate information, see Wanjiku, R (2009) *Kenya Communications Amendment Act (2009): Progressive or Retrogressive?*, available at http://goo.gl/vAP05

[65] Communications Commission of Kenya (2011b) *Sector Regulations*, available at http://goo.gl/yNHiQ

| LDCs in G1 | LDCs in G2 | LDCs in G3 | LDCs in G4 |
|---|---|---|---|
| Chad, Djibouti, Eritrea, Ethiopia, Kiribati, Lao PDR, Niger, Solomon Islands, Somalia, Timor-Leste, Yemen | Angola, Benin, Bhutan, Burundi, Central African Republic, Comoros, Guinea, Guinea-Bissau, Haiti, Liberia, Madagascar, Mozambique, Myanmar, Nepal, Rwanda, S. Tomé & Principe, Sierra Leone, Togo | Afghanistan, Bangladesh, Burkina Faso, Cambodia, Congo (Dem. Rep.), Gambia, Lesotho, Malawi, Mali, Mauritania, Senegal, Sudan, Tanzania, Vanuatu, Zambia | Uganda |

**Exhibit 5:** ITU's categorization of Least Developed Countries by generation of their telecommunications-related regulation evolution.[66] Although this scheme is becoming somewhat dated, it is still relevant. Here 'G1' in this scheme refers to Regulated public monopolies. Command & control approach; G2 refers to 'Opening markets. Partial liberalization and privatization across the layers;' G3 refers to 'Enabling investment, innovation and access. Dual focus on stimulating competition in service and content delivery and consumer protection;' G4 refers to integrated regulation. Led by economic and social policy goals.' The ITU[67] report notes that most LDCs are located within the first or second generation of regulation. Fifteen have graduated to the third generation. Uganda is the only LDC that has crossed to the fourth generation, and none is in the fifth.

### 3.2.3 NTA Capacity

Weak regulatory capacity for the implementation and enforcement of regulations are a current characteristic of regulatory oversight and supervision in DFS within a number of jurisdictions.[68] Capacity building as well as scaling up personnel to expertly handle disparate components making up each of these ecosystems and expanded remits, take time and money often not budgeted by the NTA or not provided by the national treasury.

Many of these NTA-focused capacity building programs will involve licensing, competition policy, regulatory impact assessments, dispute resolution, universal service and effective regulation.[69]

While NTAs, to some degree, can self-fund via license fees and fines for license transgressions, often NTA budgets are buffeted by unexpected and sustained legal clashes with licensees and/or the organizations that represent them. Invariably, to defend many of these legal cases (which invariably challenge regulations issued by the NTA),[70] extended and comprehensive market studies (such as on

[66] ITU (2018) *ITU Global ICT Regulatory Outlook 2017*, available at https://bit.ly/2IDUx0m; ITU (2018) *Achieving Universal And Affordable Internet In The Least Developed Countries*, available at https://bit.ly/2DNWII3

[67] ITU (2018) *Achieving Universal And Affordable Internet In The Least Developed Countries*, available at https://bit.ly/2DNWII3

[68] Author observation in visits to and interacting with financial, AML, and telecommunication regulators from over 30 countries.

[69] On schemes for undertaking capacity building for developing country NTAs, see Goulden, B (2005) *Building ICT Regulatory Capacity In Developing Economies: A Learning Framework For Regulators*, available at https://bit.ly/2KpqBSW

[70] Besides licensees taking legal action against the NTA, other government departments may take legal action. See for example, the Department of Telecommunications and Postal Services in South Africa interdicting the NTA ICASA from spectrum auction. See ITWeb (2016*) Cwele asks court to block spectrum auction*, available at https://bit.ly/2wKNf61

significant market power assessment, broadband policy development and regulatory impact assessments) by outside international consultants and priced in non-local currencies, need to be undertaken.[71]

In many cases, given budget shortfalls and deficits in local expertise to undertake capacity building, it has been up to donors such as the World Bank and its satellites[72] to provide the funding for ongoing capacity building as well as to source and provide the external expertise[73] to undertake any necessary training. Many of these capacity building events will encompass regional workshops where regional NTAs (and often other regulators) assemble in one location.[74] The GSMA also undertakes capacity building for MNOs.[75]

### 3.2.4 Cooperation between Regulators over DFS

As services move beyond purely person-to-person transfers and become more sophisticated, varied and integrated into the national fabric, other regulators – such as those overseeing credit or insurance provision - may also become involved and need to exercise their remit over participants, technology components and services. Bilateral or multilateral MoUs between these regulators are generally necessary to coordinate oversight and to prevent regulatory arbitrage.[76]

The appropriate regulator to handle a specific matter may not always be clear. Sometimes there may be an absence of enabling legislation or unclear boundaries regarding existing legislation, leaving answers as to the appropriate regulator unclear and leading to regulator shopping. But there are methods which are used to maintain peace and order between regulators. Bilateral or Multilateral; MOU is another option and is an agreement between regulators on how to handle verlap and who will have authority to handle which matter.[77]

Key to understanding the potential coincidences of NTA's remit with the DFS ecosystem is a technical insight into the technical components of the ecosystem, both at infrastructure and customer levels. These potential remits are shown in Exhibit 4.

---

[71] See a discussion thereof at ITU (2018) *ITU Global ICT Regulatory Outlook 2017*, available at https://bit.ly/2IDUx0m; ITU (2018) *Achieving Universal And Affordable Internet In The Least Developed Countries*, available at https://bit.ly/2DNWII3

[72] See for example, the World Bank's International Bank for Reconstruction and Development who funded 'Telecommunications Regulatory Capacity Building, through a USD 492,300 grant from its Institutional Development Fund. The program was aimed at supporting the Telecommunications Regulatory Authority of Lebanon in the streamlining of its internal processes, strengthening transparency, and building technical capacity on regulatory issues. The World Bank held a capacity building event for the NTA RURA in Rwanda in May 2018 alongside regional competition regulators.

[73] The DFSO itself undertook capacity building with some NTAs through the DFSO series of webinars on DFS, of which there was a nominal testing component. See https://dfsobservatory.com/content/dfso-event-archive

[74] See for example meetings on Capacity Building for ICT/Telecom Regulators and Policy Makers in the Pacific; ECOWAS country regulators in both English and French on licensing, universal service, and effective regulation

[75] See GSMA (2018) *Capacity Building,* available at https://bit.ly/2L5h5FB; GSMA (2018) *Capacity Building Course Catalogue*, available at https://bit.ly/2InrkTQ

[76] In Kenya, for example, the NTA, the Communications Authority. issued rules around account-to-account interoperability, which many believed was beyond its remit, that rather was the preserve of the Central Bank of Kenya. See FTA (2017) *Communications Authority of Kenya to force interoperability on Mobile Money Operators*, available at https://bit.ly/2EZjXF8

[77] See Annex B showing an extract from the MOU between the Malawian NTA, MACRA, and the central bank, the Reserve Bank of Malawi. For a model MOU between a NTA and a central bank, see Perlman, L (2018) *Model MOU Between a central Bank and National Telecommunications Authority For Digital Financial Services Regulation*, available at www.dfsobservatory.com

# 4 TECHNOLOGIES USED TO ACCESS DFS

## 4.1 Overview

Several technologies[78] are available in DFS ecosystems that allow users to access their stored value, each with varying degrees of ease of access, ease of use, efficacy, cost, security, and reliability. [79]

Combinations of several types of remote access may be used, for technical reasons, for confirming transactions, regulatory requirements, the user experience (UX), competition issues or simply for cost reasons. Invariably though, SPs will provide the remote access method(s) that are best suited to the access devices prevalent in the markets in which they operate whilst taking into account the technical literacy levels of their customer base[80] as well as the type of handsets in use. Basic and feature phones currently dominate most DFS markets,[81] necessitating text-based UIs.

In more recent implementations from mid-2012, DFS-oriented apps using Over The Top (OTT) internet connectivity via smartphones are emerging but are not, as yet, in mainstream use in most DFS markets[82] since the high-speed data networks required to sufficiently enable these apps are not always available nationally. The availability and ultimate use of these technologies are, in many cases, dependent on policies and interventions by the NTA. That is, *inter alia,* making the technologies available broadly; the cost of the access; and whether the technologies are made fairly available.

# A MOBILE INFRASTRUCTURE LEVEL

## 4.2 Overview

Key to the growth of DFS in many emerging markets is the ability to effectively 'bolt-on" services to mobile network access mechanisms and UIs. GSM was invented in the late 1980s in Europe and has evolved to become the dominant mobile technology worldwide.[83] The GSM specification has, at its core, the Mobile Application Part (MAP) protocol, that specifies how users can gain seamless access to mobile

[78] Data based on Perlman, L (2003) *Mobile Commerce*, *Payments Conference, Cape Town;* Perlman, L (2010) *Mobile Money*, *Mobile Money Conference at Columbia Business School*; Perlman, L (2012) *LLD Thesis: Legal and Regulatory Aspects of Mobile financial Services,* available at https://bit.ly/2KGfC8k

[79] Invariably though, SPs will provide the remote access method(s) that are best suited to the access devices prevalent in the markets in which they operate whilst taking into account the technical literacy levels of their customer base. On the effects of technical literacy on DFS use, see Grameen Foundation (2013) *Use Of Mobile Financial Services India And The Philippines,* available at https://bit.ly/2KuQfGG

[80] On the effects of technical literacy on DFS use, see Grameen Foundation (2013) *Use Of Mobile Financial Services India And The Philippines,* available at https://bit.ly/2KuQfGG

[81] 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.

[82] For example, of the 300,000 DFS clients of Bank South Pacific, only 3,000 use smartphones to access services.

[83] GSM was the digital successor to first generation – or '1G' - analogue and the largely insecure mobile networks introduced in the 1970s.

networks.[84] MAP in turn operates over Signaling System 7 (SS7),[85] a communication technology used by most telecommunication network operators around the world to allow their mobile and fixed line networks to interact and for mediating multiple voice calls used on the GSM 'traffic' channel.[86] The approach of regulators to development of mobile infrastructure is usually mediated by enquiries into market structure, investment and competition issues.[87] The design of policies is further complicated by trade-offs between short-term and long-term policy objectives.[88]

**NTA ROLE:**
Type approvals; Base station site approvals; Technology mandates; Universal service mandates; Broadband policy.

## A1 NARROWBAND MOBILE DATA TECHNOLOGIES

**2G technologies:** The initial GSM incarnations from the early 1990s to early 2000s were characterized by 'narrowband' or low-speed Second Generation (2G) technologies that used data transport mechanisms - technically known as 'bearers' - such as USSD, SMS, General Packet Radio Service (GPRS) and variations of Enhanced Data for Global Evolution (EDGE). USSD and SMS are SS7-based technologies that use the signaling channel of GSM, while GPRS and EDGE are Internet Protocol (IP)-based.[89] Importantly though, USSD and native SMS data is unencrypted and thus effectively in unencrypted clear text, an innate artifact of its SS7 pedigree.[90] The GSM specifications, however, use encryption standards for the wireless transmission of data, although these have all been, to some extent, compromised.[91]

**GPRS** is an IP-based technology used to upgrade GSM networks that use expensive and slow, time-based Circuit Switched Data (CSD) to access data.[92] GPRS allows subscribers to stay connected to any online data on the Internet and to be billed per data unit (in megabytes or gigabytes) [93] rather than to be billed in

[84] Mobile Application Part (MAP) is a SS7 protocol that provides an application layer for the various nodes in GSM, GPRS, EDGE, UMTS and HSPA mobile core networks to communicate with each other in order to provide services to users. MAP is the application-layer protocol used to access the Home Location Register, Visitor Location Register, Mobile Switching Centre, Equipment Identity Register, Authentication Centre. USSD messages travel over MAP within the core network of the MNO.
[85] SS7 was developed in 1975 and standardized in the 1980s in the ITU-T Q.700 series. SS7 itself is not secure however, as it was designed in the 1970s with no real authentication and intrusion-prevention in mind.
[86] This signaling mediation allows multiple calls to efficiently take place on a known frequency without overlap.
[87] On the role of mobile coverage on DFS and a discussion on how infrastructure is developed, see Perlman, L & Wechsler, M (2018) *The Role of Mobile Coverage on Digital Financial Services*, available at www.dfsobservatory.com
[88] Bauer, J (2010) *Regulation, public policy, and investment in communications infrastructure*, available at https://bit.ly/2OdfDRR

[89] IP is the principal communications protocol in the Internet protocol suite for relaying data. IP has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers. Its routing function enables internetworking, and essentially establishes the Internet.
[90] Curiously, no authentication was built in into the original SS7 protocols, nor even when ETSI and the 3GPP added new protocols in the 1990s and 2000s to support mobile phone services.
[91] Vijayan, J (2010) *Researchers Use PC To Crack Encryption For Next-Gen GSM Networks*, available at https://bit.ly/2rebrsa
[92] CSD data access is billed per minute compared to always-on systems like GPRS, EDGE and 3G or 4G which charge according to how much data is transferred.
[93] GPRS and the other data facilities are billed in data units like megabytes or gigabytes of use by the MNO.

units of time.[29] EDGE[94] is a bolt-on[95] enhancement for 2.5G GSM/GPRS networks that makes it easier for existing GSM networks to upgrade to it.[96] The majority of mobile phones in developing countries use EDGE.

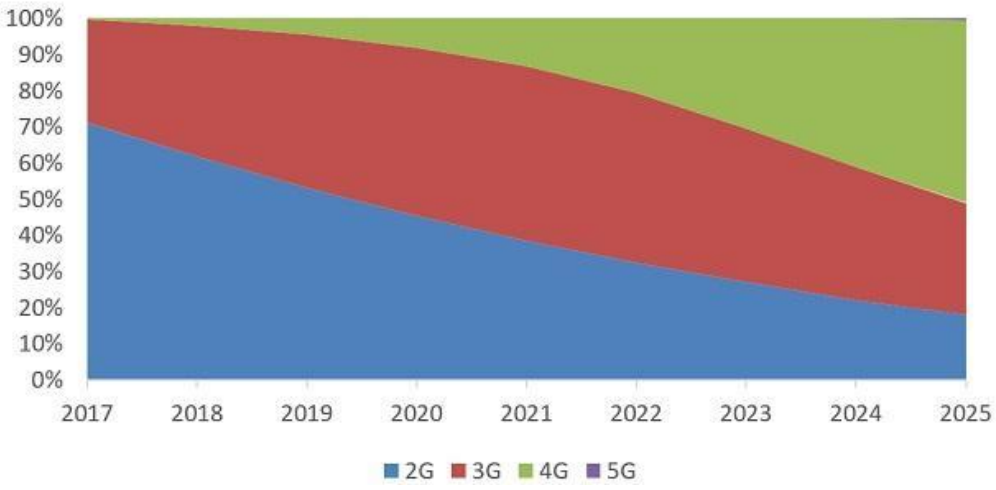



**Exhibit 6**: Current and projected share of mobile technology usage in Bangladesh. The majority of these connections are narrowband 2G-based, even though there is substantial 3G and higher broadband coverage. This is reportedly primarily due to the lack of use of affordable 3G and higher-capable mobile handsets due to high levels of taxes and fees. [97]

## A2 Broadband Mobile Technologies

**3G Technologies:** Higher-speed IP-based Third Generation Mobile (3G) technologies developed in the 1990s are based on Wideband Code Division Multiple Access (W-CDMA) technology that manifests itself in variations of Universal Mobile Telecommunications System (UMTS) and its successor, High Speed Packet Access (HSPA). 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 existing 3G mobile telecommunication networks utilizing the WCDMA protocols.[98]

**4G Technologies:** The current mobile broadband data evolution is at Fourth Generation (4G) technology, manifesting as Long Term Evolution (LTE) and LTE Advanced (LTE-A). LTE, based in part on UMTS/HSPA network technologies, was developed by the 3GPP and is specified in its Release 8 document series. [99] The first commercial deployment was in Sweden in 2009. LTE increases the capacity and speed over UMTS/HSPA by using a different radio interface together with core network

[94] This is known also as Enhanced GPRS (EGPRS).
[95] 'Bolt-on means that the MNO system can be upgraded via a software upgrade rather than by installing entirely new hardware to provide the intended result.
[96] EDGE is a superset to GPRS and can function on any network on which GPRS is deployed. It is substantially faster than GPRS, but is much slower than 3G
[97] See GSMA Intelligence (2018*) Blog: Why is Bangladesh experiencing tepid 4G uptake?,* available at https://bit.ly/2Iqtcvh
[98] A further improved 3rd Generation Partnership Project (3GPP) standard, Evolved High Speed Packet Access (also known as HSPA+), was released late in 2008 with subsequent worldwide adoption beginning in 2010.
[99] 3GPP (2018) *LTE*, available at http://www.3gpp.org/technologies/keywords-acronyms/98-lte

improvements. LTE Advanced (LTE-A) is a major enhancement of the LTE standard, which includes the Voice over LTE (VoLTE) standard.

Universal Broadband Service[100] represents a national attempt to provide broadband access across the widest area possible within a country to ensure that all residents receive an adequate level of service, enabling them with the ability to participate meaningfully in society.[101] Broadband policy is often set by the NTA, other times with an ICT-type ministry, or a combination of both.[102]

There is no single universally defined 'broadband' speed as it is a constantly evolving baseline measure of service set and defined within each country. Levels, both up and downstream, are set forth in statute and/or regulation and usually increasing.[103] In developed countries such as the US, wireless broadband speed has recently been redefined as a floor of 25 Mbps.[104] In contrast, the floor for which mobile broadband services has been redefined in India as 512 kbps and has not changed since 2013.[105] A USF is one subsidy intended to help finance the expansion of universal service into rural areas. Another method of financing is through a PPP, which funded the Rwanda WOAN. One example of universal broadband service is the WOAN in Rwanda, which covers 95% of the population.

The UN's broadband Commission advocates[106] for national broadband policy (NBPs) and universal access and service (UAS) policies that provide regulation, financing, and access goals to ensure that a country can provide broadband services. Not all countries have national broadband plans: it reports that as of the end of 2016, 151 countries had a NBP, 7 were planning on one, and 38 had not yet developed one.

**Exhibit 7:** The Evolving Nature Of Broadband

**5G Technologies:** 5G mobile data technology is touted as a major evolution in mobile data and coverage, promising mobile data speeds of up to 20 gigabits per second and intelligent allocation of bandwidth

[100] Also referred to as 'broadband universal service' and related to the concept of 'universal service.'
[101] Also see European Parliament (2016) *Broadband as a universal service*, available at http://bit.ly/2qWdNeB
[102] See for example India, where the NTA TRAI has set out the parameters for broadband. See Economic Times (2018) *TRAI Issues Consultation Paper on National Telecom Policy 2018*, available at https://bit.ly/2IFeUKw. Similarly in Malawi, the NTA MACRA held talks with industry on a draft broadband strategy. The Nation (2018) *Broadband Strategy To Address Internet Gaps, Says MACRA*, available at https://bit.ly/2rLT5OY
[103] Baseline levels of service defined as 'broadband' are often set by government or a regulator, according to the type of service (fixed line, wireless, satellite, etc.), and described in terms of 'upstream' and 'downstream' speeds to and from a telecommunications provider. In the US, no floor is specified but thresholds are required to be periodically set by a regulator or through national broadband programs such as for disbursements pursuant to a Universal Service Fund. Kruger, L G (2017) *Defining Broadband: Minimum Threshold Speeds and Broadband Policy,* available at http://bit.ly/2JlcVrr. See also FCC (2018) *Broadband Speed Guide*, available at http://bit.ly/2HohZe9
[104] FCC (2018) *ibid.*
[105] See Telecom Regulatory Authority of India (2017) *Consultation Paper on Data Speed Under Wireless Broadband Plans, Consultation Paper No. 6 /2017*, available at http://bit.ly/2HULB3z; Telecom Regulatory Authority of India (2018) *Consultation Paper on Inputs for Formulation of National Telecom Policy - 2018*, available at http://bit.ly/2vEH2YJ. MNOs such as BSNL have been offering minimum broadband speeds of 2 Mbps. BSNL TeleServices (2017) *8Mbps Is BSNL Broadband New Speed As Minimum Bandwidth*, available at http://bit.ly/2HpnXza . There is reluctance to raise the floor due to compliance issues with quality of service requirements and pressure from MNOs to avoid issues which arise in rural areas and edges of the network. See Telecom Regulatory Authority of India (2018) *Performance Indicator Reports*, available at http://bit.ly/2K9bk9b
[106] The UN Broadband Commission's advocacy Target 1 states that: 'All countries should have a National Broadband Plan or strategy or include broadband in their UAS definitions.' See World Bank (2016*) ICT for Development*, available at https://bit.ly/2rLtZ3k

across multiple devices. The first of several 5G specifications were finalized in December 2017,[107] and there are as yet no handsets or mobile networks providing commercial 5G services.[108] Improvements in antenna technology in 5G-compatible phones and base stations[109] using focused antenna arrays may improve mobile coverage.[110]

**5G Technologies:** 5G mobile data technology is touted a major evolution in mobile data speeds of up to 20 gigabits per second, coverage improvements, and intelligent allocation of bandwidth across multiple devices. The first of several 5G specifications were finalized in December 2017[111] and there are, as yet, no handsets or mobile networks providing commercial 5G services.[112] Improvements in antenna technology in 5G-compatible phones and base stations may improve mobile coverage.[113]

## B CUSTOMER DEVICES

### 4.3 Mobile Devices Used in DFS

#### 4.3.1 Overview

The predominant types of mobile handsets in DFS markets that serve those at the Bottom of the Pyramid (BOP) are what are now known as 'basic' phones and 'feature' phones, with some DFS markets showing increases in smartphone penetration. [114] Mobile phone evolution over the past few years has, to some extent, rendered distinctions between these device categorizations somewhat fuzzy.

**NTA Role:**
SIM card registration procedures; Mobile Phone Approvals; Phone QOS; Anti-Fraud and Anti-counterfeiting measures.

#### 4.3.2 Basic and Feature Phones

As noted above, basic phones, also called 'low-end' or 'dumb phones', have limited feature sets, limited or no factory-installed or user-installable value added third party applications, and very limited or no data connectivity.[115]They can, for the most part, access DFS platforms through the use of basic USSD and

---

[107] 3GPP (2017) *Release 15*, available at http://www.3gpp.org/release-15, ITU (2017) *ITU towards 'IMT for 2020 and beyond*,' available at https://bit.ly/2qS0fBl
[108] Cheng, R (2018) *What is 5G? Here Are The Basics*, available at https://cnet.co/2nRYuC2
[109] This study uses the term 'mobile base station' to refer to the situs of the access network, which is also commonly called a 'cell site' or 'cell tower. https://bit.ly/2rgrDbH
[110] See Section 7.5.3.2 on innovations in 5G.
[111] 3GPP (2017) *Release 15*, available at https://bit.ly/2GrQTS6; ITU (2017) *ITU Towards 'IMT for 2020 and beyond*', available at https://bit.ly/2qS0fBl
[112] Cheng, R (2018) *What Is 5G? Here Are The Basics*, available at https://cnet.co/2nRYuC2
[113] For example, '4x4 MIMO' technology places four antennas in one phone.
[114] 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 v1 functionality, and a phonebook - were needed (and available) to communicate. Some basic devices could however receive VAS such as ringtones via Over The Air (OTA) installation.
[115] On the types of handsets available in DFS, see a comprehensive review of their utility in DFS in Perlman, L (2017a) *Technology evolution and innovation in DFS*, available https://bit.ly/2CEufrm; and Perlman, L (2017b) *Technology Inequality: Opportunities And Challenges For Mobile Financial Service*s, available at https://bit.Ly/2r7nzny

STK feature sets. Feature phones are the dominant types of phones in DFS.[116] They have more functions than basic phones but still have limited functionality and proprietary operating systems (OS) by comparison to smartphones. Not all feature phones support third-party software but, if they do, they are usually run on Java or similar or made for the proprietary OSs of the feature phone. These devices have touchscreens and offer a better UI than the USSD and STK UIs used on basic and feature phones, as well as providing increased bouquets of service offerings.

### 4.3.3 Smartphones:

Market surveys and projections[117] indicate that smartphone penetration is increasing worldwide. However, in many DFS-focused markets, non-smartphone phones are in majority use. As noted by CGAP,[118] smartphone UIs can make basic transactions simpler and potentially address a host of other identified barriers to active use. These improvements include more intuitive icon-driven menus that address the culture of the customer, are alongside more assuring information such as the ability to confirm transactions and easily correct input errors, provide real-time pricing information as well as transaction logs. Location-relevant maps of the nearest agents with sufficient e-money or cash floats may also provide incentive to use services and save on walking. Self-onboarding with basic KYC may also be possible.[119]

### 4.3.4 Phone Approvals and QOS

In many countries, the NTA will undertake what is known as type-approval testing of mobile handsets. Only after a type approval for a particular handset is approved can it be legally distributed and sold in that country. In some cases, approval is granted after the testing of a handset is undertaken by the NTA or its contracted entity or approval is given once the handset manufacturer/distributor issues a 'Declaration of Conformity.'[120] In, India, the Telecommunication Engineering Center (TEC) of Ministry of Communications undertakes interface approval and provides approval for mobile handsets of MNO equipment and its interface for which 'TEC Interface Requirements' are available. The approval is granted after evaluating the sample of product for compliance.[121] In Pakistan, however, a complex procedure to get an approval or 'no-objection certificate' from the Pakistan Telecommunication Authority has reportedly led to an increase in fake handsets, although this has suppressed the import of Chinese-made handsets by 40%.[122]

---

[116] GSMA (2015) *From Feature Phones To Smartphones, The Road Ahead,* available at https://bit.ly/2wJ0EM8

[117] See for example GSMA (2016a) *op. cit. 32* which projects a majority global smartphone penetration by 2020. For a countervailing view on the rate of smartphone penetration, see Perlman, L (2017) *Technology Inequality: Opportunities and Challenges for Mobile Financial Services*, available at https://bit.ly/2r7NZNy; Perlman, L & Yoo, P (2017) *Mobile Handset Use In Digital Financial Services*, available at https://bit.ly/2rbHMiG

[118] Chen, G (2016) *The Power of Smartphone Interfaces for Mobile Money,* available at https://bit.ly/2rq6Ram

[119] See further, Villasenor, J (2013) *Smartphones for the Unbanked: How Mobile Money Will Drive Digital Inclusion in Developing Countries*, available at http://brook.gs/2bpciPe; Almazán, M & Sitbon, E (2014) *Smartphones & Mobile Money: The Next Generation Of Digital Financial Inclusion,* available at https://bit.ly/2rk9n1o; Tyler, E (2015) *Smartphone-Led Digital Finance: Three Areas to Watch*, available at https://bit.ly/2HmaAA7

[120] See for example the 'Declaration of Conformity' for handsets and other telecommunications equipment by the Ghanaian NTA, at National Communications Authority (2015) *The Type Approval Guidelines*, available at https://bit.ly/2jHyaJc

[121] See Telecommunication Engineering Center, Ministry Of Communications (2018) *Interface Approval*, available at http://www.tec.gov.in/interface/

[122] Daily Times (2016*) Import of Chinese mobile phones drops by 40%*, available at https://bit.ly/2rNKTO7

Some countries are planning on specific QOS standards – other than SAR values[123] - for handsets. In Kenya for example, the Communications Authority of Kenya released a draft document on proposed minimum features and technical specifications for mobile cellular devices to be sold in Kenya.[124]

### 4.3.5 Anti-Counterfeiting and Anti-Theft Measures.

#### 4.3.5.1 Overview

Intersecting with issues of AML and security is the growing problem of counterfeit phones and the resetting of identifying characteristics of stolen phones to allow for resale.[125] These issues may affect provision of DFS[126] The counterfeit phones on the exterior have the look and feel of popular of expensive brands but do not run the operating system of the brand.[127] These phones – often called 'Shanzhai,' or 'bandit' phones – have been estimated at 15-20% of the global market in terms of units sold, and about USD 9 billion in revenue.[128]

Other risks include bad actors resetting the 15-digit unique International Mobile Equipment Identity (IMEI) number[129] on a (stolen) phone to a set of zeros or some other random 15-digit number. The IMEI number of a phone[130] is important as it allows an MNO to remotely configure the phone with correct network access settings[131] as well as blacklist[132] or 'graylist'[133] a phone if that IMEI number is that of a phone which has been reported stolen.[134]

The problem is growing: Asian, Middle Eastern, and African[135] authorities have been confiscating fake devices, or devices that have zeroed out IMEI numbers. From MNO Tigo's estimation, 10% of the device types on its networks cannot be identified, mostly in Chad (63%) and Senegal (15%).[136]

---

[123] Specific Absorption Rate is, in general, related to the amount of energy a mobile phone emits. The lower SAR value the better.

[124] Phones sold must have at least one-year's warranty, have the manufacturer's identification mark and model printed on the mobile cellular device in indelible ink, readily visible and legible. Each device must have a unique International Mobile Station Equipment Identity (IMEI) assigned by GSMA. The IMEI must be printed on the device and should be retrievable electronically by dialing *#06#. Phones must have a minimum talk time of 8 hours and be equipped with a wired or a wireless earpiece interface that complies with CA's guidelines on the use of short-range devices. CA (2017) *Features And Technical Specifications For Mobile Cellular Devices Sold In Kenya*, available at https://bit.ly/2HWdX0N

[125] Similar issues include counterfeit phone components such as displays and batteries.

[126] These have an impact on AML, tax revenue, QOS, security of infrastructure and consumer protection.

[127] In Bangladesh for example, a popular fraud is to encase a fake BlackBerry with an original Blackberry casing.

[128] EC (2012) *Study On Internationalization And Fragmentation Of Value Chains And Security Of supply*, available at https://bit.ly/2ImmYR6

[129] The IMEI code style must correspond to the code specified by the GSMA document DG06 (TW.06) - IMEI Allocation and Approval Guidelines. See GSMA (2011) *IMEI Allocation and Approval Guidelines*, available at https://bit.ly/2IrcBay

[130] The IMEI number is transmitted to the MNO when the phone connects to that MNO.

[131] 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 MNO/SP cannot determine what type of handsets being used - it may not be able to send the correct OTA configuration and/or update settings to the handset.

[132] With blacklisting, the MNOs will block a phone on its stolen phone database from being able to operate on its network.

[133] With gray listing, the MNOs will monitor the use of the phone, with a view to catching the holder of the stolen phone.

[134] To circumvent the blacklisting or gray-listing, bad actors can use off-the-shelf technology to easily reset the IMEI with a fake number or simply to insert zeros in place of the original IMEI number.

[135] Standard (2016) *Sh5.2m fake Samsung phones seized in Mombasa*, available at https://bit.ly/2INa1iz

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

It appears however that in some markets some NTAs lack the mandate to disable counterfeit and stolen phones. The Uganda Communications Commission for example procured equipment and drafted policies to secure the legal backing for the planned action, but still lacks a legal mandate for a mass switch off.[137] A mass switch-off would have far-reaching legal implications for the country if it's not supported by law.[138]

#### 4.3.5.2 Country Example

**India:** In 2017, the department of Telecommunications implemented a Central Equipment Identity Register (CEIR) that connects to the EIRs of all licensees in India.[139] The CEIR will have standard white list, grey list and blacklists.

**Kenya**: In 2011 the Communications Commission of Kenya gave a notice to all MNOs to phase out counterfeit handsets on their networks. Some 1.9 million counterfeit mobile phones were phased out after 30 September 2012. A handset verification system was established to enable subscribers to verify the validity of their phones through submitted IMEI numbers. In Tanzania, the Tanzania Communication Regulatory Authority has since June 2016 has blocked 1.82 million counterfeit phones using a GSMA database of fake IMEI numbers.[140]

**Nepal:** The Nepal Telecommunications Authority has set up a register of IMEI numbers of mobile devices integrated into MNO databases. It is also blocking unregistered numbers if they do not comply with the rules within the mandated time frame. People who bring mobiles from abroad for personal usage will also be required to register.[141]

**Nigeria:** The Nigerian Communications Commission indicates that about 250 million fake or reset phones were sold in 2014 in the country.[142] Some 10% of the phones in the country are counterfeit or reset.[143] In June 2016, the Standards Organisation of Nigeria (SON) began prosecuting sellers of fake and substandard mobile phones and accessories. Any phone not registered with the SON will be seized and offenders prosecuted.[144]

**Oman**: The Telecommunications Regulatory Authority launched a new automated program that enables consumers to identify fake mobile devices. Buyers can send the 15-digit IMEI number on the product's box to 80566, and the system will check if the phone is registered in the EIR database of the GSMA.[145]

---

[137] The draft policy was submitted to the Ugandan parliament in 2012 but nothing has passed to date. See Uganda Radio Network (2016) *UCC Pushes for Legal Backing to Disable Fake Phones*, available at https://bit.ly/2rOa9Ui. See also on recent UCC initiatives on stolen phones, KFM (2018) *UCC Steps Up Efforts To Deactivate Counterfeit Phones*, available at https://bit.ly/2L2DoeS

[138] For MNOs, a mass switch-off of phones would result in a mass drop off in customers and thus (telecommunications-related) revenue. See section 4.4 on effects on DFS.

[139] Department of Telecommunication (2017) *Central Equipment Identity Register*, available at https://bit.ly/2InWOt3

[140] BBC (2016) *Tanzania 'cuts off 630,000' fake phones*, available at https://bbc.in/1Qd4Reg

[141] Kathmandu Post (2016) *NTA's IMEI Registration Plan Set To Face Delays*, available at https://bit.ly/2IJ5zBo

[142] Naira Land Forum (2015) *250 Million Fake Phones Sold In Nigeria Yearly* – NCC, available at https://bit.ly/2wLANDc

[143] Federal Ministry Of Communications (2015) *Telecom Companies To Switch-Off Fake Phones From Networks — SON*, available at https://bit.ly/2Kv32bc

[144] Punch (2016) *SON To Prosecute Substandard Phone Sellers*, available at https://bit.ly/2Ine95u

[145] Times Of Oman (2016) *Oman Launches Programme For Identifying Fake Mobile Devices*, available at https://bit.ly/1VXGEbZ

**Uganda:** A study by the Uganda Communications Commission indicates that about 30% of Uganda's estimated 17 million mobile phones are Chinese-made counterfeits. The government loses about UGX 15 billion (USD 4 million) in tax revenue to counterfeit mobile phones.[146]

**Supra-national Initiatives:** At a more supranational level, there are moves to create a global system for exchange of unique telecommunication/ICT devices identifiers in line with the ITU's TDC-14 Resolution 79 and PP-14 Resolution COM 5/4.[147] The ITU deems 'counterfeit' to include counterfeit and/or copied devices and equipment as well as accessories and components. The GSMA database for now serves this purpose: it provides access to the database to 3GPP network operators, device manufacturers and qualified industry parties.[148]

### 4.4 Effect on DFS

The effect of blacklisting phones at the DFS level includes the handset being prevented from accessing a MNO network and without notice to the user. The indirect effect on DFS is that users will, albeit temporarily until they get a new phone, be unable to access to their funds. The device is also rendered unable to receive proper network access settings OTA from the MNO/SP due an inability to properly identify the phone brand and model. If a DFS customer's phone is blacklisted without notice, access to stored DFS funds may be cut off.

The blacklisting of mobile phones has happened in several countries following instructions from national authorities to MNOs to turn off, en masse, phones with identical or zeroed IMEI numbers. Customers lose the value of their blocked phone and must then purchase a new phone and place their SIM card in a new phone re-access their DFS accounts.

Additional effects of phones with fake IMEI numbers, zeroed IMEI numbers or which are counterfeit include:

- Inability to get OTA updates from MNOs/SPs to correctly set up – 'provision' - the phone
- Performance degradation
- Confiscation of the handset by authorities
- Failed warranty and technical support
- Potential for blocking of the mobile handset for use on the MNO by a regulator/industry blacklist preventing access to DFS-based funds
- High percentage of dropped calls
- Access failures to networks
- Handover problems
- Low reliability
- Battery explosions

---

[146] KFM (2018) *UCC Steps Up Efforts To Deactivate Counterfeit Phones*, available at https://bit.ly/2L2DoeS
Protsenko, D (2014) *Regulatory Procedures And Solutions For Protecting The Market Against Counterfeit/Substandard Terminal Equipment In Ukraine*, available at https://bit.ly/2ItgDiv

[147] ITU (2014) *Resolution 79: The Role Of Telecommunications/Information And Communication Technologies In Combating And Dealing With Counterfeit Telecommunication/Information And Communication Devices*, available at https://bit.ly/1umNjNs

[148] See GSMA IMEI database: https://imeidb.gsma.com/imei/login.jsp

- Potential hazard to health through high Specific Absorption Rates (SARs)
- Increased incidences of malware, spyware and viruses

## C USER INTERFACES & TELECOMMUNICATION SERVICE BEARERS FOR DFS ACCESS

**NTA Role:**
Pricing of Bearers; QOS; Competition Intervention; Shortcode allocation;

### 4.5 Overview

#### 4.5.1 Native Phone Interfaces

**GSM Voice Channel:** The GSM voice channel[149] uses the traffic channel component of GSM, and was the original method of access to basic non-voice transactional services offered by MNOs and other SPs. Users could, for example, access infotainment-type menus and general services by simply dialing special Interactive Voice Response (IVR) numbers linked to infotainment services provided by VAS SPs.[150]

The latest use of the voice channel for DFS purposes is for NSDT which uses the speaker and microphone of a merchant Point of Sale (POS) devices and a user's mobile handset to silently exchange payment information in merchant payments.

**Short Message Service:** Short Message Service (SMS) – also known as 'text messaging' – was designed in the 1980s to act as a data bearer for mobile network system engineers developing and maintaining the initial version of GSM systems.[151] From these beginnings, text messaging has become a ubiquitous consumer-facing P2P messaging facility. An SMS sent by a user from their mobile handset is known as a Mobile Originating (MO)-SMS, or MO, to signify that the message originated on a mobile handset. An SMS received by the user on their handset (whether it be from another person or from an automated machine) is known as MT-SMS, or simply MT, for to indicate that an SMS has terminated on a mobile handset. Unencrypted 'plain text' SMS in relation to DFS is primarily used for transaction notifications, 2-factor authentication using one time passwords. Encrypted SMS is used in STK and Java applet-based DFS transactions.

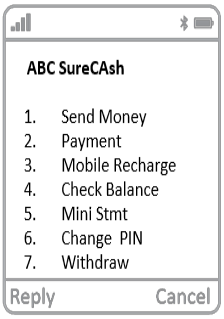
**Unstructured Supplementary Service Data**: USSD is a novel standard within the GSM and 3G specifications. As with SMS, USSD is an artifact of the original 1980s GSM specification used by MNO engineers to send and receive test messages over GSM networks without interrupting customer calls. It is

[149] During a GSM call, speech is converted from analogue sound waves to digital data by the phone itself, and transmitted through the mobile phone network by digital means.
[150] They would input touch-tone codes that would supply the services either through an immediate voice response, or by the service later providing the requested service – such as a ringtone - off-band via SMS to the GSM handset. IVR as a gateway to these basic transactional services has been supplanted by use of USSD and SMS using the GSM signaling channel to access more robust transactional services such as those provided by DFS.
[151] SMS uses GSM signaling channels. The initial SMS protocol allowed users to send and receive messages of up to 160 alphanumeric characters.

both a GSM bearer technology and a DFS UI, does not require any additional installations by customers, nor does it require a IP-based data access connection by customers. As a result, USSD has been termed 'The Third Universal App.'[152] And as with SMS, USSD uses the mobile signaling channel inherent in SS7 networks. The use of USSD for DCB and DFS is shown in Exhibit 8.

As USSD is session-based, quality of the signal the phone receives and can transmit back to a mobile base station is important. USSD can then only be accessed or be consistently accessible when there is robust communication with MNO base stations.[153] Poor mobile signals and substandard antennas in some mobile phones may cause USSD session initiation and sustainability issues. Similarly, competition issues arise when an MNO competing with a SP on DFS provision, may limit that SPs access to USSD services and access shortcodes or limit the session times and menu trees.[154]

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




There are two types of USSD: Mobile Originated USSD and Network-Initiated USSD, also known as Push USSD. In the former, a user - a customer or agent, in a DFS environment - will initiate the USSD session to do a transaction or simple enquiry. In typical USSD session, this executes in increments of 20 seconds, with a typical USSD session lasting up to 2 minutes. This means that the handset cannot make or receive any voice calls during that time, a potential revenue loss given that voice calls usually cost more than (non-premium rated) USSD sessions. In the latter, the USSD session is initiated by a provider or MNO, usually in circumstances where some secondary authentication is required while the user is on a call, for say payment authentication,[155] or for use in providing VAS such as call answer advertising services.[156] In both cases data is provided to a user interface dynamically, with relatively fast access and response times. In some markets USSD is still required for DFS smartphone apps, particularly for 2-factor security authentication.

**Exhibit 8:** A USSD-based DFS transaction menu.

[152] Perrier, T, DeRenzi, B & Anderson, R (2015) *USSD: The Third Universal App*, available at https://bit.ly/2vA3Skc

[153] Mobiles handsets and base stations must transmit enough power, with sufficient fidelity to maintain a call of acceptable quality or USSD session to completion without transmitting excessive power into the frequency channels and time-slots allocated to others. Receivers must have adequate sensitivity and selectivity to acquire and demodulate a low-level signal. GSM handsets are measured by Class 1-5, with Class 1 being the highest transmitting power. See Keysite (2014) *Understanding GSM/EDGE Transmitter and Receiver Measurements for Base Transceiver Stations and their Components*, available at https://bit.ly/2rfkLwe

[154] See Section 6 below on competition issues in DFS.

[155] Here, a call center agent at a bank or a SP 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 the Boloro combination of NFC and Push USSD. 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 Network Initiated (Push) USSD session. The customer receives a NI-USSD message requesting them to respond with their PIN on their mobile handset. As soon as the correct PIN is entered, the NI-USSD session closes.

[156] USSD may sometimes be the secondary authentication mechanism in DFS. In some cases, the primary will be via an OTT smartphone application, using of encrypted STK or cleartext (unencrypted) SMS-based access to a server, with Network Initiated (push) USSD serving as the second-factor authentication, requiring the user to input the answer to a challenge question whose answer only they would know.

**SIM Toolkit:** SIM Toolkit (STK) is a popular SMS-based remote access and UI GSM technology used to provide DFS and related services to markets where basic and feature phones are the plurality. It is currently one of the most extensively and globally used mobile interfaces in DFS, other than USSD.[157] A specialized SIM to host the STK application and STK-compatible phone is required.[158] The STK will usually uses SMS as a bearer for communication with a host,[159] encrypting the (usually) cleartext SMS to/from the handset and STK server.

As with USSD, competition issues arise when an MNO competing with a SP on DFS provision, may limit that SPs access to STK-based services and access shortcodes.[160]

### 4.5.2 Application Based

**Java Applications:** A growing alternative access method for access to DFS using feature phones is to use icon-based Java applications using secure encrypted SMS communications methods installed on feature phones.[161] The menus are relatively easy to use, with an icon-based UI that makes it easier for illiterate/semi- literate users to navigate financial service menus. Unlike STK-based applets, this access method does not require the MNO to enable the application to operate on its network and the user can interact and transact with the SP with or without mobile data being available.[162]

**Feature Phone Applications:** Feature phones may operate on proprietary phone operating systems, or mass-market OSs such as those from chip manufactures Mediatek and Spreadtrum. Even so, not all feature phones support third-party software but, if they do, they're usually run on Java or similar or made for the proprietary OSs of the feature phone.[163] The most common 'application' platform across feature phones is Java through the J2ME[164] software environment.[165] Anticipated is a similar future influx of 'smarter' feature phones – for example using NFC and 3G, and with factory-installed social media applications - sold as part of a larger phone portfolio by some manufacturers.

**Smartphone Applications:** These devices provide a rich-media experience, by allowing OTT apps to be installed to access DFS and mobile banking applications, allow for NFC-based payments to merchants and for transit, and have large touch screen displays. They also facilitate greater innovation at the edge of the network by providing more processing power to the users, as well as making the DFSP far less dependent on the MNO as there is – ordinarily - no need USSD codes and there is no great prospect of

---

[157] As with USSD, STK is especially prevalent in developing nations where entry-level phones are mostly used.
[158] These commands are standard for all mobile equipment and defined by ETSI and *3rd Generation Partnership Project* (3GPP) specifications.
[159] STK as a technology can use USSD as a bearer, but it is very dependent on the STK implementation on the particular handset. Some handset manufacturers have not adequately implemented STK support for USSD however. In practice though, STK will almost always use only SMS as a bearer.
[160] See Section 6 below on competition issues in DFS.
[161] This allows end-to-end security for transactions rather than the cleartext inherent in USSD.
[162] Except if using a WAP link for application download, which requires data.
[163] These are usually standalone applications that do not necessarily integrate with other features of the phone.
[164] 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.
[165] However, this is still not ubiquitous, since some phone chipsets are emerging that do not support J2ME, but instead support application development alternatives such as MRE. MRE is implemented by system-on-a-chip (SOC) manufacturer Mediatek.

the potential of discriminatory/excessive pricing for using the USSD channels.[166] At least for some DFS customer segments, the rich media designs may enhance the UX compared to the fixed-menu text-based design of USSD and STK. At the same time, however, some caveats relating to the DFS ecosystem are present. For example, not all smartphones being sold in developing markets have 3G or 4G capabilities, often because the manufacturer wants to save on 3G chipset licensing costs.

### 4.5.3 Role of NTA

**Shortcodes:** Shortcodes are the consumer's primary access to USSD, STK or Interactive Voice Response (IVR) DFS bearer channels. The usability of these primary bearer channels is usually dependent on what specific codes the user must input into the mobile handset to allow them to access a service – the so-called Man Machine Interfaces (MMIs). In the case of access to services relating to DFS, the MMIs are specific short codes, which can be provider-specific or a generic single access number usable across all MNOs, meaning that a specific number for a specific service is the same across all MNOs.[167]

The short codes could manifest as 3, 4, 5, or even 6 digits the user will input to get direct access to a service or access to a gateway of menu items which give downstream access to a particular service. In some cases the short code could be 'split,' prefaced with a 2 or 3 digit number mandated for DFS by the telecommunications regulator or the central bank. That number is then followed by a star (*) entry, and then a 3 or 4 digital number and then a hash (#) that is directed to a specific service or DFS SP.

Mobile phone and fixed line phone numbers are generally part of a national resource, usually controlled by the telecommunications regulator as part of a national numbering plan based on the ITU-T E.164 specification.[168] Short codes, while not necessarily a direct ITU specification, are still a finite and scarce resource[169] and may be part of the national numbering plan.

While in many countries DFS access for consumer will be via a nationally mandated short code, in many others individual services may have a 3 or 4-digit short code that become the 'brand' of the provider.

Short codes can be obtained in the following ways:

**a)** Directly from the national telecommunications authority if that is the issuing authority for all short codes.[170]

---

[166] USSD may however be required even with smartphone app use, for example by the use of Network Initiated (NI/Push) USSD for 2 factor authentication for security in financial/banking applications. In Rwanda, the smartphone DFS apps still use USSD, which the MNOs there say speaks to market demand for a 'familiar' interface. For technical details on NI-USSD, see Perlman, L (2017b) *Technology Inequality: Opportunities And Challenges For Mobile Financial Service*s, available at https://bit.Ly/2r7nzny

[167] Technically these are referred to as 'Common Short Codes,' usually cross carrier short numbers used to address USSD, SMS and MMS messages from mobile phones or fixed lines.

[168] Numbering plans may be part of the E.164 ITU Recommendation called the international public telecommunication numbering plan that defines a numbering plan for the world-wide public switched telephone network (PSTN) and some other data networks. E.164 defines a general format for international telephone numbers. Plan-conforming numbers are limited to a maximum of 15 digits, excluding the international call prefix. See ITU (2010) *Recommendation E.164 (11/10),* available at https://www.itu.int/rec/T-REC-E.164-201011-I/en

[169] In many countries, numbering resources used in the provision of communications services are seen as a valuable scarce national resource, finite in size whose management and administration affects the national interest.

[170] In India, the national DFS access prefix is *99# is run by the NPCI. In Tanzania, MNOs, third party providers of VAS and users such as banks receive USSD short codes directly from the regulatory authorities. See also Mazer, R (2015) *USSD Access:*

**b)** From the MNO, who is allocated a numbering block or specific code by the national regulator.[171]
**c)** From TSPs acting as aggregators, who may themselves get the short code numbers directly from the telecommunications regulator or from an MNO who has been allocated the numbers by the telecommunications regulator.[172]
**d)** From a licensed MVNO, who may themselves get the short code numbers directly from the telecommunications regulator or from their home MNO, who in turn has been allocated the numbers by the telecommunications regulator.
**e)** Generally, choices b, c and d (above) present specific competition issues for non-MNO entities if the codes are initially allocated to the MNO. In such scenarios, the MNOs control the entire vertical chain of access, from the infrastructure to the short code allocation and access, and may result in 'refusal to supply' behavior.
**f)** If a short code is obtained via a leasing agreement with an MNO, it remains the property of the MNO. If an MNO is involved in DFS, conflicts of interest may arise such that the MNO may decide not to allocate short codes to a potential DFS competitor or delay allocation of a short code.

# 5 LICENSING, ALLOCATIONS AND SERVICE AUTHORIZATIONS

## A Mobile Service Provision

### 5.1 Overview

The purview of telecommunications regulators generally concerning matters of mobile networks includes spectrum management to MNO products, services, infrastructure and third-party providers utilizing the network and spectrum. Licensing is about structuring market entry and conduct to achieve desired competitive outcomes at each relevant layer of the market while protecting against certain technical risks such as technical interference. This may also include considerations of interconnection between telecommunications providers as well as wholesale infrastructure/service access.[173]

Separate licenses or authorizations may be needed to provide DFS-related services. When MNOs began to operate in the DFS ecosystem, NTAs were concerned that MNOs would be participating in and spending CAPEX on what they NTAs (initially) perceived as on 'non-core' activities,[174] and impacting on a MNO's ability to provide core telecommunications facilities. Most markets now allow MNOs to

---

*A Gateway and Barrier to Effective Competition,* available at https://goo.gl/za1P1C . By contrast in Kenya, licensing of USSD short code services is done by the regulatory authority, but it is the MNOs which issue the codes.

[171] In tandem with the increased popularity of short code services, there is also a growing demand for service interoperability and common codes between networks. Though many of these SMS short codes are network specific and therefore are not based on the international ITU-T E.164 standard, end-users of any network can use the same code to access the same services, if the service is accessible in their respective networks.

[172] In some cases, SPs may obtain secondary assignments from 'Network Facility Providers' and 'Application Service Providers' with primary assignments from a regulator for provision of short codes and even premium rate numbers. CA (2012) *Procedures And Guidelines For The Management Of Telecommunications Short Codes And Premium Rate Numbers In Kenya,* available at http://bit.ly/2jlOjpe

[173] On considerations of access to frequencies and telecommunications infrastructure, see Perlman, L & Wechsler, M (2018) *The Role of Mobile Coverage on Digital Financial Services*, available at www.dfsobservatory.com

[174] Non-core at least in terms of the MNO's initial service license. That is, that DFS activities by MNOs may fall into some telecommunications licensing regime beyond just the provision of telecommunications-only services.

provide DFS, although some NTAs still prohibit MNOs from directly participating in DFS except to provide bearer and agent services to banks and DFSPs.

**Role of the NTA:**
VAS authorizations; Spectrum allocations; MNO Licenses; Tower Authorizations

## 5.2 Role of NTA

### 5.2.1 Licenses to Operate

For provision of mobile-based services, license types are usually designated by law. Service types are often termed 'class licenses.'[175] For example, there may be individual spectrum licenses and individual service licenses. License terms are specified by regulation and generally include the type of service which can be provided using a specified frequency band;[176] the technologies which can be used;[177] the duration of the license; and coverage obligations.[178] VAS licenses may also be added in any addenda to a license.

Some revised NTA licensing approaches favor a generic license – often called a 'unified' or 'converged' license – for all providers of telecommunication services, regardless of what technology they deploy or services they ultimately offer through their telecommunications facilities.[179] This is related in some measure to the concept of 'technology neutrality'[180] where licensees can transfer any type of data across their network without differentiating between the service and data types.[181]

The duration of licenses varies depending upon license type but most individual licenses will consist of 15-20 year terms with potential rights of renewal.[182] Renewal terms vary and must be determined in

[175] ITU (2000) *Telecommunications Regulation Handbook*, available at https://bit.ly/2Gng9sw
[176] For example, mobile communications.
[177] Specifying usable technologies within a license may act to prohibit an MNO from upgrading their network to a new generation of technology over the duration of the license and upgrades to new technologies may require an additional license. As applicable to DFS, an MNO possessing a license to provide narrowband-based 2G service may not be permitted to operate a mobile network upgraded to 3G technology without an application for a new 3G license.
[178] Massaro, M (2017) *Next Generation Of Radio Spectrum Management: Licensed Shared Access For 5G*, available at http://bit.ly/2HVz0gy
[179] Under a converged license framework there are two major principles: technological neutrality and services neutrality. For a discussion of converged licenses, see Narayan, A (2007) *Overview of Regulatory Challenges in the Converged Telecommunication/ICT Environment*, available at http://goo.gl/32OlY. In 2005, the Tanzania Communications Regulatory Authority introduced the Converged Licensing Framework. See ICT Regulation Toolkit (s.d.) *Tanzania – The Converged Licensing Framework*, available at https://bit.ly/2Ktlelr
[180] Many unified and converged telecommunications licenses cover the open-ended range of services plus infrastructure in a vertically integrated manner. Where this is so, the license structure isn't directly relating to net neutrality, which concerns discrimination against third party services running across the licensee's network. Some new licenses follow a horizontal layered approach, applying only to infrastructure, which is partly intended as a tool for dealing with net neutrality.
[181] Blowers, A (2010) *'Net Neutrality: Ofcom Briefing for Analysts 21st July 2010'*, available at http://goo.gl/t8j8d
[182] Lengths of this duration are necessary to provide MNOs with the belief that an adequate return on investment will occur versus taking a high risk of not recovering the investment from a shorter duration. In the EU and in many parts of the world, spectrum licenses of a 15 to 20 year duration are common. Recent efforts have been underway to increase licensing duration (such as Sweden, cite GSMA) but a 25 year licensing plan was recently rejected by over a dozen member states, citing that it would stifle innovation. See thereto, Stupp, C (2017) *Member States Reject Commission Plan For 25-Year Spectrum Licences*, available at http://bit.ly/2FaHTQz; Spectrum licenses have often been auctioned for 15-20 years as standard although Sweden has implemented a 25 year license duration with the EU seeking to do the same. GSMA (2017c) *Effective Spectrum Pricing: Supporting Better Quality And Affordable Mobile Services*, available at http://bit.ly/2Hm73h2

advance by necessity to avoid risks of interruption of service and postponement of approvals.[183] Limitations on and requirements of spectrum usage may be contained within a spectrum license, such as a levy specifying the percentage of a MNO's gross revenue or net profit to be contributed to a fund such as for universal service.[184] Accompanying requirements may include the need to provide a specified level of QOS to possess a MNO license or for a specialized type, such as to provide backhaul and backbone services. License renewals offered may also contain similar additional requirements.

Some jurisdictions allow Mobile Virtual Network Operator licenses, which entitles licensees to buy at bulk, wholesale rates, turnkey mobile services – data, voice, SMS, USSD – from mobile infrastructure licenses services. The MVNO will usually own some SMSCs and other gateways but usually does not own any spectrum or base station infrastructure. It then markets and sells mobile services under its own brand, sometime competing with the MNO it buys services from.[185]

### 5.2.2 SIM Card Distribution and Registration

Most of the mobile phones in use today use what is known as the Subscriber Identity Module or SIM card,[186] a 1970s technology that allows and mediates access to MNO services.[187] SIM cards are generally low-cost plastic cards with a special embedded SIM access chip embedded and available for sale at agents and retail outlets. Usually access to MNO services is as simple as inserting the SIM card into a compatible phone.[188] In many countries customer identification and verification (CIV) regulations issued by the NTA require that the customer provide verifiable forms of identity to the agent or merchant before the SIM card is activated for use on an MNO.[189]

---

[183] Spectrum renewals are generally handled as (i) a presumption of renewal based upon certain conditions, e.g. a circumstance or the requirement a different service, annual fee or technology be used.to qualify; (ii) an invitation to bid for another term against competitors; (iii) an inability to renew resulting from reassignment of spectrum to another user by an authorized authority. GSMA (2015) *Best Practice in Spectrum License Renewals*, available at http://bit.ly/2qSnBqJ

[184] The concept of universal service is to assist under/unserved areas by providing access to telecommunications services such as funding the extension of mobile coverage into rural and remote areas and providing universal broadband service. The USF is often run by an autonomous agency or entity or agency administered by a management board and is designed to act independently, although this may not always be the case in practice.

[185] MVNO from banks include Equitel by Equity Bank in Kenya, and First Connect by First National Bank in South Africa. There are various MVNO permutations, some of which may reach the switch level of complexity and implementation.

[186] A SIM is a smart card with a chip that has an internal digital processor and storage capacity, and it contains specific digital imprints or keys that determine a user's access rights to the relevant MNO, and sometimes also to a range of services like DFS. These may include digital keys for data encryption that is done on the SIM using a STK data session using a specific encryption program embedded in the SIM. The SIM may also contain small applications – called 'apps' or 'applets' – that are preprogrammed by the MNO at the factory or updated wirelessly once the SIM is inserted into a phone. These apps may be secure banking applications or some other VAS that will appear on the handset screen with its own menus and functionality when that SIM with that app is placed in the mobile handset.

[187] In the 3G environment, the SIM card is known as the Universal SIM (USIM), and uses what is known as the Third Generation Partnership Project (3GPP) set of mobile data standards.

[188] A SIM card has what is known as an International Mobile Subscriber Identity (IMSI) number programmed into it that provides a unique identifier to the MNO when inserted into a compatible phone. Based on the IMSI, the MNO will allocate a specific phone number to the handset. Similarly, the handset in a GSM environment has a unique serial number called an IMEI (International Mobile Equipment Identity) number. Both the IMSI and IMEI numbers are transmitted to the MNO when the user accesses the MNO's network.

[189] See Section 5 on CIV procedures on SIM cards and DFS, and in particular, Section 5.3 describing that the Ugandan NTA banning the sale of new and replacement SIM nationally for two months due to KYC issues.

There are also 'Thin SIMs' - also known as 'Sticky SIMs' - a paper-thin plastic sheet embedded with a number of contact points and a chip on top of a standard SIM card.[190] It is used primarily for access to cheaper services from an MNO other than the SIM it is placed on, for example for roaming rates or for DFSPs to bypass restricted or unfavorable access to STK and USSD by an MNO that may be competing in DFS with the DFSP. The Thin SIM is a full-featured SIM[191] and essentially converts any handset into a dual-SIM phone.[192] Switching between the networks is done either manually via the accompanying STK menu or entering a specific short code to do the selection.[193] Because of concerns, *inter alia,* about their fragility, providers often have to seek approval from the NTA to issue thin SIMs.

### 5.2.3 Infrastructure Provision

In many cases, the NTA may set coverage requirements for an MNO. In most cases this is provided for in an MNO license based the concept of 'teledensity' and the need for universal service. With the advent of DFS though, the national financial inclusion goals and an ability to provide DFS has become another factor in determining the location of mobile base stations. To provide DFS, a minimum of 2G coverage, powering basic and feature phones, is required. In our survey of and discussions with telecommunications regulators though, it is evident that they are highly reluctant to mandate broadband coverage because of considerations of loading MNOs with debt, both in buying spectrum to provide 3G/4G, as well as the capex costs required to build out the infrastructure. Licensing provisions may also be conditioned upon satisfaction of additional requirements, such as mandatory mobile coverage areas and/or expansion, technology type and the use of infrastructure sharing where deployment may be involved.

NTAs and MNOs though are embracing the concept of sharing some or all of their infrastructure to free up capex and, through sharing or leasing of infrastructure, shift infrastructure related expenses to opex.[194] A new trend is privately owned tower/infrastructure companies that present a more efficient model specializing in resource management and servicing multiple MNOs as a profit driven business. The Bangladesh Telecommunication Regulatory Commission, for example, has mandated that only tower companies can own all mobile base station towers and then provide services to MNOs.[195] MNOs are also prohibited from laying fiber-optic cable, usually a necessary backhaul component for providing broadband.[196]

---

[190] 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. See thereto, Perlman, L (2017) *Technology Inequality: Opportunities And Challenges For Mobile Financial Service*s, available at https://bit.Ly/2r7nzny

[191] The Thin SIM supports GSMA/3GPP/ETSI standards, making it compatible with all standard devices from older feature phones to the latest smartphones. See thereto, *ibid.*

[192] Users can then access services on both networks and having two SIM cards in one slot of the device means the user does not have to physically remove and exchange the SIM card when the user travels, eliminating the possibility of losing and misplacing the cards.

[193] Invariably, the Thin SIM will listen out 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. On thin SIMs, see Perlman, L (2017) *Technology Inequality: Opportunities and Challenges for Mobile Financial Services*, available at https://bit.ly/2r7NZNy

[194] Compared to standalone deployment which is wholly owned, the components of a cellular site and its network operations can be divided into two parts: passive and active. Passive elements are primarily the physical, non-electrical components such as land, structures, power supplies, climate control and the physical mast and antenna extended from the structure. Active elements include the electronic components which transmit information from the site through the backhaul and to the core of the mobile network.

[195] Daily Star News (2017) *Telenor To Invest More, Seeks Clear Terms*, https://www.thedailystar.net/business/telenor-invest-more-seeks-clear-terms-1485118

[196] *ibid.*

Another sharing model is called wholesale open access networks (WOAN),[197] representing efforts to capitalize on the efficiencies provided by centralized deployment of infrastructure, selling equal access on the wholesale level while maintaining a competitive marketplace at retail.[198] While many variations exist, the infrastructure layer is often developed and managed by a single entity,[199] potentially in the form of a public-private partnership (PPP) which is licensed to sell to MNOs at wholesale prices on FRAND terms.[200] A primary objective of national WOANs, such as those in Rwanda and Mexico, is the expansion of mobile coverage near or at universal coverage and broadband policy levels,[201] resembling a public utility.[202] The WOAN may be licensed separately by the NTA. Opponents of WOANs such as MNOs who generally champion alternative solutions claim that they threaten competition and investment.[203] [204] In Uganda, the Ugandan Communications Commission (UCC) is providing backhaul satellite services for MNO MTN to expand 3G and higher services.[205]

### 5.2.4 Spectrum Allocation

Part of the license to operate a mobile network, usually includes provision on use – exclusive or otherwise of regulated spectrum bands. Renewal of a licensee's operating license may simply allow continued use of that spectrum at the same or different fees or may mandate the need for the licensee to provide additional services beyond that specified in their original license. Often this would mean that the licensee would have to obtain new spectrum at a set cost or through some other mechanism. The NTA may manage spectrum allocation and the NTFA,[206] spectrum assignment, and licensing to operate services. Provision of new spectrum can be allocated under a number of methods, for example beauty context, pure sale,

[197] Data from Perlman, L & Wechsler, M (2018) *The Role of Mobile Coverage on Digital Financial Services*, available at www.dfsobservatory.com

[198] Cramton, P & Doyle, L (2016) *An Open Access Wireless Market - Supporting Competition, Public Safety, and Universal Service*, available at https://bit.ly/2HmBcg7

[199] In three layered WOANs the infrastructure is owned by one party, management and maintenance is handled by a second party and retail service providers consist are the parties at the top layer.

[200] 'Open Access in a network context refers to a scenario where wholesale access is provided to electronic communications network infrastructure or services on terms that are reasonable, effective, transparent and non-discriminatory.' See South Africa's controversial open access paper, Department of Telecommunications and Postal Services (2016) *National Integrated ICT Policy White Paper*, available at https://bit.ly/2cMinI3. "…open access regulation has been seen as a way of overcoming the problems associated with the high sunk costs required of infrastructure industries that make competition in certain networks unfeasible." Gillwald, A, Esselaar, S & Rademan, B (2016) *Do Open Access Wireless Networks Threaten Competition And Investment?*, available at https://bit.ly/2vMRw8P

[201] Rwanda's WOAN and the Red Compartida in Mexico are mandated to expand coverage into rural areas and reaching 92.2% and 95.5% of the population, respectively. See also Cooper, D (2018) *A State-run Wireless Network Isn't A Crazy Idea, Just Ask Mexico*, available at https://engt.co/2FaGuJG

[202] In some cases, such as is being proposed in South Africa, a WOAN can also consist of a portion of spectrum allocated to a WOAN with the remainder provided to MNOs who are allowed to compete with the WOAN at predefined levels which, in the case of South Africa, requires 30% of the WOAN capacity being purchased.

[203] Gillwald, A (2016) *Open Access Wireless Networks Threaten Competition and Investment*, available at https://bit.ly/2nCqXKN

[204] Alternatives include voluntary infrastructure sharing, lower priced spectrum in the digital dividend, reduction or elimination of sector taxes, modest QOS requirements, and support for privately sponsored data plans such as zero rating.

[205] Satellite Today (2018) *Uganda to Boost 3G Infrastructure Deployment via Satellite*, available at https://bit.ly/2jQmnsh

[206] The NTFA may sometimes be designated to a specific and specialized authority.

various auction types[207] and administrative assignment.[208] When regulators divide spectrum, there is a trade-off between cost-effectiveness and competition but that spectrum policy and antitrust policy should be aligned.[209]

Although growing, 3G (and 4G) coverage is not ubiquitous in many DFS markets, instead, being predominant in urban areas and along national roads and their periphery. That is, compared to their 2G mobile network coverage areas, MNOs in a number of countries do not necessarily overlay their existing coverage with required Third Generation mobile coverage to power new-generation devices. MNOs may satisfy their universal services obligations imposed by regulators to cover rural areas with 2G coverage but this does not necessarily equate to universal quality of service. There is a need, however, for faster network access speeds to power the increased data speed needs of smartphones. This means that many of those possessing these devices in primarily rural areas may experience a degraded smartphone user experience.

The next arms race for MNOs and 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.[210] Lower frequencies generally mean more coverage per base station and, generally, the need for less base stations to cover a specific area. The new spectrum is part of what the ITU call the 'digital dividend,' the amount of spectrum in the frequency band 470-862 MHz to be released – 'refarmed' – as a result of the switchover from analogue to digital TV worldwide.[211] The propagation characteristics of these bands should facilitate improvements in mobile broadband coverage in rural areas for DFS, as well as better indoor coverage in more densely-populated areas since the signal at this frequency covers a larger area which means fewer base stations, and thus less capital costs by licensees.[212]

Cooperation between NTAs often extends cross-border, especially where there are issues of frequency coordination required for small neighbouring countries. For example, the Democratic Republic of Congo's telecommunication regulator Autorité de Régulation de la Poste et des Télécommunication du Congo and the NTA in neighbouring Rwanda, the Rwanda Utilities Regulatory Authority signed a MOU to cooperate on cross-border telecom-related matters that include improper frequency coordination, automatic roaming and the ability of devices to access DFS facilities.[213] Similarly, it is reported that the Zambia Information and Communications Technology Authority and the Malawi Communications and

---

[207] See further on these methods, Perlman, L & Weschler, M (2018) *Mobile Coverage And The Effect On Digital Financial Services*, available at www.dfsobservatory.com

[208] See for example in Kenya, where market leader MNO Safaricom was given 4G spectrum for free by the NTA in exchange for constructing a turnkey communication and surveillance system for the National Police Service. Daily Nation (2016) *Safaricom To Slap State With Sh9bn Bill For Security Network*, available at https://bit.ly/2ww5dJC

[209] Peha, J (2017*) Cellular Economies of Scale and Why Disparities in Spectrum Holdings are Detrimental*, available at https://bit.ly/2jPAcqH

[210] Regulators around the world are beginning to auction off or sell the freed former analogue TV frequencies, including the 700 MHz, 800 MHz, and 2,600 MHz ranges. South Africa is auctioning off the 700 MHz, 800 MHz and 2600 MHz spectra. See Engineering News (2016) *ICASA Opens Auction For Long-Awaited Spectrum*, available at https://bit.ly/2rAlMPy. In India, the regulator will be auctioning off the 700 MHz spectrum. See Indian Express (2016) *Union Cabinet Approves Mega Spectrum Auction,* available at https://bit.ly/2jOhn7o/

[211] Some markets already have phones compatible with the 450 MHz frequency spectrum. The 450 MHz band is being used by some 115 operators in 60 countries, primarily in LATAM and with CDMA networks. See GSMA (2015a) *LTE 450 MHz: Taking The Road Less Travelled,* available at https://bit.ly/2IihWRe

[212] Cartesian (2015) *Mobile Platform Access for USSD-based Applications (MPA-USSD),* available at https://bit.ly/2KHrqY1

[213] IT Web Africa (2017) *DRC, Rwanda Commit to Telecoms-focused MoU*, available at https://bit.ly/2IOkaLR

Regulatory Authority have committed to a MOU to address issues of cross-border spillover of telecommunications and broadcasting frequencies.[214]

### 5.2.5 Universal Service Funds

A Universal Service Fund (USF)[215] is a ring-fenced fund which consists of contributions made by MNOs to fund national universal service policy goals.[216] Funding is often based on MNO gross revenues less offset such as interconnection of other operators. The concept of universal service is to assist under/unserved areas by providing access to telecommunications services such as funding the extension of mobile coverage into rural and remote areas and providing universal broadband service. The USF is often run by a NTA or an autonomous agency or entity or agency administered by a management board and is designed to act independently, although this may not always be the case in practice.[217]

### 5.2.6 Effect on DFS

It is self-evident that good MNO coverage is critical to the success of DFS and its further evolution: it is in the DNA of DFS. In most cases, regulator-derived 'universal service' obligations[218] as well as commercial exigencies will push MNOs to establish national mobile coverage. Complete geographic coverage has strong momentum. Indeed, in many or most countries competitive forces push MNOs toward nationwide coverage, and regulators add further impetus through 'universal service' obligations.[219]

But not all regulators insist on universal service needing to equate to universal quality of service, meaning that 3G coverage lacks compared to 2G coverage and that some areas - although covered by 2G - may have poor QOS. 3G and better coverage is usually associated with urban areas, where there may be more disposable income for purchase of smartphones and affordability of mobile data. That means while 2G may be relatively ubiquitous in many DFS markets – albeit of possibly poor QOS - 3G[220] coverage (and its variants) is not always a given. This gap in 3G coverage topography is currently characteristic of many DFS markets in the developing world.[221]

Even universal service does not necessarily equate to universal quality of service (QOS). That is, even though USSD is a narrowband technology requiring very little MNO bandwidth to operate, it is not always certain, for example, that the edge of the mobile network coverage will be of sufficient quality to initiate and sustain a full USSD session.[222] A poor connection to a base station will invariably terminate a USSD session, forcing the user to start the transaction or query session again.[223] By contrast, STK is a store-and-

---

[214] See Smart Green African City (2017) *DRC, Rwanda Commit To Telecoms-Focused MoU*, available at https://bit.ly/2IfFc2k

[215] Sometimes called a Universal Access Fund (UAF) or other variation, covered in greater detail in Section 7.2 and 7.2.1.

[216] Universal Service is covered above in Section 4.3.2

[217] See Section 4.3.2 on USF.

[218] 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 ITU (2013) *Universal Service Fund And Digital Inclusion For All Study*, available at https://bit.ly/2Hl46x5

[219] 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 ITU (2013), *Universal Service Fund And Digital Inclusion For All Study*, available at https://bit.ly/2Hl46x5

[220] 3G hereon will mean representative coverage providing broadband speeds, including (but not technically) HSPA and 4G LTE. See Annex B for mobile phone technologies.

[221] Ubiquitous 3G/4G coverage in the developed world is of course also not a given.

[222] Cartesian (2015) *Mobile Platform Access for USSD-based Applications (MPA-USSD),* available at https://goo.gl/9nEZ9n

[223] For example, and as noted earlier, access to and sustaining a USSD session using a basic or feature phone, some fidelity of the GSM signal – to and from the mobile handset - is required.

forward communications technique based on SMS, which although sensitive to a poor signal will in many cases[224] be able to auto-initiate to (re)send a transaction message when the mobile signal is stronger.

Implementing 3G nationally becomes a major capital and opex cost - costs are derived from spectrum purchases, infrastructure purchases and deployment costs, and ongoing opex - for MNOs, who as a result may only concentrate on densely populated urban areas for provision of 3G. The frequency band of 3G coverage also affects the totality of the coverage area: higher frequencies such as (the typical) 2100 MHz 3G band will have less coverage area (range) than 3G at 900 MHz but will have more capacity than 900 MHz. Not all smartphones have 900 MHz 3G capabilities though: the norm for handsets generally is 900 MHz for 2G use and 2100 MHz for 3G use. The 3G coverage may improve of course over time, especially if the new 700 MHz frequency bands are implemented as these have better range than the current 2100 MHz coverage. This can also occur, or if MNOs are mandated to implement 3G coverage by the national regulator as part of national universal service obligations. This lack of 3G coverage and inability for users to properly use the media-rich features of smartphones means that vendors and MNOs need to cater to feature phones and USSD for the foreseeable future.[225]

These factors – the lack of availability of high quality high speed coverage, especially in rural areas – have profound implications for financial inclusion policy: for the next several years, vendors and MNOs should and are expected to continue to cater to feature phones and USSD. Without a shift to reliable 3G and 4G coverage, users will remain unable to fully utilize the media-rich features of smart phones.[226] 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 and may remain used by low income users for many years beyond. Until these 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 other DFS products, such as more innovative credit products.

## B DFS-RELATED LICENSES & AUTHORIZATIONS

### 5.3 Overview

The NTA's role as a 'pure' telecommunications regulator began to change in the 1990s with the emergence of premium-rated VAS that included some financial-type services and which is now known as Direct Carrier Billing (DCB).[227] As DCB evolved into DFS, the NTA has taken on a new role of often – but not always – regulating financial-type services and its adjacencies. MNOs in particular have become leaders in providing these new services, with new license categories developed by regulators to allow non-banks to provide financial services. It has also led to necessary close cooperation between normally

[224] An ability to self-repair to resend a critical message may depend on the STK implementation and the handset.

[225] See thereto, Perlman, L (2017) *Technology Inequality: Opportunities And Challenges For Mobile Financial Service*s, available at https://bit.Ly/2r7nzny; Perlman, L & Weschler, M (2018) *Mobile Coverage and Its Impact on DFS*, available at https://www.dfsobservatory.com

[226] See, for example, the National Payments Corporation of India, which is planning for feature phones and USSD being the primary access mechanism to DFS. CNBC (2016) *Move To Cashless Society To Be Driven By Feature Phones: Hota,* available at https://bit.ly/2Iq6hnF

[227] For a historical overview of the first use of the mobile phone bill and prepaid airtime wallet for VAS and other services, see Perlman, L (2012) *LLD Thesis: Legal and Regulatory Aspects of Mobile Financial Services,* available at https://bit.ly/2KGfC8k

distinct regulatory bodies with distinct service or institutionally -focused remits: central banks and telecommunications regulators.[228]

Depending on the jurisdictional approaches, financial transactions that involve receiving and storing of fiat-based[229] customer funds and payments using fiat funds used in DFS is usually under the remit of the central bank or similar financial regulator.[230]

### 5.4 Role of NTA

Providers of DFS can be authorized to provide services through the following regulatory devices:

- **Letter of No Objection (LONO):** Regulators can decide to issue a LONO when a law allowing a provider to provide services or where an existing law is silent or inconsistent, provided other requirements, such as risk management structures and capital adequacy are met, and where the provider is fit and proper. Such letters are given within the NTA's general mandate to oversee telecommunication services in a country.[231]
- **No Action Letter:** This is given to innovators in circumstances where the regulator may be uncertain as to whether the new product/service constitutes a regulatory risk.[232] These letters constitute assurances from the regulator that it has no intention of taking enforcement action against the company for introducing a new (financial) service. Such letters can, however, be revoked at any time if the regulator changes its mind or circumstances necessitate that the authorization be terminated or suspended.
- **Licensing:** This is issued under circumstances where there are appropriate legal and regulatory frameworks for issuance of a license.[233] Most countries in Africa and Asia where DFS is prevalent have now put in place enabling legislation in the form of a payments or equivalent framework law which covers most or all electronic payments including DFS.[234] The licensing may be temporary, for example, when used in a 'regulatory sandbox'[235] environment.

The license types seen globally in DFS-focused ecosystems are outlined in **Exhibit 9.**

---

[228] Perlman, L (2018) *Model MOU Between a central Bank and National Telecommunications Authority For Digital Financial Services Regulation*, available at www.dfsobservatory.com

[229] *Fiat* means, in essence, currency (money) issued by a central bank and backed by the state. Compare this to virtual currencies such as mobile airtime value 'issued' by an MNO; or to crypto currencies - such as Bitcoin and Ether - which are mostly cryptographically secured and derived, tradable currencies created and issued mostly without a central issuer.

[230] In Indonesia, these remits have been split between Bank Indonesia and OBJ, the banking regulator. In most jurisdictions, the central bank is the sole financial regulator where receipt and storage of customer funds is involved. Where there are ancillary services in the DFS ecosystem such as credit provision, a credit regulator may also have sole or simultaneous remit with the central bank over use of the stored funds.

[231] The LONO and NAL could also be used where the 'test-and-learn' approach is being followed. See further, Buku, MW and Meredith, MW (2013) *Safaricom and M-PESA in Kenya: Financial Inclusion and Financial Integrity*, available at https://bit.ly/2HLSAhG.

[232] In 2016 the US Consumer Financial Protection Bureau issued a new policy on fintech innovation allowing the granting of such letters of no action. For a commentary thereto, see Sullivan & Cromwell LLP (2016) *Regulatory Guidance Regarding FinTech Products and Services*, available at https://bit.ly/2KvdAao

[233] For example laws on payments or micro-credit provision.

[234] Examples are payments laws in Kenya, Ghana, India, Bangladesh and Jordan.

[235] Regulatory 'sandboxes' are limited-activity authorizations by regulators for services to experiment with innovative product and services. The authorizations confine the service provider to provide limited services for a specified time only. The spectrum of regulations that could ordinarily apply to the innovation may be waived in part for the duration of the period of authorization. See further CGAP (2017) *Regulatory Sandboxes and Financial Inclusion,* available at https://goo.gl/XMAA2m

| License Models | Responsible Authorities | Features | Advantages | Disadvantages |
|---|---|---|---|---|
| **Non-bank DFS Provision** | • NTAs, if the DFSP is an MNO<br>• Central Bank<br>• Competition Authorities<br>• ICT Ministries<br>• Data Protection<br>• AML Unit | • Non-banks have own DFSP license and can issue e-money<br>• Stand-alone licenses given by Central Banks for issuance of e-money & provision of transactional payment services to customers.<br>• Special vehicle for non-bank DFSs may be required by regulators | • New, nimble entrants may provide low-cost transactional services<br>• If an MNO, could use airtime agent network for DFS cash-in, cash out | • High bar to obtaining DFS license<br>• Often an absence of proper enabling licensing regulations<br>• User lack of technology literacy leads to OTC use and low DFS account activity<br>• Difficult to scale and maintain activity levels<br>• Lack of regulatory coordination in DFS<br>• Lack of interoperability with other DFSPs<br>• Often cannot connect to merchants for national payments<br>• KYC process strict, expensive<br>• MNOs may be excluded from being DFSPs<br>• Cannot provide credit products |
| **Bank & Non-Bank DFS Provision** | • NTAs, if NBSP is an MNO<br>• Central Bank<br>• Competition Authorities<br>• ICT Ministries<br>• Data Protection<br>• AMLU | • Non-bank DFSPs must partner with a licensed bank for DFS to distribute e-money<br>• Non-bank DFSP can only distribute e-money provided by licensed banks<br>• DFSP can provide agent network to banks for KYC and cash in/cash out<br>• Special vehicle for non-bank DFSPs may be required by regulators | • Provides access to e-money and the market for non-bank DFSPs<br>• Customer funds are safeguarded in bank escrow accounts<br>• Banks may gain access to bearer services at favorable terms<br>• DFSPs may be able to provide credit products | • DFSPs often cannot connect to merchants<br>• Lack of interoperability with other DFSPs<br>• Higher KYC costs for DFSPs<br>• User lack of technology literacy leads to OTC use and low DFS account activity<br>• Higher compliance costs for DFSPs<br>• DFSP must share revenue with bank<br>• Less incentive for non-banks to enter DFS market<br>• Difficult to scale and maintain activity levels |
| **Bank-only DFS** | • NTAs, if NBSP is an MNO<br>• Central Bank<br>• Competition Authorities<br>• ICT Ministries<br>• Data Protection<br>• AMLU | • Only licensed banks can operate DFS & issue e-money<br>• DFS may be same as mobile banking<br>• Banks may create special low cost bank-lite simplified accounts; but no credit provided | • Existing bank licensing frameworks can largely be used to provide e-money<br>• Credit may be provided | • Excludes non-bank DFSP from providing full DFS services<br>• Does not promote financial inclusion<br>• Difficult to scale as bank must build own agent network<br>• Banks often struggle to get bearer services at viable rates<br>• No incentive for banks to pursue efforts than may cannibalize their mainstream banking business |
| **Direct Carrier Billing Using Mobile Airtime** | • NTAs, if NBSP is an MNO<br>• Central Bank<br>• Competition Authorities<br>• ICT Ministries<br>• Data Protection<br>• AMLU | • Allows purchase of a range of digital goods and services | • Airtime top-up can be used to provide digital liquidity | • Not yet available to purchase wider range of goods and services<br>• No 16 digit primary account number for use across POS and merchants, |

**Exhibit 9:** DFS license types seen globally in DFS-focused ecosystems with their advantages and disadvantages. DCB is included because it can often be used to purchase corporeal goods as with fiat money.

In some countries, DFS is seen by the regulator as a VAS license required not only of licensed MNOs but any entity providing DFS. Where the entity is an MNO, the VAS license may be part of their overall

license requiring a time-consuming license alteration or a relatively faster provision of an addendum to the license. In all cases – even where an NTA does not require the entity to obtain a DFS-related VAS license – the entity still requires some type of authorization from the central bank.

## 5.5 Effect on DFS

Both DCB and DFS ecosystems have led to a sea change in regulatory oversight over financial-type services. For DFS, new license categories were developed and modified by regulators to allow non-banks to provide these services. Both have also led to necessary cooperation between two normally distinct regulatory bodies: central banks and telecommunications regulators. DFS is usually under the remit of the central bank, with the telecommunications regulator involved if the provider is a licensed MNO. For DCB, the telecommunications regulator leads as the source of airtime value is from a licensed MNO, with the central bank providing supporting guidance for the ability to use airtime value in the broader (physical) economy.

The approaches of central banks in imposing restrictive policy and regulatory and licensing precepts for non-banks to operate DFS has been flagged[236] as handicapping efforts at financial inclusion. In particular, policies by central banks in mandating partnerships between banks and non-banks for DFSPs is said[237] to handicap efforts in promoting financial inclusion by making back-end processes too expensive along with increasing compliance costs. In Bangladesh and Nigeria, for example, the NTAs have decreed that MNOs are not allowed to provide any stand-alone DFS-related services. The result is not surprising that DFS has been only partially successful only in limited markets towards nudging people into the formal economy and concomitantly that the use of mobile airtime as a form of currency continues to be widespread.[238] In Nigeria, the Nigerian Communications Commission signed a MOU with the Central Bank of Nigeria to enable digital mobile operators to incorporate Special Purpose Vehicles to offer mobile money services. To date, MNOs have not been allowed by the NCC to directly provide DFS, except to act as agents for banks and DFSPs.[239]

## 5.6 Agents

### 5.6.1 Overview

In many cases the NTA issues regulations in relation to third party agents who may provide telecommunications-related services and/or DFS services. In many cases the agents – and if required by CIV regulations – undertake customer identification during signup for mobile services by making copies of identity documents and, if available and required, capturing biometric data from the customer. In the DFS realm, additional information may be required that facilitate additional transaction levels. Agents themselves may need to be authorized by the NTA where mobile telecommunications–only services are

[236] See, in summary, Staschen, S & Meagher, P (2018) *Basic Regulatory Enablers for Digital Financial Services*, available at https://bit.ly/2s8b2YX; and similarly UNSGSA (2018) *Financial Inclusion*, available at https://bit.ly/2qfOcNI;

[237] *ibid*

[238] Perlman, L (2017) *Technology Inequality: Opportunities And Challenges For Mobile Financial Service*s, available at https://bit.Ly/2r7nzny

[239] Nigeria's ban on MNOs providing DFS is thought to be the primary reason for low volumes of DFS use in Nigeria and high rates of financial exclusion. The MOU reportedly also relates to co-remit over the banking and telecommunication industries in order to drive payment systems and increase financial inclusion. Leadership NGA (2018) *NCC, CBN Sign MoU On Mobile Money, Financial Inclusion*, available at https://bit.ly/2JAqRP8

involved while other regulators, such as the central bank, may need to authorize the same agents for DFS services provided by the agent. 'Super agents' may be authorized by the central bank and/or the NTA to do know your agent (KYA) procedures on agents.[240]

### 5.6.2 Effect on DFS

Agent networks represent the frontline of the transformational nature of DFS systems, bringing financial inclusion to previously excluded areas. The ubiquity of these agents – representing non-banks, banks and the Malawi Posts Corporation (MPC) - embedded throughout a country can create a network effect of convenience and access that grows the financial ecosystem.

But as the networks grow, there are often challenges in balancing policy and business goals, exemplified by whether or not to allow present and continued agent exclusivity.[241] This exclusivity may relate to DFS-only or mobile airtime-only agents, or agents that act in both capacities. But as other entrants appear and require access to agents, policies on agent exclusivity may be strained.[242] Regulators may then struggle to balance the convenience of ubiquitous agents, with investments by market participants and with competition policy. With the growth of agent networks, there are also increased risks, requiring proper Risk Management Frameworks (RMF) for agents as well as shared agent blacklists.

Ongoing competition-related issues have percolated around exclusivity of agents in providing CICO services as well as for customer signup. Some jurisdictions have banned exclusivity for DFS provision whilst leaving intact exclusivity where the DFS agent sells mobile airtime vouchers for only one MNO, as is the situation in Malawi. In some cases, like Kenya, it appears than agent exclusivity assisted in growing the market for DFS.[243] In Kenya in 2014, MNO Airtel complained about agent exclusivity arrangements enforced by competitor Safaricom for their M-PESA agent network. Safaricom countered that it had invested in building an agent network and should not be required to share agents with competitors and lose its return on investment. A ruling by the Competition Authority of Kenya (CAK) ordered Safaricom to open up its M-PESA agent network to rival DFS firms.[244] A recent report, however, indicated that there are aspects of exclusivity being enforced through marketing requirements.[245] Airtel lodged a complaint with the CAK thereto.[246]

---

[240] In Malawi, any company needing to distribute its goods or services through appointment of distributors/agents are required to seek authorization from the Competition & Fair Trading Commission (CFTC). If an enterprise feels that it is important for them to distribute their goods or services through exclusive dealing, then they are required to seek authorization from the CFTC.

[241] In some cases, like Kenya, it appears than agent exclusivity assisted in growing the market for DFS. See Matibe, E (2014) *The Status of Agents in Kenya: Proliferation, Dominance, Evolution & Impact,* available at https://bit.ly/29Nq2AV

[242] Any company needing to distribute its goods or services through appointment of distributors/agents are required to seek authorization from the CFTC in terms of the CFTA. The CFTC assesses the likely effect of the arrangement on competition and consumer to decide whether to authorize or not.

[243] See Matibe, E (2014) *The Status of Agents in Kenya: Proliferation, Dominance, Evolution & Impact,* available at https://bit.ly/29Nq2AV

[244] ZDNet (2014) *How Kenya's Mobile Money Is Opening Up Now Middlemen Have Been Set Free,* available at http://zd.net/1wgcaHD

The ban on agent exclusivity was further solidified in the National Payment Systems Regulations of 2014, which prohibited exclusivity in agent contracts of payment service providers such as mobile money providers. See CBK (2014) *National Payment Systems Regulations of 2014*, available at https://goo.gl/f9cnLc

[245] CGAP reported that interviews with agents indicates that one MNO requires that a minimum of 75% of signage must be for their brand. See Mazer, P & Rowan, P (2016) *Competition in Mobile Financial Services: Lessons from Kenya & Tanzania*, available at https://goo.gl/osF8Mo

[246] Business Daily (2015) *Competition Authority Of Kenya Asks Airtel For Evidence Against Safaricom In Mobile Cash Agents Row*, available at https://goo.gl/F4x2Rm

In Malawi, the Competition and Fair Trading Commission (CFTC) has outlawed agent exclusivity *per se.* However, it allows MNOs to have exclusivity for their airtime-selling agents but not for their DFS agents even though these may be the same person. It does, however, not appear to tightly enforce the DFS agent exclusivity rule, allowing some DFS SPs to have exclusive agents.

# 6 AGENT & CUSTOMER IDENTITY AND VERIFICATION

## 6.1 Overview

Security, anti-social behaviour and money laundering concerns have spurred many governments to mandate that users of prepaid mobile SIM cards confirm their identity to activate and/or continue to use their SIM cards. In most countries where this occurred, [247] it has involved attempts – some unsuccessfully - to register millions of users who have long-since been using these cards.

A new trend is the use of biometric identifiers linked to national identity numbers to facilitate these registrations. Under these 'eKYC' systems, users need to register their biometrics with a national ID agency and these biometrics are used for authentication when they request a new SIM card. A biometric reader certified by a regulator or the ID agency is required.

Initial implementations have involved capturing fingerprint data, with evolving implementations using Iris capture, bolstered by drops in costs for this technology.These types of eKYC systems are in place or planned in, *inter alia,* Nigeria, Ghana,[248] Pakistan,[249] Bangladesh, Indonesia, Malaysia, Brazil, South Africa, Uganda,[250] Jordan and India. [251] While SIM registration is often not sufficient KYC to open a DFS

[247] Prepaid SIM card registration is currently mandated in over 90 countries. See further GSMA (2016b) *Mandatory 'Real Name' Registration By Prepaid SIM Card Users: Considerations For Policymakers*, available at https://bit.ly/2L7kkMI

[248] Biometric IDs are issued by the National Identification Authority (NIA). Ghana began re registration of SIM cards in November 2017. Modern Ghana (2017) *Ghana To Witness Massive Re-registration Of SIM Cards From November*, available at https://bit.ly/2rx7NKs

[249] The Pakistan Telecommunications Authority mandated verification of all active SIM cards using biometric verification where every SIM owner was required to visit an operator outlet where their MSISDN and Computerized National Identity Card were confirmed or updated in the existing ownership database and fingerprints were matched with the National Database and Registration Authority. Gidvani, L (2015) *The Promise of Biometric KYC and Remote Account Opening for Branchless Banking in Pakistan,* available at https://bit.ly/2rFPhiP

[250] The Ugandan SIM card registration process was affected during the course of 2017 by conflicts between the MNOs, the UCC and the government over deadlines for registration and availability of required ID documents. Users were switched off then on again following intervention by the president. New Vision (2017) *Telecom firms given 72 hours to deactivate SIM card*s, available at https://shar.es/1Pemkq . Similarly in Mexico in 2009, Mexico's introduction of its mandatory SIM registration program called RENAUT was marred by concerns on the privacy and security of the database, and the program and database was scrapped in 2012. The database was decommissioned and the significant financial investment by all the operators and the authorities was written off. A new system was introduced in August 2014. GSMA (2016b) *Mandatory Registration Of Prepaid SIM Cards*, available at https://bit.ly/2rysm90.

[251] In India for example, Unique Identification Authority of India's national identity verification system uses a sequence of biometric capture devices to collect the biometric and demographic data of residents, store them in a centralized database, and issue a 12-digit unique identity number called Aadhaar to each resident. It is considered the world's largest national identification number project. Iris is becoming the preferred biometric capture method in DFS countries. This is set to increase with emergence of APIs for Iris capture and phones with Iris scanners. See United Identification Authority of India (2018) *United Identification Authority of India,* available at https://uidai.gov.in. In Jordan the ID agency is the Civil Status and Passports Department.

account, some jurisdictions where there is registration allow a DFS account linked to each SIM card under registration to be opened.[252]

**Role of the NTA:**
SIM card registration; Agent registration and identification; certification of biometric readers for registrations

### 6.2 Role of the NTA

The specific requirements vary by country but usually involve provision of a designated form of identity. For locals, residents and citizens this may be a type of ID issues by an authority in that country as well as proof of recent address or, for foreigners visiting a country, passports may be used. In many cases, a huge challenge has been to provide proper identity documents generated by other government departments – such as interior ministries, drivers' licenses – to fulfil the requirements of the registration, especially where the infrastructure and capacity to produce these documents is lacking.

As noted by the GSMA,[253] the availability of national identity documents and whether the identity documentation being used can be validated against a government registry, either at point of sale or at point of activation, has a significant bearing on the registration solution. Similarly, the e-KYC solutions noted above that use biometric data captured on registration can augment or even replace the need for ID documents.[254] Thus while SIM registration can provide access to many services such as DFS, uncoordinated or over-bearing regulations issued by the NTA as part of the mandate may unintentionally exclude vulnerable and socially disadvantaged consumers. In some cases, the registrations have been largely successful. In others, coordination and technology failures have led to expensive effects on the society and the economy. Tourists who use their passports to obtain SIM cards often cannot be verified in real-time nor are they subject to restrictions on the number of mobile phone lines they may obtain. They may potentially give their mobile phone lines to others who are not able to obtain lines (for example, those on a security blacklist) or to citizens who wish to circumvent the restriction on the use and number of mobile phone lines that can be registered in their name.[255]

There have been some regional efforts to undertake KYC. The East African Community (EAC) presidents - Kenya, Uganda and Rwanda - launched the One Area Network to develop a uniform policy on the registration of SIM cards[256]

[252] SIM registration may sometimes be sufficient to open a DFS account that does not allow cash-out, but additional KYC is required for full functionality. In some countries, the number of DFS accounts may be limited. In Jordan for example, a user may only have 2 DFS accounts, even though they may have multiple mobile numbers and SIMs.
[253] GSMA (2016b) *Mandatory Registration* of *Prepaid SIM Cards*. *Addressing Challenges Through Best Practice*, available at https://bit.ly/2rx7NKs
[254] The lack of a verifiable address or similar document for onboarding and which assists in verifying identity for transaction purposes has been a handicap to these efforts. In addition, most of these onboarding and verification procedures have involved manual processes and involve fragile documents.
[255] In Jordan, the planned TRC SIM card biodata enrollment will reportedly capture the fingerprints of foreigners using passports for SIM card registration may provide greater security.
[256] Standard Kenya (2015) *EAC Banks On Regional SIM Card Law To Curb Insecurity*, available at https://bit.ly/2rCflui

NTAs have imposed large fines on licensees for perceived deficiencies in SIM card registration by MNOs. In Tanzania in September 2017, six MNOs were together fined a record USD5 million by the Tanzania Communication Regulatory Authority (TCRA) for registering new SIM cards for subscribers whose details of Identification Cards (IDs) were questionable and others which could not be traced in the database. The TCRA also indicated that there were other irregularities such as were failure to confirm customers' information, allowing the registrations with another person's IDs and the mismatch of the customer's photos with the one appearing on the ID.

In Nigeria, the Nigerian Communications Commission (NCC) fined South Africa-headquartered MNO MTN for not disconnecting 5.2 million unregistered subscribers. A fine of USD 5.2 billion was imposed by the NTA, the NCC. The fine caused a diplomatic rift between the Nigerian and South African governments. Negotiations between the two governments reduced the fine to USD 927 million.[257] The settlement however was challenged in court by Nigerian parliamentarians, who sought to revoke MTN's operating license.[258]

**Exhibit 10:** NTA enforcement actions relating to KYC/CIV

### 6.3 Effect on DFS

As DFS grows in developing countries, regulators have imposed KYC rules that require DFSPs to identify users on their systems. With a few exceptions, some type of identity must be provided by the user for account openings and CICO services.[259] The most salient distinctions between the DFS and DCB ecosystems and the respective regulatory approaches is on use of the funds and in KYC and ongoing customer due diligence (CDD). In many jurisdictions, where financial integrity is prioritized over financial inclusion by regulators, KYC and CDD requirements are usually stricter for DFS than for DCB.

DFS-focused KYC rules are derived from standards established by the G7's Financial Action Task Force (FATF) on standards in financial services aimed at AML and countering the financing of terrorism (CFT) initiatives. FATF encourages moves towards the provision of electronic ID cards to support financial inclusion while appropriately mitigating the ML/TF risks, recognized and supported by FATF's November 2017 'Guidance on CDD.'[260] Often, though, there may be duplicate or even conflicting requirements from various regulators. For example, the central bank may have different requirements to the NTA on KYC documents and processes, such that registration for a SIM card using 'eKYC' biometric identifiers may not be enough to satisfy the requirements from the central bank for opening a DFS account. That is, registration for a new SIM card may be insufficient for the contemporaneous opening of a DFS

[257] ITWeb Africa (2017) *MTN survives Nigeria fine debacle,* available at https://bit.ly/2rNF17B

[258] Vanguard News Nigeria (2017) *N1.40trn fine: Court refuses to revoke MTN's operating licence*, available at https://bit.ly/2KwwHkr

[259] See also, McGowan, K (2015) *Know Your Customer is the Secret to MNO Negotiations*, available at https://bit.ly/2Im2WpJ; Gidvani, L (2015) T*he Promise of Biometric KYC and Remote Account Opening for Branchless Banking in Pakistan*, available at https://bit.ly/2InUWjV

[260] The FATF *G*uidance provides country examples of simplified CDD (SDD) measures adapted to the context of financial inclusion. Those examples illustrate how SDD can support both financial inclusion and financial integrity policy objectives, especially where supported by alternative forms of identity verification, for example the use of e-identity tools. See FATF (2017) *Guidance On AML/CFT Measures And Financial Inclusion, With A Supplement On Customer Due Diligence*, available at https://bit.ly/2wLMObN

account.[261] NTAs may also restrict the number of SIM cards that can be registered to one person or company.[262]

Where DFS is provided by MNOs and where biometric data captured during the SIM registration is stored online and can be accessed and verified, this registration data can be used as a proof of identity (sufficient for KYC) for DFS services offered by that MNO, where the customer gives consent for their ID go be used. Any seamless use of the stored identity may, of course, not be available where the DFS is provided by a non-MNO third party, or where the identity database is not online.

Regulatory coordination also plays a role here: while the SIM card registration is under the mandate of the NTA, any DFS registration will usually be under the CDD mandate and rules of the central bank, and/or an FIU.

In many cases, the SIM card registration process and proof of identity provided may suffice for a 'basic' DFS account of limited transaction value, balances and velocity. Higher proof usually triggers higher allowed levels of DFS transactional ability within the tier limits set by the central bank and/or FIU. Because fiat money – rather than airtime value – is involved in the DFS wallet, money laundering concerns relating back to FATF AML requirements are applicable, triggering then higher CDD requirements for DFS than for SIM registration. The nirvana for efficiency's sake is for the SIM registration CDD to be fully usable for all levels of DFS CDD requirements. But this is unlikely to happen in markets where there is disparate quality of ID documents and ability to do proper CDD. Unless there is regulatory coordination, rules from various regulators and lack of integration with specified components such as (national) ID databases may conflict and cause harm to the DFS ecosystem.[263]

Switch-off of unregistered SIMs involves barring all incoming and outgoing calls, barring data services, enabling only mobile money cash-out but no cash in or receipt of funds, calls only for emergency services and calls to customer care. Unused DFS balances are retained in accordance to mobile money regulations as was stipulated for example by Bank of Uganda when the Communications Commission of Uganda imposed switch-off.[264]

The issue in Nigeria still percolates, as issuance of national IDs take up to one month and requires often unavailable birth documents. The issue highlights concerns that, despite ostensibly applying Risk Based

[261] In India though, the Aadhar biometric database would allow this contemporaneous ID check. Jordan plans on doing the same.

[262] In Bangladesh, a user will can use a maximum of 15 SIM cards with their national identity. Risingbd (2017) *BTRC Orders To Close Extra Sim Cards By Dec 31*, available at https://bit.ly/2IbkNLT.

[263] Such was the case in Uganda when the UCC banned the sale of new and replacement SIM cards until an API into the National Identification Registration Authority ID database was developed and integrated and until MNO agents – who sell at places licensed by a city authority - could employ and use biometric readers to undertake real time online verification of customers' information with the database. The ban lasted for 2 months and was lifted, with some remaining restrictions in May 2018. This followed the UCC ordering MNOs in 2017 to switch-off, then later switched back on following an outcry, some 2 million unregistered SIM cards. In both cases, the effect was manifest on DFS: inability to access the mobile networks led to inability to access their DFS accounts. See New Vision (2018*) UCC Lifts Ban On Sale And Replacement Of SIM Cards*, available at https://bit.ly/2rzdwiT. In Jordan, citizens over 18 can register up to 10 SIMs per provider for each of the three MNOs in Jordan. A person may therefore have up to 30 lines in total. There is no such mobile number maximum restriction on non-Jordanians.

[264] EDGE (2017) *UCC Directs Telecoms To Switch Off Unverified SIM Cards*, available at https://bit.ly/2whzolo

Approaches (RBA) for financial inclusion imperatives suggested by FATF,[265] mandated requirements to undertake Customer Identification and Verification (CIV) of users is seen to be too restrictive and too expensive to implement in relation to the assessed and relative threat offered by relatively low-value DFS activity.[266] National consideration – especially in relation to security matters – may override the suggested RBA though.[267] In all, compliance costs are a major cost locus for DFSPs (and MNOs acting as DFSPs) and a significant hurdle to their growth and profitability.

Despite seemingly impressive numbers of registrations for DFS services, user activity levels and deeper penetration into the broader payments ecosystem in many DFS-focused countries is disappointing, with trend lines showing large inactivity levels. Data from the World Bank's 2017 Findex Survey[268] for example suggest that while DFS accounts have grown from 2014, activity levels have fallen. Analysis from the Center for Financial Inclusion at Accion of Findex data found that roughly half of the new accounts — nearly 235 million — have not been used in a 12 month period. The number of active account holders only increased by 285 million, much less than the overall growth, they say, in account ownership from 2011–2014. Similar trend lines have been reported by the GSMA, whose State of the Industry Report on Mobile Money 2017[269] highlighted – as noted above - that of the 690 million 'mobile money' accounts opened, active account use within a 90 day period was at disappointing 35.8% and active account use within a 30 day period at a worrying 24.3%.

One reason may be that restrictive onerous CIV[270] has meant that many potential users cannot or do not want to meet the strict CIV policies. And while for DFS, cash out through licensed agents and general use of the funds is allowed, with DCB only a few NTAs allow a cash-out from the mobile airtime wallet. This has had the unintended consequence of a growth in anonymous OTC activity with DFS agents, counterproductively reducing the regulator's visibility over transactions.

[265] A RBA is generally based on guidelines and principles – rather than rules - for addressing a particular risk, so as to lead to a desired outcome. A feature of a RBA is that compared to a normative, rules-based approach, the supervisory entity does not specify the precise steps required to achieve the desired outcome, rather leaving it to the implementing entity to address the risks outlined in guidelines by implementing procedures and rules that are contextually relevant to it. The rules and procedure of each entity may thus differ, although the net effect of each variation is to address the risks outlined in the guidelines. On the use of a RBA for CDD, see FATF (2017) *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion with a Supplement on Customer Due Diligence*, available at https://bit.ly/2taubZM; and Lyman, T & de Koker, L (2018) *KYC Utilities & Beyond: Solutions for AML/CFT Paradox?*, available at https://bit.ly/2OqOgso. On CIV and identities, see Perlman, L & Gurung, N (2018) *Focus Note: The Use of eIDs and eKYC for Customer Identity and Verification in Developing Countries: Progress and Challenges*, available at www.dfsobservatory.com

[266] The lack of standardized national identities in many countries is a particularly complicating factor in undertaking full KYC for users to allow them to participate in full range of financial and transactional services.

[267] In Uganda, the 2018 ban came after kidnappers were found to have used unregistered SIMs. New Vision (2018*) UCC Lifts Ban On Sale And Replacement Of SIM Cards*, available at https://bit.ly/2rzdwiT

[268] World Bank Group (2018) *The Global Findex Database 2017,* available at https://globalfindex.worldbank.org;

[269] See GSMA (2018) *2017 State of the Industry Report on Mobile Money*, available at https://bit.ly/2IvPZ94

[270] See generally on CIV processes and their impact, Perlman, L & Gurung, N (2018) *Focus Note: The Use of eIDs and eKYC for Customer Identity and Verification in Developing Countries: Progress and Challenges*, available at www.dfsobservatory.com

# 7 PRICING

## 7.1 Overview

Price controls on telecommunications-related voice and bearer prices – at a wholesale and retail level – are common. In many market, regulatory intervention on rates for interconnecting between MNOs for voice and SMSs – often known as termination rates - are common.[271] Intervention – usually price maxima – at the retail price level are also common.

**NTA Role:**

Wholesale Bearer Cost regulation; Retail price regulation; Net Neutrality

## 7.2 Role of NTA

Often pricing is a commercial negotiation that satisfies all parties but sometimes disputes are escalated to a sectoral regulator or the courts. Regulators would look at regulating prices in relation to (theories of) market power, abuse of dominance in excessive, discriminatory and exclusionary pricing. Price regulation generally can be burdensome if it requires cost modelling, or use of benchmarks and may take many years to accomplish, especially if market participants stonewall on providing necessary data to undertake a cost analysis.[272] This may also include market definition reports, detailed proposals for market definitions, an analysis of whether an entity has significant market power (SMP),[273] effective competition analysis, and principles for pro-competitive intervention as may be required. A conclusion of ineffective competition may to be to find that pricing is inefficient because it has not driven down to cost through competition.

For regulators looking to regulate USSD (or other) charges, determining the 'correct' price level has not been an easy exercise, requiring sophisticated cost analysis measures. Other regulators, however, may simply use blunt force: by slashing bearer pricing to a level they believe will stimulate a market.

Regulators may use a cost-based model to determine pricing, although there are only a few apparent cases of where this complex exercise has been undertaken, at least in telecommunication-cost related

[271] Smaller MNOs may benefit from asymmetry in termination rates. That is they do not pay the same termination rates for interconnecting as larger MNOs. See ICASA. Columbia, India. On mobile termination rates and their regulation in general and in relation to the South African telecommunications sector, see Hawthorne, R, Mondliwa, P, Paremoer, T & Robb, G (2016) *Competition, Barriers To Entry And Inclusive Growth: Telecommunications Sector Study*, available at https://goo.gl/uaiUMq. On Uganda, see Macmillan Keck Attorneys & Solicitors & ACACIA Economics (2017) *Draft Non-Confidential Summary Of Final Report, Public Consultation Document, Support to the Uganda Communications Commission on USSD and SMS services*, available at https://bit.ly/2KbRXg3

[272] Business Tech SA (2014) *MTN and Vodacom termination costs a "dark secret",* available at https://bit.ly/2Ojwoek

[273] A European Commission commentary on competition policy refers to SMP being whether an entity 'enjoys a position of economic strength affording it the power to behave to an appreciable extent independently of its competitors, customers and ultimately consumers.' The power must relate to a relevant market, as the definition of the relevant market is of fundamental importance since effective competition can only be assessed by reference to the market thus defined. Usually a SRA with competition powers or competition authority with similar or co-jurisdictional remit will undertake an assessment of that 'relevant market' before making a SMP determination. The EC also says that use of the term 'relevant market' implies the description of the products or services that make up the market and the assessment of the geographical scope of that market. See EC (2001) *Commission Working Document - on Proposed New Regulatory Framework for Electronic Communications*, available at https://bit.ly/2EZwlVD. A telecommunications entity designated as having SMP may be subject to specific obligations such as the requirement to have cost-oriented tariffs. It may also determine if this power is sustainable phenomenon and define market power with respect to the sectoral traits of this sector. See Welfensm, J (2004) Significant Market Power in Telecommunications: Theoretical and Practical Aspects, available at https://bit.ly/2SzjnQW

instances.[274] Where regulators have mandated – or proposed - USSD channel access prices, MNOs have complained that the set charges are below market value and do not compensate MNOs for the additional investments needed for network capacity to absorb increased traffic from USSD and ensure the sustainable delivery of quality service.[275]

Further, MNOs may complain that they are then not compensated for the opportunity costs of lost call revenue due to their signaling channel being used by low-cost USSD DFS sessions.[276] As noted above, the regulators may also set high pricing for simple SMS short codes, impacting setup and annual costs from the regulator to the provider.[277]

### 7.3 Effect on DFS

While MNOs may grant third parties access to their STK and/or USSD gateway facilities, the issue of pricing for these bearers often percolates. A regular feature of the DFS ecosystem is commercial disputes between MNOs and other SPs over the cost of USSD access and the consequence of dropped USSD sessions. Such complaints have emerged in Nigeria, India, Uganda, Zimbabwe, Kenya, and Bangladesh.[278] This is not necessarily the norm as there are many instances of sound commercial arrangements between MNOs and third parties, for example in Tanzania, Malawi and South Africa. They may also relate to differential pricing, whereby the MNO provides cheaper access pricing to a favored party such as its DFS subsidiary. Competition issues have been raised by MNOs in respect of being forced by regulations to provide access services to other SPs and banks in the DFS ecosystem.[279]

In some cases, the USSD session is charged to the customer at a fixed rate no matter the length of the session; or the Technical Service Provider (often an aggregator) or Payment Service Provider (PSP) is charged at wholesale rates for a transaction, no matter the length, or *pro rata*; or is charged via a percentage

---

[274] See for example in Zimbabwe, where the telecommunications regulator, POTRAZ, used a bottom-up costing model to set a floor price on mobile data and bearer access. This however resulted in large retail price increases for voice and bearer services, market confusion, and consumer anger.

[275] They also express concern that by mandating a price and commercial arrangement for the provision of USSD, regulators preclude businesses from striking innovative partnerships and commercial arrangements that may be more advantageous for consumers.

[276] Mas, I (2012) *What is the Telecom Regulator's Role in Fostering Mobile Money*?, available at https://goo.gl/X9cDFQ

[277] A recent report to the Uganda NTA, the UCC by Macmillan Keck. Attorneys & Solicitors compared regulator pricing from three East African Countries. The report notes that the UCC in Uganda set the application fee for a short code at USD 250, the annual authorization fee for a USSD short code at USD 10,000, and the annual authorization fee for an SMS code at USD 2,000, all excluding applicable VAT. The Rwanda Utilities Regulatory Authority (RURA) requires a USD 30 application fee when applying for a short code, and allocated USSD codes are subject to a USD 1,000 annual maintenance fee, while the annual maintenance fee for SMS codes range from USD 200 to USD 1,000. The Tanzania Communications Regulatory Authority charges a one-time USD 2,000 registration fee for allocation of 'ordinary' USSD and SMS short codes and a USD 3,000 annual maintenance fee thereafter, their report notes. See Macmillan Keck Attorneys & Solicitors & ACACIA Economics (2017) *Draft Non-Confidential Summary of Final Report, Public Consultation Document, Support to the Uganda Communications Commission on USSD and SMS services*, available at https://bit.ly/2KbRXg3. In Bangladesh, the Bangladesh Telecommunication Regulatory Commission charges a short code allocation fee of USD 1,230 and an annual fee of USD 615 for short codes used for 'commercial purposes' including general information, banking information, customer care service, helpline, news, e-business and other similar services. The short code allocation procedures do not distinguish between SMS and USSD short codes.

[278] Hanouch, M and Chen, G (2015) *Promoting Competition in Mobile Payments: The Role of USSD*, available at https://bit.ly/1RFMIVY

[279] Banks and DFS providers share 7% of their revenue with MNOs in exchange for gaining access to their USSD channels. Agents and distributors gets 77 % and the banks/SPs 16 %. Daily Sun (2018) *Session-Based USSD Price To Raise Mobile Banking Cost*, available at https://bit.ly/2rGjQ7n

of the transaction value. The MNO may also charge the SP a setup fee for access to its USSD gateway and/or a monthly facilities charge on top of any USSD session charges. While some TSPs and PSPs absorb the USSD charge, others will recoup the USSD cost incurred by directly debiting the customers' wallet with the charge.[280]

In Bangladesh, the NTA and CB have conflicting goals on DFS access: the NTA sees USSD access as necessitating a cost-recovery plus basis for wholesale pricing while the CB sees access pricing as being informed by financial inclusion goals.[281] The NTA pricing proposal submitted to government is four times higher than the proposal of the central bank.[282]

# 8 COMPETITION

## 8.1 Overview

Competition policy is complex and may involve economics and law; definition of relevant markets; identification of dominance; problems where market power is leveraged into downstream or adjacent markets; margin squeezes and other abuses of dominance; feedback loops between telecommunications and DFS markets, and remedies such as price regulation, and functional and structural separation.

There is a lot of debate on many of these issues, but for now these issues though are far beyond the scope of this section (and paper) and best left for specialized studies. What is important to note for this section (and paper) though is that often competition powers are found in sectoral regulation, such that each of the sectoral regulators may have mandates that allow them to intervene in their sector if there is a competition-related concern. In the cases of Uganda and Kenya, for example, both country's NTAs have been provided competition-related oversight powers by the legislature. However, in the case of India, the NTA has *ipso facto* assumed competition powers over a narrow band of technology issues affecting the DFS sector. Much of the competition-related concerns in DFS relate to USSD and STK-based access to services.

While smartphones may be seen by some as a panacea to the USSD and STK gateway access and pricing issues, DFSPs and WASPs in some smartphone markets still require USSD access, for example by the use of Network Initiated (NI/Push) USSD for 2 factor authentication for security in financial/banking applications. In Rwanda, the smartphone-based DFS apps still use USSD, which the MNOs there say speaks to market demand for a 'familiar' interface.[283]

**NTA Role:**

Wholesale Bearer Cost regulation; Retail price regulation; Net Neutrality; FRAND access to bearers; QOS in bearers; Net Neutrality; Intervention

---

[280] Mazer, P & Rowan, P (2016) *Competition in Mobile Financial Services: Lessons from Kenya & Tanzania*, available at https://goo.gl/osF8Mo

[281] MNOs in Bangladesh for example have complained of being forced by regulations to provide USSD access to other DFSPs below the MNO's opportunity cost. See on costing for USSD in Bangladesh, session-based, Daily Sun (2018) *USSD Price To Raise Mobile Banking Cost,* available at https://goo.gl/yvZiw5. The Bangladesh Telecommunications Regulatory Commission (BTRC) and the central bank, Bangladesh Bank, have each proposed different pricing models for USSD access, the former looking out for the interests of its licenses, the latter with a focus on affordability and financial inclusion.

[282] Daily Sun (2018) *Session-based USSD price to raise mobile banking cost*, available at https://bit.ly/2z7uGHm

[283] For technical details on NI-USSD, see Perlman, L (2017b) *Technology Inequality: Opportunities And Challenges For Mobile Financial Service*s, available at https://bit.Ly/2r7nzny

## 8.2 Role of NTA

Much like a competition regulator and where it has remit, the NTA may intervene in relation to level access to technology and services of scarce supply, especially if an entity has significant market power and abuses that power. Action to reduce harm may relate to USSD, STK, SMS short codes, pricing and national tariffs, zero rating and any anti-competitive practices that may arise within the marketplace.

In developing countries, fewer MNOs may exist, resulting in greater potential for anti-competitive behavior and dealing with state-owned MNOs and a monopoly of providers.[284] Often there will be a competition regulator or authority with which jurisdiction over such matters may be delegated or shared in some fashion. Often the NTA may provide technical assistance to the competition authority for telecommunications and DFS-related issues. A number of remedies that may be imposed where there are instances of abuse of dominance and general anti-competitive behaviour discovered through an investigation or legal action.[285]

An emerging issue in the provision of services is what has been termed 'net neutrality,' describing non-discriminatory provision of services over bearer channels. The issue crystallizes in the OTT mobile app domain in multiple ways: whether apps by third parties can install on MNO-locked mobile phones; whether the apps themselves will operate with the same degree of fidelity over the MNO bearers as would (possibly competing) MNO apps; and whether there is any price disparity in access to any bearer.[286] Even if the MNO does not directly compete with the third party, favoring a particular entity over another regarding access, QOS or price could trigger net neutrality and anti-competitive behavior concerns.[287]

For example, in April 2015, Airtel India launched its zero-rated platform Airtel Zero, which allowed customers to access certain apps for free.[288] Facebook itself launched its free but limited internet in August 2013 available only to Reliance Communications customers.[289] In response to complaints on net neutrality, TRAI held public consultations on the issue and released regulations in 2016 that banned the practice.[290] It is not clear if TRAI's decision – highlighting 'discriminatory' tariffs - was a direct competition issue in so far as there was (or was not) an abuse of dominance, it still telegraphs the potential for abuse of dominance in pricing (and access) to scarce resources where one of the parties is indeed seen by an authority as being dominant.

---

[284] In Ethiopia, Ethio-Telecom is the only MNO.

[285] These include interdicting a specified prohibited practice; ordering a party to supply or distribute goods or services; imposition of an administrative penalty; ordering divestiture; declaring conduct to be a prohibited practice; declaring an agreement void; and ordering access to an essential facility. See BKM Attorneys (2018) *The Basics Of Competition Law*, available at https://bit.ly/2wQXRjR

[286] While this is unlikely in IP-based networks, it is not impossible. It but could happen though with bearers such as STK and USSD. And so-called 'net neutrality' rule changes in the US however could usher in tiered pricing for IP access. Business Insider (2017) *The FCC plans to repeal net neutrality this week — and it could ruin the internet*, available at https://read.bi/2SvtEgV

[287] This could include the MNO sharing in advertising revenue on service access with a favored third party.

[288] Airtel India (2015) *Airtel launches 'Airtel Zero': A win-win platform for customers and marketers*, available at https://bit.ly/1H0I8L7

[289] News 18 (2016) *TRAI Says No To Differential Pricing; Favours Net Neutrality,* available at https://bit.ly/2GnKaIV

[290] TRAI (2016a) *Prohibition of Discriminatory Tariffs for Data Services Regulations*, *2016*, available at https://bit.ly/2wMiM7x

## 8.3 Effect on DFS

### 8.3.1 Overview

Because USSD and STK access to DFS can mostly only be offered by aggregators and licensed MNOs through their own USSD gateways, they are scarce technology resources. If the MNO is in competition with the DFS SP over a DFS-related service, it could potentially block that service, either by denying the SP access to the gateway or by not supplying it with short codes required for customer access. This refusal to supply service is not necessarily the norm as there are many instances of sound commercial arrangements between MNOs and entities that may compete with it in relation to DFS. Robust competition between DFSPs and WASPs (providing VAS) in Tanzania, Kenya, Zambia, Nigeria, Uganda, Malawi and South Africa, for example, has made USSD access a very profitable revenue source for MNOs, even where provided to SPs who may compete with the MNO on some services. However, the vertical integration between the MNOs infrastructure business and its DFS business has in some markets raised competition issues where there has been, objectively or an allegation of, a denial of service. These instances are outlined below.

**Access to the USSD components and gateways:** Access to USSD is crucial to the business plans of SPs. Loss of this access may irrevocably damage their business.[291] Usually the access given by MNOs to SPs is the Mobile Originated USSD (MO-USSD) accessible via short codes.[292] Inability to (and delays in provision of) access the gateway is fatal to a business predicated on USSD access given the scarcity of USSD. SPs denied access by the MNO could, however, approach aggregators who have access to the MNO gateway for access, but potentially at a higher price as the aggregator will charge a fee. In some countries, the provision of Network Initiated (NI)-USSD can provide a competitive advantage for SPs. For example, if there is a dropped USSD session and the transaction is not completed, the customer may not want to re-initiate the transaction to avoid potential double billing. NI-USSD will allow re-initiation of a dropped USSD-based transaction so that customers can complete their unfinished transaction.[293] However, even if NI-USSD is provisioned on the MNOs USSD gateway, the MNO may decide not to make it available to third parties.[294]

**Pricing of USSD Gateway Access and Use:** Pricing of USSD access to a USSD gateway is an issue in some markets. This may relate to wholesale and/or retail pricing for USSD. Usage on a wholesale basis may be charged by a MNO on a revenue-share, or usage per hop or per session basis. There may be conflict between the NTA – who may look at access pricing with a commercial-type, cost-recovery plus basis – and the CB who may have a financial inclusion lens and want a simple cost-recovery pricing regime used for the MNO's USSD pricing.[295]

**Time Allowed For a USSD Session:** The length of a USSD session may be restricted by the MNO for third party providers, such that there is not enough time for customers to input long account numbers when

[291] MNOs though may have legitimate reasons for denying a SPs access to their USSD gateway, for example a history of fraudulent use of USSD-based services with other MNOs or bad credit history. See also CGAP (2014) *Consumer Protection and Emerging Risks in Digital Financial Services Perspective from Bangladesh, Uganda, Colombia, and the Philippines,* available at https://bit.ly/2IaNMDK

[292] See Section 3.5.3 on short codes.

[293] TRAI (2016b) *Consultation Paper On The Review Of Regulatory Framework For The Use Of USSD For Mobile Financial Services*, available at https://goo.gl/dSSPLN

[294] *ibid*

[295] Daily Sun (2018) *Session-based USSD price to raise mobile banking cost*, available at https://bit.ly/2z7uGHm

prompted. Similarly, MNOs may restrict the time allowed for the input or for the customer to provide input to advance to the next tree on the menu. MNOs may cite the so-called 'opportunity cost' inherent in providing USSD to third parties, since they argue that the GSM system design may mean that use of USSD (signaling) channel may block revenue-generating incoming and outgoing voice calls for the duration of the live USSD session.[296] Further, they believe that a commercially and technically viable arrangement would allow for a price and length/stages of sessions that are commensurate since increased time increases the use of the USSD resource. MNOs have discouraged sessions lengths being increased whereas in India, it is implemented in tandem with a cap on the pricing per session.

**USSD Menu Tree Length:** USSD menu trees may be restricted by MNOs to a maximum number of stages. As noted earlier, MNOs cite the 'opportunity cost' inherent in providing USSD to third parties, since the GSM system design may mean that use of the USSD (signaling) channel may block revenue-generating incoming and outgoing voice calls for the duration of the live USSD session. MNOs indicate that increasing the number of menu stages would put a load on their signaling infrastructure and any increase in the number of stages contemplated is either practically impossible or should be accompanied by a commensurate increase in the ceiling tariff for USSD sessions.[297]

**SIM Toolkit Access:** Key to providing STK-based services is that the MNO provides access to its STK gateway; allows the SPs menu to be placed on the MNO SIM; allows Over The Air (OTA) updating of the SIM menus as needed; and that the MNO provides the DFS SP with short codes the SP's customers will use to access the SPs DFS service.[298]

**Access to STK Gateway:** For third party SPs to provide STK-based services to their customers, the MNO must provide these third parties access to their STK gateway. If this is refused, the third party may need to use another access bearer such as USSD, Near Sound Data Transfer (NSDT), Java applets, Wireless Application Protocol (WAP)-based access, or Over The Top (OTT) smartphone apps. Some of these alternate access mechanisms, however, may not have the same relative mass-market discovery potential as STK-based access.

**Pricing of STK Access:** Pricing of STK access has an issue in some markets. This may relate to the charges for a transaction, which may be per transaction no matter how many SMS are used, or per SMS. The MNO may also charge for OTA updates to a SPs STK-based SIM menu.

### 8.3.2 Country examples

[296] See for example the responses the TRAI received when canvassing local MNOs on use of USSD. The MNOs indicated that any move to increase the number of stages in a USSD menu would put a load on their signaling infrastructure and, therefore, that there should be a commensurate increase in the ceiling tariff for USSD session from the present level if the number of menus available were increased. Other MNOs were agreeable to increasing the number of stages provided such USSD sessions were restricted to transactions related to financial inclusion only and not for any other additional financial services such a mobile banking. TRAI (2016b) *ibid*

[297] *ibid*

[298] Since MNOs own the SIM card and thus control anything on it, this includes controlling the ability of third parties to load and use their own applications and encryption keys for use by their own customers. And as only the MNO can provision the SIM, the ability of a SP to receive or gain access to the required mobile encryption keys independently of the MNO is usually a complicated and expensive negotiation.

**Bangladesh:** By regulation, MNOs in Bangladesh are mostly only permitted to act as bearers - usually via USSD - for banks and other DFS SPs. Currently, access to USSD is provided on a revenue sharing basis. That is, instead of a unit or time-based charge, the MNOs are compensated only for those USSD sessions where the DFS providers earn revenue. USSD usage charges vary from MNO to MNO for DFS providers.[299] According to the MNOs, this revenue sharing model is unsustainable for them as the transactions which exhaustively use the USSD channel are extensively misused and mostly free of cost as 86% of USSD traffic and 100% of SMS are being provided for free. The MNOs indicate that they are not incentivized to provide access and sustainability depends on a justified return for the consumption of the used resource. Universal access is even more important to MNOs and overall Quality of service (QOS), they indicate, is being affected because of 'free' usage of telecom resources/ spectrum, which also reduces the value of spectrum if this is forced through. The Bangladeshi MNOs have been lobbying for a change in the USSD charging model towards usage-based pricing.[300] Even so, there are complaints from SPs and banks that wholesale USSD prices are too high.[301] The NTA and CB have different views on whether to increase USSD pricing for DFS, with the NTA siding with MNOs, while the CB says pricing should reflect financial inclusion priorities. As noted above, the NTA USSD pricing proposal for DFS submitted to government is four times higher than the proposal of the central bank.[302]

**Colombia:** After negotiations between banks and MNOs failed to resolve bank complaints over USSD pricing and access from MNOs, the Colombian telecommunications regulator, the *Comisión de Regulación de Comunicaciones*, mandated access to USSD and introduced a case-by-case resolution of complaints about price and quality.[303] And in relation to STK, Daviplata – a low-cost mobile banking platform used primarily for G2P payments offered by Banco Davivienda - implemented a dynamic menu via STK designed to simplify the UI and make it more understandable by the target segments. As services increased, the number of SMS per update increased to 20 SMS per update. The MNOs, however, increased the cost to Daviplata from being a per-transaction charge to a per-SMS charge. This meant that the cost of over a month's usage of the mobile channel consumed the entire commission that the bank received for managing the payments. Even simple balance enquiries with no transactional revenue value cost the bank substantially in profits. The issue was referred to the telecommunications regulator for review.[304]

**India:** The telecommunications regulator, TRAI, slashed USSD access prices by two thirds to INR. 0.50 per USSD session in November 2016 after complaints about the service ensuing form a public consultation on pricing.[305] TRAI has also pushed back against linking the number of menu trees to an increase in USSD

---

[299] Grameenphone, the largest MNO, charges all DFS providers - except bKash - up to 0.25% of the cost of the cash out value. Other MNOs charge 1.8% to 1.85% for cash out, of which the MNOs take 7% to 15%. For example, for a BDT 1000 cash out, the PSP charge to the customer is BDT 18.5. An MNO will get 7% of the BDT 18.5 amount.

[300] The Association of Mobile Telecom Operators of Bangladesh recently submitted its proposal to the Bangladesh Telecommunication Regulatory Commission to increase USSD fees. Daily Star (2016) *Telcos Propose To Hike Charge For Mobile Wallet Users,* available at https://goo.gl/TSrPLP

[301] Hanouch, M and Chen, G (2015) *Promoting Competition in Mobile Payments: The Role of USSD*, available at *https://bit.ly/1RFMIVY*

[302] Daily Sun (2018) *Session-based USSD price to raise mobile banking cost*, available at https://bit.ly/2z7uGHm

[303] Hanouch, M and Chen, G (2015) *Promoting Competition in Mobile Payments: The Role of USSD*, available at https://bit.ly/1RFMIVY

[304] Consultores, M (2015) *Going Mobile with Conditional Cash Transfers Insights and Lessons from the payment of Familias en Accion through DaviPlata wallets in Colombia*, available at https://goo.gl/fsvyfZ

[305] TRAI (2016c) *The Telecommunication Tariff (Sixty First Amendment) Order, 2016 No. – 1 Of 2016*, available at https://goo.gl/7kHo45. These moves coincided with a sudden demonetization program in November 2016 by the government

access costs, citing evidence that MNOs may, for their own customers, have more menus than they allow DFS SPs to have.[306] In November 2016, TRAI mandated an increase in the ceiling on number of menu stages from five to eight per USSD session and also reduced USSD pricing.[307] The outcome followed a consultation process initiated in August 2016.[308]

**Kenya:** Equity Bank complained of high STK access charges from market leader MNO Safaricom that made access to its mobile banking products uneconomical. It built an MNVO called 'Equitel' and used a thin-SIM to bypass Safaricom and using a cheaper STK from competitor MNO Airtel. [309]

**Peru:** The telecommunications regulator in Peru, Osiptel, issued standards to ensure fair and equal access of electronic money issuers to telecommunications services in 2014, including non-discriminatory pricing for access to USSD.[310] While these regulations were set by Osiptel, the central bank played a significant role in creating the regulatory framework around pricing for access.[311]

**Uganda:** A study on the wholesale USSD market as part of a broader Market Power Assessment by UCC found evidence of dominance by the MNOs with a potential to abuse.[312] Some TSPs and PSPs say that their customers experience QOS issues with USSD sessions but the TSP/PSP is unable to 'fix' the issue because some MNOs refuse to provide a QOS guarantee to them in their service contracts.[313] SPs have also alleged to the UCC that they may not have visibility of some failed USSD transactions.[314] The length, duration, quality and wholesale charges of USSD sessions used in DFS are the subject of an ongoing exploratory investigation by the UCC.[315] DFS SPs have complained about 'unjustifiably high' or unfair revenue share structures for USSD session fees.[316] These, in the view of the UCC, may be designed to foreclose independent DFS OSPs from the downstream DFS market segment.[317]

---

of India aimed at ridding the country of high value cash notes thought to be used for money laundering. DFS access surged in the wake of the demonetization announcement.

[306] First Post (2016) *TRAI Lowers Tariff For USSD Based Mobile Banking To A Maximum Of 50 Paise Per Transaction*, available at https://goo.gl/zF9ggZl, TRAI (2016d) *Information Note to the Press (Press release No 110/2016)*, available at https://goo.gl/V1qZJ0; TRAI (2016e) *ibid*

[307] TRAI (2016e) *The Mobile Banking (Quality Of Service) (Second Amendment) Regulations, 2016*, available at https://goo.gl/XwPxzn

[308] *ibid*

[309] In the case of Equitel in Kenya, use of the shortcode *247# will divert the session to use the Airtel network. See Equitel (2016) *Get Activated*, available at http://www.equitel.com/my-phone/get-activated.

[310] Mas, I (2014) *Shifting Branchless Banking Regulation from Enabling to Fostering Competition*, available at https://goo.gl/1Fb48a

[311] CGAP (2014) *Consumer Protection and Emerging Risks in Digital Financial Services Perspective from Bangladesh, Uganda, Colombia, and the Philippines,* available at https://bit.ly/2IaNMDK

[312] See Cartesian (2015) *Mobile Platform Access for USSD-based Applications (MPA-USSD),* available at https://goo.gl/8RrIq4

[313] In Uganda, service providers reported limited scope for negotiation of service level agreements with MNOs, that it was not possible to negotiate the level of service availability. Cartesian (2015) *ibid;* Macmillan Keck Attorneys & Solicitors & ACACIA Economics (2017) *Draft Non-Confidential Summary Of Final Report, Public Consultation Document, Support to the Uganda Communications Commission on USSD and SMS services*, available at https://bit.ly/2KbRXg3

[314] Macmillan Keck Attorneys & Solicitors & ACACIA Economics (2017) *ibid*

[315] *ibid*

[316] *ibid*

[317] *ibid*

**Zimbabwe:** In January 2017, the Zimbabwe Telecommunications regulator, POTRAZ set floor prices on access to MNO services. It had used a study of a bottom-up costing model[318] to determine pricing. Implementation of the new pricing, however, led to market confusion and massive retail price increases in mobile data, USSD, SMS, and voice call costs. This led to recriminations between POTARZ, the MNOs and consumers. Ultimately the retail price increases were suspended by the MNOs a few days after initial implementation.[319]

# 9 INFRASTRUCTURE QUALITY OF SERVICE

## 9.1 Overview

Customers are sensitive to issues of Quality of Service (QOS) in the telecommunications portion of DFS provision, as non-availability of services and poor service quality can have detrimental effects on access to stored value and user confidence the ecosystem.[320]

## 9.2 Role of NTA

QOS may relate to availability of mobile coverage; availability of time slots to set up, execute and properly retain/sustain calls, channel/bearer congestion; successful sending and receipt of SMSs, audio quality of calls, the rate of frequency of dropped calls; and data speeds.[321] With the move to packet rather than GSM-based circuit switched-based calls – for example using voLTE – issues of call-muting,[322] jitter, latency, end-to-end delay arise. Automatic fallback to traditional circuit switched - called circuit switch fallback (CSFB) – may also be necessary in QOS standards.

[318] There are two approaches to estimating unit costs: top-down, bottom-up. These can be combined to form a 'mixed approach'. A bottom-up approach is used to estimate the costs of service usage and involves identifying all resources used to provide a service, and then assigning a value to each of those resources. These values are summed and linked to a unit of activity to derive a total unit cost. Top-down costing is more amenable to estimating the society level costs which are often intangible and where data is scarce. See UK Cabinet Office (2017) *Top Down And Bottom-Up Unit Cost Estimation*, available at https://goo.gl/nZWX3M

[319] Techzim (2017) *New Tariffs - POTRAZ Says It Consulted The Mobile Operators, They Actually Wanted Even Higher Prices*, available at http://bit.ly/2isSXNz

[320] Mobile handset QOS parameters specified by NTAs are covered in Section 3.3.4.

[321] QOS parameters include the following, as contemplated by the Nigerian Communications Commission's QOS regulations: Call Completion Rate (CCR): The ratio of successfully completed calls to the total number of attempted calls (ITU-T E600/2.13). That is, the ratio of the number of completed call attempts to the total number of call attempts, at a given point of a network; Answer Seizure Ratio (ASR) is the ratio of the number of successful calls over the total number of outgoing calls from a carrier's network (i.e. On a route or a Destination Point Code (DPC) basis, and during a specified time interval, the ratio of the number of seizures that result in an answer signal to the total number of seizures: ITU-T E600/2.14); Call Setup Success Rate (CSSR) is the number of the unblocked call attempts divided by the total number of call attempts; the Dropped Call Rate (DCR) is the number of dropped calls divided by the total number of call attempts. See NCC (2018) *Quality of Service*, available at https://bit.ly/2rqXiIB

[322] Where poor network quality on packet switched calls and attempts by the MNO to keep the call connected results in audio not being heard by one or either parties for a few seconds. TRAI in India has issued a consultation paper on addressing the issue. See TRAI (2018) *Consultation Paper on Voice Services to LTE users (including VoLTE and CS Fallback),* available at https://bit.ly/2K3DLo7

NTA mostly have a turnkey and exclusive remit over mobile service provision.[323] *Ex ante,* they may include QOS and key performance indicators (KPI) parameters in licenses or may add additional parameters, *ex post,* as customer complaints increase.

In many cases, QOS parameters are self-reported every quarter[324] or may be the result of *de novo* QOS testing by the NTA using mobile 'testing' trucks which set up, execute and retain calls.[325] In India for example, TRAI conduct regular drive tests to check the quality of service of MNOs to make sure they are within set benchmarks.[326] TRAI has a free analytics portal for customers where the results of their testing and operator reports can be downloaded.[327] NTAs regularly issue fines to licensees if the QOS falls below minimum standards.[328] A similar portal is offered by the Nigerian Communications Commission (NCC).[329] In some cases, QOS may impact on license renewal.[330]

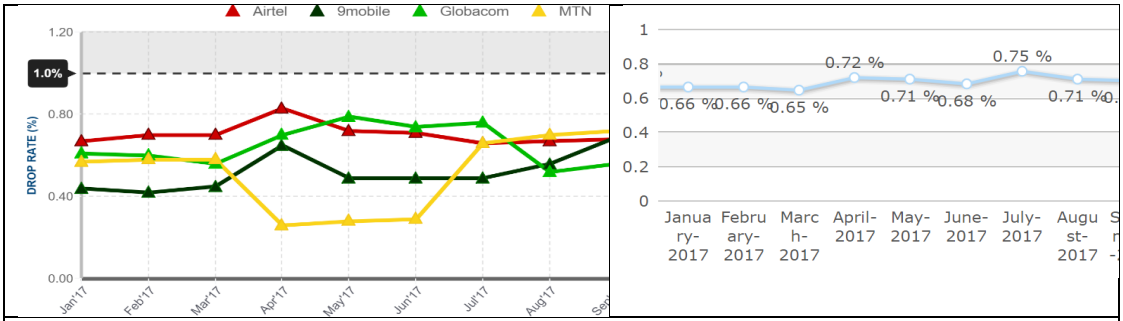



**Exhibit 11** Range of dropped call percentages for Nigeria (left) and India (right) as measured by the respective telecommunications regulators. Fines imposed by regulators have significant improved QOS relating to dropped calls.[331]

[323] Other regulators, departments and agencies may have associated remits over coverage provision, for example on spectrum allocation and policy, and on right of way for mobile tower installation. See further, Perlman, L & Weschler, M (2018) *Mobile Coverage And The Effect On Digital Financial Services,* available at www.dfsobservatory.com

[324] See for example the NCC in Nigeria, which requires QOS reporting from licenses every quarter. Vanguard News Nigeria (2017) *NCC Creates Minimum Service Quality For Telecom Industries*, available at https://bit.ly/2rsbss3

[325] Analysis is often done using monthly weighted averages based on data collected from MNO Network Operating Centers (NOCs) and during busy hours at the Base Station Controller (BSC). See on these parameters, NCC (2018) *ibid*

[326] TRAI checks the telecom operators network coverage, call quality, call drop rate, call success rate, blocked calls and carrier to interference ratio. These are measured against benchmarks set in QOS regulations. See TRAI (2017*) The Standards of Quality of Service of Basic Telephone Service (Wireline) and Cellular Mobile Telephone Service (Fifth Amendment) Regulations*, available at https://bit.ly/2rpVOhp. For QOS parameters in Rwanda, see RURA (2013) *Regulations For Quality Of Service Of Cellular Mobile And Fixed Networks Services*, available at https://bit.ly/2rrDtk4

[327] See updated TRAI QOS data at their analytics portal. TRAI (2018) *TRAI IDT,* avalable at https://bit.ly/2InFFns

[328] In Kenya, the NTA fined MNOs Safaricom, Airtel and Telkom Sh311 million (USD 3.1 million) for not meeting service standards for the 2015/16 financial year. Safaricom scored 62.5%, while Airtel and Telkom scored 75%, below the 80% required in terms of NTA regulations. See Capacity Media (2018) *The CA Fines Safaricom, Airtel And Telekom Kenya $3 Million For Poor Quality Of Service*, available at https://bit.ly/2wjL8pD

[329] NCC (2018) *Quality of Service*, available at https://bit.ly/2rqXiIB

[330] UCC (2018) *Application For Renewal Of A National Telecommunication License By MTN Uganda Limited*, available at https://bit.ly/2rou4tS

[331] Indian MNOs have requested that the NTA, TRAI lower QOS standards for call drop issues. See Money Control (2018) *INTERVIEW: Call drop a powerful consumer issue, not a theoretical construct, says TRAI chief*, available at https://bit.ly/2IsjmsI

### 9.3 Effect on DFS

QOS for DFS is often a co-competency between the central bank and the NTA,[332] especially in relation to USSD sessions – a primary user interface for DFS globally. Often USSD sessions drop, leading to a poor customer experience and maybe even loss of the customer's funds. This may dissuade customers from using the DFS service again, instead opting to use an over the counter (OTC) provider to do a transaction for them. The reasons for the dropped USSD session may be poor GSM signal,[333] network congestion or – as some TSPs and PSPs have alleged – deliberate throttling of their customer's USSD sessions.[334] Such drops may reflect poorly on the TSPs and PSP's service offering. That is, complaints from SPs allege that while MNOs may provide access, the QOS is poor, characterized by a high proportion of dropped USSD sessions that abruptly end before the customer session is completed.

As noted above, technical issues relating to GSM networks and coverage may be the issue although some SPs have alleged that they are being handicapped through implementation of random throttling or prioritizing of access.[335] Whether quality can be selectively degraded by the MNOs, and if they are doing so is a factual issue that can be further explored by a regulator in markets where these allegations arise.[336]

A competition study commissioned by the UCC indicated that TSPs and PSPs reported issues with service quality and that it was not possible for them to negotiate service level guarantees, nor be compensated for poor QOS and dropped USSD sessions.[337] Minimum QOS standards may also be embedded in MNO-SP contracts.[338] These may provide, in a USSD context, for the provision – if and where available - by an MNO to an SP of NI-USSD, which would be automatically initiated to resume a dropped user-initiated USSD session.

---

[332] On specific regulations for DFS access, see for example TRAI (2016e) *The Mobile Banking (Quality Of Service) (Second Amendment) Regulations*, available at https://bit.ly/2jIQx0x

[333] Mobile handsets & base stations must transmit enough power to maintain a call of acceptable quality or USSD session to completion without transmitting excessive power into the frequency channels & time slots allocated to others. See Keysite (2014) *Understanding GSM/EDGE Transmitter and Receiver Measurements for Base Transceiver Stations and their Components*, available at https://goo.gl/n6kqnF

[334] These QOS issues relate primarily to random, dropped USSD sessions affecting DFS SPs and aggregators. As noted by CGAP, selective degradation is technically possible, but is reportedly difficult to do and extremely difficult to prove. And as noted further by CGAP, even if a discrepancy in the quality of USSD is proven, it is not straightforward to identify the cause of the inferior quality. The point of failure could, for example, be with the DFS provider, the USSD gateway operator, or the MNO. See CGAP (2014) *Consumer Protection and Emerging Risks in Digital Financial Services Perspective from Bangladesh, Uganda, Colombia, and the Philippines,* available at https://bit.ly/2IaNMDK

[335] See further Hanouch, M & Chen, G (2015) *Promoting Competition in Mobile Payments: The Role of USSD*, available at https://goo.gl/kWZcUw; CGAP (2014) *ibid*

[336] CGAP (2014) *ibid*

[337] Cartesian (2015) *Mobile Platform Access for USSD-based Applications (MPA-USSD),* available at https://bit.ly/2KHrqY1

[338] See ITU FG DFS (2016) *QOS and QoE Aspects of Digital Financial Services*, available at http://www.itu.int/en/ITU-T/focusgroups/dfs/Pages/default.aspx. The report considers the appropriate role for telecommunications regulators in ensuring the provision of high-quality DFS and offers recommendations for telecommunications regulators on how to select Key Performance Indicators (KPIs) for DFS, including technical KPIs for bearer channels used with basic phones, feature phones and smartphones.

# 10 SECURITY ASPECTS

## 10.1 Overview

A number of vulnerabilities in the DFS ecosystem have been identified that, individually or in aggregate, can potentially disrupt and exploit flaws in mobile phones and networks. This can result in system disruption as well as data and financial loss to MNOs, SPs and their customers. NTAs in the developed world have recognized the issue and have initiated studies and procedures to mitigate these vulnerabilities. In the developing world uses of DFS, central banks have largely taken the lead however.[339]

These risks and vulnerabilities are both at the MNO infrastructure and customer levels. At the MNO-level, these include Signaling System 7-based exploits; USSD-based exploits;[340] and man-in-the-middle attacks using IMSI catchers.[341] New vulnerabilities have however been identified in LTE networks.[342]

**NTA Role:**
Ensuring security of the mobile and fixed interface to protect interception of voice calls, text and data; setting reporting standards for security breaches; Undertaking tests for IMSI catchers and other interception devices.

## 10.2 Signaling System Seven Vulnerabilities

Chief among the vulnerabilities in the DFS ecosystem are those in Signaling System 7.[343] SS7 is the connective tissue of most telecommunication systems around the world, allowing mobile and fixed line networks across the globe to seamlessly interact and, crucially, to allow effortless mobile roaming across MNOs.

The exchange of customer information between MNOs is required, achieved by using SS7 messages that are required to be exchanged between the networks.[344] However, this need for a seamless exchange between MNOs means that an attacker with SS7 access anywhere in the world can use legitimate functions of inter-MNO SS7 communications to send common but fraudulent SS7 messages that may allow them access to the core network functions of the attacked MNO. This can also potentially expose consumer information and facilitate fraudulent financial transactions.

Curiously, when SS7 was introduced in 1975,[345] it had not been designed with any security in mind as the only participants in international SS7 interactions at the time were trusted (mainly state-owned) fixed-line telecommunication operators. It was thought that this trusted group of operators would not cause or allow any security breaches. Any use of SS7 by bad actors today are therefore not 'hacks' of SS7 security *per se*, but exploitations of SS7's inherent lack of security by design.

**Exhibit 12:** The Origin of SS7 Vulnerabilities

Critically though, the need to facilitate roaming using SS7 introduces vulnerabilities in these networks and affects the core network and base stations at the extremities of the networks. These SS7 vulnerabilities

[339] See CBN (2018) *Regulatory Framework for the Use of Unstructured Supplementary Service Data (USSD) in the Nigerian Financial System*, available at https://bit.ly/2wLIcCm
[340] See Section 3.5.1 on USSD
[341] At the customer level vulnerabilities include application tampering and phone number spoofing
[342] Oodaloop (2018) *Researchers Publish Security Flaws In LTE* (4G), available at https://bit.ly/2uCaY45
[343] See Section 3.5.1 on USSD
[344] 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 MNOs Short Message Service Centre.
[345] See Teralight (2016) *The History of Signalling System #7,* available at https://bit.ly/2k1OOmR

can be exploited via the SS7 component 'MAP'[346] – which, as noted earlier, in turn powers USSD, one of the primary customer UIs for accessing DFS around the world.

This SS7-derived vulnerability is a systemic problem with all USSD-based mobile access systems, ostensibly allowing a bad actor with relatively basic telecommunications skills to perform dangerous attacks that may lead to direct customer financial loss, confidential data leakage, or disruption of communication services. This is not to say that these risks will always - or even practically can - come to fruition and that financial harm will always follow, but ventilating these risks allows for appropriate planning and risk mitigation by providers and customers. Indeed, for many of these vulnerabilities and the risks they create, there are available mitigants both at the SS7 and handset levels.

Several SS7-related intrusions have been reported, some with loss of value for customers. The reported cases included interception by bad actors of one-time passwords sent by banks as confirmatory SMSs of any account changes: the bad actors get account access, change payment beneficiaries, and intercept the OTP SMS from the bank to the real customer needed to authenticate the transaction. Other SS7-related studies have shown similar value theft via SS7.

### 10.3 IMSI Catchers

Bad actors can use fake MNO base stations, called 'IMSI Catchers' (ICs),[347] to surreptitiously extract customer data OTA at the edge of the mobile network. The IMSI Catcher allows the bad actor to impersonate any MNO by causing the customer's handset to connect to them. It can be used by hackers to intercept data from agent and customer handsets. Bad actors could potentially position themselves with these almost invisible devices near areas where DFS is likely to be used, such as at agent locations, G2P cash disbursement areas and markets.[348]While they were originally designed for law enforcement purposes only, advances in technology allow anyone to build an IMSI Catcher for under USD 400. These relatively easy to build devices take advantage of the SS7 vulnerabilities noted above and the fact that the GSM A5 series of encryption technologies designed to keep information safe when transmitted over GSM networks have all been compromised.[349] This is a classic man-in-the-middle-attack, which may lead to loss of customer data and compromising of the MNO's systems. In many countries, special permissions are required to import, own and operate these devices. In South Africa for example, they fall under a special category of equipment in South Africa designated for the interests of national security and can therefore only be bought with presidential authority. [350]

### 10.4 Role of NTA

The primary defense of SS7-based attacks is ordinarily the remit of MNO. Because of the innate insecurity of SS7, there are few preventative measures that can be taken by MNOs, but those that exist include

---

[346] *ibid*

[347] Also known as 'Stingrays.'

[348] Shaik, A, Borgaonkar, R, Asokan, N, et al. (2016) *Practical Attacks Against Privacy And Availability In 4G/LTE Mobile Communication Systems,* available at https://bit.ly/2rLEV13. Importation and use of commercial IMSI catchers usually requires a special license and end user certificate validated by national governments. Despite these ostensible precautions, commercial IMSI catchers have made their way into the wild. See thereto, Swingler, S (2016) *Meet The Grabber: How government and criminals can spy on you (and how to protect yourself)*, available at https://bit.ly/2IlRw5e

[349] Vijayan, J (2010) *Researchers Use PC To Crack Encryption For Next-Gen GSM Networks*, available at https://bit.ly/2rebrsa

[350] Swingler, S (2016) *Meet The Grabber: How government and criminals can spy on you (and how to protect yourself)*, available at https://bit.ly/2IlRw5e

'fingerprinting' software to check their SS7 systems for any suspicious activity or firewalls art critical part of the infrastructure. The role of NTA, if they recognize the potential of SS7 intrusions, is to put into effect risk management and breach reporting requirements for MNOs.

For ICs, there are only a few ways to detect their presence and usr. A number of providers have developed so-called 'IMSI Catcher Catchers' (ICCs)[351] that function by determining whether a mobile base station is suspicious. Two implementations of ICCs are currently in use: stationary and mobile. The other method is checking at a MNO level for signs ('fingerprinting') of IMSI catcher activity. A mobile ICC (mICC) can be operated by an MNO and/or a regulatory authority or a national intelligence network, and is usually placed in a surveillance truck. With a stationary ICC (sICC), a network of stationary measurement units installed on rooftops in a specified geographical area by a MNO and/or telecommunications regulator that constantly scans all frequency bands for cell announcements, and fingerprints any mobile network parameters that may cause suspicion.[352]

To integrate breach management responses and to develop cyber resilience frameworks, NTAs could also sign MOUs with other regulators and security-related entities such as Computer Emergency Response Teams (CERTs).[353]

### 10.5 Effect on DFS

Security is an industry wide problem, requiring all stakeholders to cooperate. This includes PPPs between the industry and NTAs especially since it has been shown that the ability to move funds via SS7 exploits has occurred.

As a result of the potential for bad actors to use IMSI Catchers at busy agent locations to undertake man-in-the-middle attacks and siphon customer and agent credentials, MNOs and regulators should cooperate in assessing and mitigating many of these risks through collegial cooperation between MNOs, SPs, telecommunications authorities and banks with the use of 'IMSI Catcher Catchers' and base station fingerprinting to discover and isolate fake base stations. Similarly, there is asymmetry in consumer liability in terms and conditions (T&Cs) which may be affected if it cannot be proven conclusively that MNO/SP is effectively impenetrable from hacking. Updated MOUs between the regulators involved in the DFS ecosystem to cover roles and responsibilities for network and access security

With the advent of interoperability[354] of DFS systems into the broader national payments infrastructure – for example, to ACHs and national switches – the percolating issue of systemic risk-based intrusions into these systems has heightened visibility. The issue of security thus manifests as a national issue, with an NTA amongst and possibly leading efforts at cyber resilience in the face of increased attacks on financial

---

[351] Dabrowski, A, Painata, N, Klepp, T, et al. (2014) *IMSI-Catch Me If You Can: IMSI-Catcher-Catchers*, available at https://bit.ly/2rAXd4X

[352] See also a new technique for detecting ICs using electronic fingerprinting. Zhenhua Li, Z, Wang, W, Christo Wilson, C, et al. *(*2018) *FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild,* available at https://bit.ly/2KU9gCz

[353] The first CERT was established in the US in 1988 to prevent attacks on internet backbones and sites. CERTs have now been established in a number of countries to provide national and regional responses to attacks. See Techtarget (2011) *What is CERT (Computer Emergency Readiness Team)?,* available at https://bit.ly/2Iufo6d

[354] See on interoperability in DFS, Economides, N & Jeziorski, P (2017) *Compatibility and Interoperability in Mobile Phone-Based Banking Networks*, available at https://ssrn.com/abstract=2944395

institutions, MNOs and even penetration of payment systems and central banks.[355] Many countries are not only developing these cyber resilience frameworks that impact multiple private and public stakeholders, but are also developing National Authorities whose remit it is to coordinate the cyber resilience plans and responses.[356]

These responses could include:

- MNOs should deploy hardware and software solutions that filter rogue SS7 messages derived from potential attackers
- Use of more intuitive Java-based applications for feature phones than unsecure text-based USSD menus
- Check apps for data leakage and potential for intrusion

NTAs should develop and implement risk management frameworks (RMFs) to anticipate, prevent, deal with, and mitigate the effect of any intrusions into their systems**.**

# 11 PRIVACY

## 11.1 Overview

As DFS evolves from its genesis as primarily a remittance-type service to a more transactional offering that includes services such as insurance, investments and credit provision, SPs may want better data sets to assist them in development of new products, assessing customer risk, and targeting the correct market segments.[357] In the telecommunications (use) context for example, Call Data Records (CDRs) captured in the course of their operations by MNOs are evolving from simply being flat records of telecommunications service use by individual customers to being the cradle of rich data insights made possible by the connective tissue of big data algorithms. This so-called 'exhaust' data scraped from these data sources can reveal a lot more on customer behavior and thus credit worthiness.[358] These metrics are the maximum types of data sets that can be derived from customers with feature phones,[359] augmented however if the MNO also provides DFS products.

**NTA Role:**

Ensuring that call records are not made available, unless with consent of customers; Ensuring security of the mobile and fixed interface to protect interception of voice calls, text and data; Preventing spam calls and texts, and spoofing

[355] In 2016, hackers stole USD 81 million from the central bank of Bangladesh - Bangladesh Bank. - in a sophisticated attack on its systems, and stealing its SWIFT codes. See Reuters (2018) *Bangladesh To Sue Manila Bank Over $81-Million Heist*, available at https://reut.rs/2G4pTcE t

[356] See Perlman, L (2018) *Security Aspects of DFS*, available at www.dfsobservatory.com

[357] See further on the nature of adverse selection and data sets, Mazer, P & Rowan, P (2016) *Competition in Mobile Financial Services: Lessons from Kenya & Tanzania*, available at https://goo.gl/osF8Mo*;* and generally on big data and DFS, Chen, G & Faz, X (2015) *The Potential of Digital Data: How Far Can It Advance Financial Inclusion*?, available at https://goo.gl/dxxSIU

[358] See San Pedro, J, Proserpio, D & Oliver, N (2015) *MobiScore: Towards Universal Credit Scoring from Mobile Phone Data*, available from https://goo.gl/Mkwp5T; Medine, D (2016) *Making the Case for Privacy for the Poor*, available at https://bit.ly/2k3rIfP

[359] Also through some feature phones that have Facebook, Twitter, and Whatsapp installed.

## 11.2 Role of NTA

While terms of license conditions are not usually visible, reading T&Cs of prepaid and DFS-related products – where available – can give insight into what data privacy restrictions, if any, are imposed on licenses under the remit of an NTA. TRAI in India has noted the potential for the emergence of data monopolies[360] and the need for regulations – at least for a need to bring in a set of regulations to ensure that consumer data remains safe and protected. In India, following the scandal surrounding Cambridge Analytica,[361] the government is to incorporate data security and privacy provisions into MNO licenses.

NTAs are known to be monitoring DFS transaction. For example, in Rwanda and Tanzania the NTAs have 'probes' inside the MNOs DFS servers and have real-time visibility over transactions, including numbers, value and type of transactions as well as their real-time liquidity position (including total cash-ins and cash-outs). MNO Safaricom in Kenya won an injunction in court against the NTA to halt its plans for installing a similar probe in their network.[362]

## 11.3 Effect on DFS

For provision of credit, be it short-term micro-credit or a longer term macro-credit product, providers need specific data sets to assess risk and credit worthiness.[363] The data is limited though: only 10% of people in eight sub-Saharan countries, for example, have verifiable online financial data.[364]

For many DFS markets, the most cogent data sets are often those that can be gleaned from mobile phone use, either from conventional telecommunications activity use, through transactional data in DFS or similar transactions obtained by DFS providers such as MNOs or through third party smartphone app providers.[365]

Harms may fasten on individual consumers, societal groups and society as a whole through data driven innovations [366] While many developed world and some developing world societies appear to have discarded or discounted privacy concerns for the sake of access to free or freemium type services (such as through free online email systems, or useful apps for their smartphones), the indiscriminate use of any collected data may have serious consequences for individual users. By way of example, inaccurate and discriminatory conclusions about a person's creditworthiness based on insufficiently tested or inappropriate algorithms or unanticipated aggregation of a person's data from various sources to draw conclusions which may be used to manipulate that person's behavior, or adversely affecting their

---

[360] Times of India (2018) *Data Monopolies Are Developing, There Is Need For Regulation: Trai Chief* , available at http://toi.in/ATX5IZ/a24gk

[361] Wired (2018) *Cambridge Analytica Shuts Down All Offices Amid Ongoing Facebook Crisis*, available at https://bit.ly/2wuEQn7

[362] Nation (2018) *Judge Blocks Plan To Spy On Private Telephone Calls*, available at https://bit.ly/2qLZcCg

[363] This information asymmetry, in a credit-provision context, may result in what is termed adverse selection, such that without a credit risk assessment – or credit score – the borrower will seek and often be given credit by lenders who are unable to obtain enough information on hand to have made a more seasoned determination of whether the loan would be repaid. Thus, those with access to cogent data sets will mitigate the risks of adverse selection. See further Mazer, P & Rowan, P (2016) *Competition in Mobile Financial Services: Lessons from Kenya & Tanzania*, available at https://goo.gl/osF8Mo

[364] Christensen P (2015) *Credit Where Credit Is Due*, available at https://goo.gl/h0Oapm

[365] Data can of course be gleaned from bank-related activity but this may be restricted through bank secrecy laws in some countries - for example Pakistan - which have often gotten in the way of sharing data that could otherwise be valuable in the hands of alternative financial providers. Here then, traditional credit providers benefit from their 'proprietary' data.

[366] Kemp, R & Moore, AD (2007) Privacy, available at https://doi.org/10.1108/07378830710735867

prospects of obtaining employment or credit. Even basic phones can provide and determine such results, which in environments where there is little financial literacy or technical literacy can have profound effects.[367] For example, 10% of the adult population is now negatively listed as bad borrowers in Kenya based on use of DFS and phone-derived credit identification. That is the algorithms assessed these persons as being creditworthy but were unable to properly assess their ability to service any loans provided.[368]

Even richer data sets can be gleaned from users with smartphones, who may use apps that reveal further information about them. For example, some new smartphone apps from DFS credit providers will request and obtain from the user consent to mine their contact lists, get device details, obtain biographical data in registration forms beyond that can be obtained in (often mandatory) SIM card registration, as well as track their calls, SMSs, instant messages, digital purchase habits and location.[369] This accumulated data becomes valuable in creating alternative credit scores and in facilitating the provision of credit to some of these profiled users. In many cases, however, users may not be aware data is being scraped and used as a basis for developing an alternate credit score or affecting current credit bureau scoring data. These privacy concerns have garnered the attention of some regulators.[370]

Entities who may be in a position to accumulate data used to create alternative credit scores may potentially use the data to their own advantage by not providing the complete data sets, as required to credit bureaus, and/or selectively providing the data only to preferred parties. Entities determined by regulators to have SMP – such as certain large MNOs - may be able to utilize their internal data for profit to the potential exclusion and detriment of smaller players who cannot obtain access to the same data. This may rise to an abuse of dominance if so determined by an authority.

Similarly, it may potentially rise to a competition concern of the NTA if the licensee does not share or properly share data whose collection and storage it effectively controls and, in the interests of equity, may have to share complete data on customers as mandated, for example in developing alternative credit scores for credit provision to DFS customers. Checking for and applying rules around this data provision may, of course, also (or only) be the remit of a credit regulator and/or competition regulator, where such exists, with the predicate enforcement trigger to the competition regulator where the licensee does not provide any such data or the data is incomplete.

In a recent survey by the ITU on consumer protection,[371] 83% of the contracts reviewed had clauses that permit the provider to share information with third parties, such as credit reference bureaus, law enforcement agencies (both domestic and international), regulators, provider agents, lawyers, auditors and

[367] Moerel, Lokke & Prins, Corien (2016) *Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things*, available at https://ssrn.com/abstract=2784123 or http://dx.doi.org/10.2139/ssrn.2784123

[368] Wright, G (2017) *Data- Is Digital Credit A Silver Bullet? CITI Webinar,* available at www.dfsobservatory.com

[369] In most cases prospective (and existing) users can only install and thus the app to get credit only if they agree to all these metrics being monitored. Similar data and results can be obtained by messaging and social network apps who have payment components added, such as those from Tencent's 'WeChat Pay' application in China, and social network behemoth Facebook's 'Messenger' application.

[370] See Government Of Kenya (2016) *Gazette Notice No. 678: Proposed Market Inquiry And Sector Study On The Kenya Banking Sector-Phase II By Competition Authority Of Kenya,* available at https://goo.gl/wbqDX6

[371] Anderson, CL, Reynolds, T, Aylward, C, *et al.* (2016) *DFS Consumer Protection Regulations*, available at https://bit.ly/2I4Rm1X

subsidiaries. The study also noted that 'sharing of customers' personal information is also permitted in some cases 'for reasonable commercial purposes related to the provision of services.' [372]

In the absence of a general data protection law and an overseeing agency, sector rules where they exist will apply. The African Union finally ratified the *Convention on Personal Data Protection* in January 2015.[373] Article 8 of the Convention calls for a strengthening of legal frameworks in relation to physical data.[374] The Convention will enter into force 30 days after the 15th instrument of ratification or accession in a member state is deposited, which as of the end of 2017 has yet to occur.[375]

# 12 CONSUMER PROTECTION

## 12.1 Overview

Consumer protection encompasses the following broad aspects and objectives:

- To prevent unfair practices by service providers
- To provide levels of comfort to consumers to transact

**NTA Role:**

Handling consumer complaints as the point of first instances; or acting as an ombudsman for consumer complaints; Enduring T&Cs conform to standards

## 12.2 Role of NTA

NTAs are tasked with providing consumer protection, at the very least, for services under their remit, that is for telecommunications related services. This will include regulations that outline responsibilities of the licensees in ensuring that consumers have enough information to make informed financial decisions and have access to recourse mechanisms to resolve disputes.[376] NTAs usually issue consumer protection rules through regulations.[377] Often these rules are placed in QOS regulations.

---

[372] For example, Airtel's Malawi's policy in relation to use of customer data is outlined in Section 2 of their online T&Cs says that: '2.1.4 You accept and confirm that we may disclose or receive personal information or documents about you:- **...** 2.1.4.2 [T]o and from our service providers, dealers, agents, or any other company that may be or become our subsidiary, parent company or partner, for reasonable commercial purposes connected to your use of the mobile service or Airtel money services, such as marketing and research related purposes.' See Airtel Malawi (2016) *Mobile Money Terms and Condition,* available at https://bit.ly/2G2cCzL. This internal policy appears then to allow Airtel to self-select, self-approve, and thus use customer CDRs - and any other customer data, it so appears – for commercial purposes. There is no opt-out provision for consumers.

[373] African Union (2014) *African Union Convention on Cyber Security and Personal Data Protection*, available at https://bit.ly/2xVAh5H

[374] Although physical data is not defined per se in the Convention, the context of this clause in relation to the preamble to the text indicates that it may apply to electronic and physical data.

[375] The Convention is thus not in force as of the end of 2017. Only 9 of the 55 AU member states had signed the Convention as of the end of 2017.

[376] See thereto, World Bank (2012) *Good Practices for Financial Consumer Protection*. Available at https://bit.ly/1wNE7ni

[377] In India, the Telecom Consumers Protection Regulations mandate licenses to (i) provide, through SMS or USSD, information alerts related to the consumer's data usage (ii) offer an alert immediately after a consumer roams outside the territory of India, advising the consumer to deactivate the data services in his mobile phone if he does not intend to use data services while roaming outside the country; (iii) to not activate or deactivate the data service without his explicit consent through toll free short code; and specify the validity of special Tariff Vouchers or Combo Vouchers or add-on-packs will be deemed to have been activated with consent till the expiry of the validity period of the voucher/pack or on the consumption of entire data, whichever is earlier.

The Communications Authority of Kenya's remit is to protect and safeguard consumers with regards to the provision of ICT.[378] In Kenya, consumers can report their complaints against licensed communication service providers to the Communications Authority if they reported to the service provider first and the issue was not satisfactorily resolved.[379] Based on the Kenya Information Communications Act, 1998, the authority can fine or penalize service providers that do not conform to the rules and regulations outlined by the Authority.[380] The relationship between Safaricom and the NTA – acting in relating to telecommunications and associated competition issues - continues to be fractious.[381]

The Nigerian Communication Commission (NCC) provides minimum QOS standards for the telecommunication industry[382] with a 'Number of Customers Satisfaction Index' of the percentage of the number of customers satisfied with the services of an operator in randomly distributed samples of customers.[383] For service complaints, consumers can file complaints via a toll free telephone line, online consumer web portal, social media as well as written complaints.[384] The NCC's 2018 Consumer Code of Practice Regulations outlines complaint-handling mechanisms.[385] The NCC either forwards the complaint to the licensee if the consumer has not first contacted the provider or investigates the complaints.[386] Where there are multiple regulators who may have remit over consumer protection, potential arbitrage is usually mediated by inter-regulator MOUs.

In many cases, the NTA will be the primary point of contact for redress of consumer complaints, often referring a complaint it receives back to the licensee affected.[387] The NTA may also liaise with an internal or external ombudsman. In India for example, TRAI has recommended that an Office of Telecom Ombudsman be established to address grievances of telecom consumers and to have a new and specific funding mechanism. [388]

---

[378] Communications Authority of Kenya (2014) *The Role of the Communications Authority of Kenya in Consumer Protection,* available at https://bit.ly/2I9r7Ua

[379] Communications Authority of Kenya (2018) *How to Make a Complaint,* available at https://bit.ly/2GoxQI4

[380] Communications Authority of Kenya (2014) *The Role of the Communications Authority of Kenya in Consumer Protection,* available at https://bit.ly/2I9r7Ua

[381] In August 2018, the CA fined Safaricom USD 4.5 million after it found it culpable of blocking calls from the smaller telcos, Elige Communications Ltd and Geonet Communications. Safaricom obtained an injunction against the CA pending a review of the case.

[382] NCC (2018) *Quality of Service,* available at https://bit.ly/2IeBYMw

[383] The index includes the Speed of Problem Resolution; Number resolved problems in day one; Total number of problems received on day one; % cleared in three days and above; and the total number of problems received on day one. See NCC (2018) *QOS Metrics and Definitions,* available at https://bit.ly/2rzZf4w

[384] NCC (2018) *Consumer Complaints,* available at https://bit.ly/2Ib0I8E

[385] NCC (2018) *Draft Consumer Code of Practice Regulations 2018,* available at https://bit.ly/2IbNmc7

[386] NCC (2018) *Consumer Complaint Procedures,* available at http://consumer.ncc.gov.ng/consumer-complaints-info/; NCC (2018) *Draft Consumer Code of Practice Regulations 2018,* available at https://bit.ly/2IbNmc7

[387] In India, TRAI has Telecom Consumers Complaint Monitoring System (TCCMS). The TRAI disclaimer is that In terms of the TRAI Act, 1997, that it does not envisage handling of individual consumer complaints and advises consumers to take up their complaints with their respective service providers. Complaints, if any, received in TRAI are forwarded to the service providers and no follow up action is taken by TRAI on individual complaint(s). See TRAI (2018) *TCCMS,* available at http://www.tccms.gov.in/

[388] Through the Ombudsman, a three-stage grievance redress mechanism for telecom sector is proposed that includes — resolution by TSPs, resolution by Consumer Grievance Redressal Forum (CGRF) — and determination by Telecom Ombudsman. A portion of the existing, not in addition, license fee may be the funding mechanism for the Ombudsman, from a fixed fee plus a variable component payable by each licensee depending on the volume of complaints being filed against it and admitted before the ombudsman's office. TRAI also has an online portal for lodging complaints. TSPs will be required to

### 12.3 Effect on DFS

Consumer surveys[389] on DFS across four continents have identified the following risks as being top of mind for BOP customer to whom DFS is targeted:[390]

- Service downtime
- Agent liquidity
- Data privacy and protection
- PIN security
- Customer recourse and support
- Incorrect transactions
- Agent Overcharging
- Transparency
- Unclear Pricing

From a review of the consumer protection regimes around the world, often many of the consumer protection goals and concerns are not addressed, at least not within the context of the remit of the consumer protection regimes that NTAs may develop and oversee of their licensees.[391] Usually then and in the absence of a coordinated omnibus consumer protection regime, consumer protection in DFS is often punctuated by patchworks of available remedies, confusion as to the role of each authority and a complaints and resolution infrastructure that is seemingly burdensome and expensive for consumers to lodge complaints; to have these complaints properly ventilated and investigated; and to then seek ultimate redress.[392]

On a practical level, consumers may not have seamless means to lodge complaints. In many cases and, except for MNOs own customers to call their DFS customer care centers, there do not appear to be universal toll-free numbers provided by the NTAs who many have remit over consumer protection in DFS. This means that valuable mobile airtime value could be used to lodge a complaint, such that the cumulative cost of the calls may ultimately exceed the value of the redress sought.

The Indian NTA, TRAI sets quality of service regulations for mobile banking transactions and USSD based mobile banking and payment services which includes requirements on delivery of messages, quality of service, security, reporting and access to provider.[393] If services are not satisfactory, consumers can file

---

maintain video calling facilities at their local offices, which can be used by the consumer to interact with the CGRF or ombudsman's office, in case it is required. See Hindu Business Line (2018) *TRAI To Centre: Appoint An Ombudsman To Address Telecom Consumers? Grievances*, available at https://goo.gl/7ctXgK

[389] CGAP (2014) *Consumer Protection and Emerging Risks in Digital Financial Services Perspective from Bangladesh, Uganda, Colombia, and the Philippines,* available at https://bit.ly/2IaNMDK

[390] These appear to be universal consumer concerns, and as such can reasonably be similarly applied to Malawi.

[391] See thereto, Mauree, V (2016) *Regulatory Issues for Consumer Protection in Digital Financial Services*, available at https://bit.ly/2KSyFfT

[392] Mauree, V (2016) *Regulatory Issues for Consumer Protection in Digital Financial Services*, available at https://bit.ly/2KSyFfT; Anderson, CL, Reynolds, T, Aylward, C, *et al.* (2016) *DFS Consumer Protection Regulations*, available at https://bit.ly/2I4Rm1X

[393] TRAI (2012) *Mobile Banking (Quality of Service) Regulations, 2012*, available at https://bit.ly/2GqSfwb

a complaint at the complaint center and, if not addressed satisfactorily, to the appellate authority established by the service provider under the Telecom Consumers Complaint Redressal Regulations,[394] A Telecom Consumer Complaint Monitoring System allows consumers to lodge and view the status of their complaint.[395] Recently, a three-tier complaint mechanism was also proposed. If the issue is still not resolved by the appellate authority, the consumer can report to the new ombudsman, which will be formed under the TRAI, and will report directly to the Telecom Secretary.[396]

The Ugandan NTA, the UCC is responsible for supervising and licensing mobile network operators. They also ensure telecommunication networks are effective, reliable and robust. If the telecommunication services are poor and they are not satisfied with the response of the provider, consumers can also report to the Consumer Affairs Office of the UCC.[397]

In Jordan, the Central bank of Jordan and the NTA, the Telecommunications Regulatory Commission have an MOU that specifies which regulator has which remit over which aspect of a consumer complaint, for example, whether there is a value loss and the telecommunications component is the proximate or full cause of the loss. And in Malawi, the Malawi Communications Regulatory Authority (MACRA) has a Consumer Affairs Unit designated to directly process and investigate consumer complaints.[398] In practice, however, MACRA do not undertake any initial customer complaint assessments, but instead will refer a consumer's complaint received back to the MNO or DFSP. Only if it is unresolved after 14 days will MACRA step back in to address the complaint.

# 13 Taxation

## 13.1 Overview

Mobile connectivity and even DFS services aimed at the financially excluded is often seen by NTAs and the (national) treasuries[399] as a deep well of revenue. Indeed, mobile devices – even the most basic types – are perceived by NTAs as luxury goods. Associated goods and services such as SIM cards and prepaid mobile airtime are also taxed higher than other sectors. Some or all of the taxes applicable to telecommunications or DFS services may originate from the NTA, either as a directly recipient of a tax, or as advisor to the fiscas in identifying taxes to apply or regulation of the tax collection process. The taxes may find their way to the NTA, but are invariably given to the national fiscas, who may then provide the NTA with some of the (taxed) revenue. Governments often also tax MNOs and their customers more than other standard goods and services. The range of taxes applicable to telecommunications and DFS-related services include Value Added Tax (VAT); mobile sector specific taxation such as excise duties, and regional/state taxes, and local right of way charges. Taxes can also be applied to imported hardware, spectrum use, and mobile airtime.

---

[394] TRAI (2012) *Telecom Consumers Complaint Redressal Regulations, 2012,* available at https://bit.ly/2GoDDNT

[395] TRAI (2018) *Welcome to The Telecom Consumers Complaint Monitoring System (TCCMS),* available at http://www.tccms.gov.in/

[396] Dovall, P (2018) *Soon, You Will Have Ombudsman To Address Telecom Complaints,* available at https://bit.ly/2L7QE1N

[397] UCC (2018) *Complaint Handling Procedure,* available at https://bit.ly/2wPShOQ

[398] The MOUs that the NTA has in place with other regulators with remit over DFS and provide for the parties to notify one another where there concurrency in the cases brought to them. The MOU also provides for referral of cases.

[399] Also known in some countries as the national treasury

**NTA Role:**
Taxation of mobile airtime value; social media tax; USF tax; taxation on SIM card sales; taxation on DFS transactions.

### 13.2 Role of NTA

A comprehensive study on taxation on MNOs and associate services issued by the GSMA[400] draws on data from 30 developing countries and indicates that while many governments recognize the role of mobile in supporting digital connectivity and the related benefit for social development and economic growth, tax treatment of the sectors is not always fully aligned to the objective of advancing connectivity. That is, government's tax MNOs and consumers more than other standard goods and services.

The Tanzanian NTA introduced a 14.5% excise duty on all mobile devices in 2014 in addition to an excise duty of Sh 1,000 on each SIM card sold.[401] Rwanda's excise duty is 8% and Kenya 10-12%.[402] In Uganda, a 10% tax is levied on fees for all DFS transfers[403] while a tax of 14% levied on revenues from all mobile services including DFS.[404] A controversial new 1% tax on all social media activity undertaken on mobile phones was introduced in June 2018.[405]

The GSMA study indicates that Jamaican MNOs pay a 20% import duty on network equipment, a special telephone call tax of USD 0.004 per minute of call as well as a Universal Service Contribution.[406] In Nepal, mobile operators pay a Telecom Service Charge on revenues from calls and SMS, of which the rate was increased to 11% from 10% in 2015, a Rural Telecom Development Fund of 2% of revenues and an ownership tax of 2% on SIM cards and recharge cards.[407] And in Jordan, NTA-imposed tax on mobile airtime is an astounding 45%.[408] A GSMA study showed that in the 2013/14 financial year, the Tanzanian NTA introduced a 14.5% excise duty on all mobile devices as well as an excise duty of Sh1,000 on each SIM card sold.[409] Rwanda's excise duty is 8% and Kenya 10-12%.[410]

In Nigeria, some MNOs have rebelled against what they term 'unapproved taxes' levied by state governments, such as an Environmental Sanitation levy, generator emission tax.[411] They are threatening to abandon mobile base stations sites where these taxes are supposedly applicable. Altogether some 38 different taxes and levies are fastened on the MNOs per base station. The MNOs have petitioned the Nigerian president to declare telecommunications infrastructure as critical national infrastructure to address the problem of shuttering of base station sites in the country.[412] Similarly, in India, the government

---

[400] GSMA (2016c) *Digital Inclusion And Mobile Sector Taxation 2016*, available at https://bit.ly/2KcKJHB
[401] All Africa (2017) *Tanzania: Cellphones Now Overtake Beer in Tax Contribution*, available at http://allafrica.com/stories/201708180268.html
[402] *ibid*
[403] Afadhali, J (2016) *Taxes hindering growth of mobile services in Africa, new report says,* available at https://bit.ly/2jRrf0c
[404] BBC (2013) *Uganda to tax mobile money transfers,* available at https://bbc.in/2IBSdHe
[405] CNN (2018) *Violent Protests Force Uganda Government To Review Social Media Tax*, available at https://cnn.it/2zuyJRj
[406] GSMA (2016c) *Digital Inclusion And Mobile Sector Taxation 2016*, available at https://bit.ly/2KcKJHB
[407] *ibid*
[408] *ibid*
[409] All Africa (2017) *Tanzania: Cellphones Now Overtake Beer in Tax Contribution*, available at https://bit.ly/2L7J9Im
[410] *ibid*
[411] Nigeria Communications Week (2018) *Telcos May Switch Off GSM Services in S/East, Others over Taxes*, available at https://bit.ly/2KRkasM
[412] The head of Association of Telecommunications Companies of Nigeria has indicated that the association's members do not see any viability in further investing in an environment that appears hostile to them and that until the government seriously

is attempting to streamline the regulatory environment to avoid the current situation of multiple agencies having remit over MNOs, and each levying some tax or levy on the MNOs.

### 13.3 Effect on DFS

A separate GSMA study[413] on Kenya, Tanzania[414] and Uganda indicated a 10% excise duty on DFS transaction fees, while Zimbabwe has imposed a USD 0.05 tax on each DFS transaction, with the Democratic Republic of Congo planning to introduce a 3% mobile money tax on turnover.[415] In Tanzania, fees collected on DFS transactions were around US$ 8.7 million in the third quarter of 2016.[416]

## 14 CONCLUSIONS

This study demonstrates the evolving and increasing complex role of National Telecommunications Authorities (NTAs) in their role in regulating components in the provision of Digital Financial Services (DFS) in the developing world.

DFS in many countries is in ubiquitous use as a payment and value transfer mechanism and, in some cases, has systemic effect on the entire financial system. The telecommunications components of DFS over which the NTA often has exclusive remit, thus ascends to similar systemic considerations, requiring the NTA to properly and carefully exercise its remit on those components.

Regulation is complex: policy objectives behind regulation before they translate into regulatory frameworks and tools require in-depth investigation of market dynamics and issues of *inter alia* competition, market entry and market structure (including through licensing), and dynamics that affect market ignition, rapid growth and market power, as well as capital-intensive investment and network effects.

NTAs thus need to understand DFS markets to understand how to ensure telecommunication services can effectively serve them since financial services run across them; and how telecom services markets are affected by them since lock-in feedback loop network effects can even have an impact on the telecommunications market.

DFS though, we find, often stretches a NTA's competency beyond a 'traditional' telecommunications-related focus to now also include issues of financial inclusion; financial service provision; interoperability between payment systems; blended and integrated customer identification (CIV) and verification processes; monitoring of money laundering; quality of payment user interfaces (UIs); as well as issues of payment and infrastructure security, competition, and fraud.

---

addresses the multiple taxation issue, multiple regulation and the harmonization of taxes and removal of exorbitant Right of Way charges applied to its members. Nigeria Communications Week (2018) *Telcos May Switch Off GSM Services in S/East, Others over Taxes*, available at https://bit.ly/2KRkasM

[413] GSMA (2017a) *Taxation And Mobile Money In Tanzania*, available at https://bit.ly/2rHwpiX

[414] GSMA's analysis of Tanzania showed that MNO fees collected as DFS taxes amounted to around USD 8.7 million in the third quarter of 2016, which the GSMA estimates to be around 0.09% of the Tanzanian government's total expenditure of around USD 9.23 billion for that quarter. GSMA (2017) *op cit*

[415] GSMA (2017b) *Rethinking Mobile Money Taxation,* available at https://bit.ly/2IyvAmF

[416] GSMA (2017a) *Taxation And Mobile Money In Tanzania*, available at https://bit.ly/2rHwpiX. Around 0.09% of the Tanzanian government's total expenditure of around US$ 9.23 billion for that quarter

Key to the NTA's role in facilitating frictionless use of DFS is hardening the telecommunications components of DFS through *inter alia* promoting or mandating ubiquitous universal service-based national mobile coverage, with defined pathways for national provision of broadband mobile coverage that allows movement from current dependencies in many parts of the developing world on 2G-type text-based DFS UIs such as USSD and STK.

These movements are, however, dependent to a large degree on complicated and long-term initiatives by NTAs to provide 'digital dividend' mobile spectrum seen as best suited for provision of broadband mobile coverage across large swatches of DFS-dependent rural areas.

Adjacent but equally important NTA priorities relating to DFS include ensuring that licensees harden security of mobile bearer channels and ensuring that quality of service of the bearer channels is maintained to ensure customer confidence in their ability to reliably complete DFS transactions.

NTAs, in undertaking mandated mass single-day national switch-off of phones with fake IMEI numbers, should coordinate such events with at least the central bank along with a mass publicity campaign lest the resultant mass inability of users to access value in their mobile wallets leads to disruption of, and decreased user confidence in, the DFS and broader financial ecosystem. NTAs should also develop and implement risk management frameworks to anticipate, prevent, respond to and mitigate the effect of any intrusions into their systems**.**

Competition-related issues that affect fair access for the telecommunications and agent-related access to the DFS ecosystem involve more complex market inquiries and responses to findings and complaints from the NTA. Access at fair, reasonable and non-discriminatory terms to scarce mobile bearer channels and components such as shortcodes, USSD and STK have proven particularly difficult to enforce given the challenges in investigating and proving any abuse of dominance.

Similarly, NTAs often send mixed signals to market participants on the desirability of agent exclusivity provisions by not reconciling the NTA's exclusivity policies relating to agents providing mobile signup and airtime services for one provider exclusively, versus the NTA's mandated non-exclusivity provisions for the same agents providing DFS signup and CICO services.

We find that many of these complexities arise from determining which authority has competition-related competencies for particular component of the DFS ecosystem. Determinations of which authority has competency over the issue may further delay remedies. These require coordination then with other regulators who may have similar competencies: we suggest that to avoid any expected regulatory arbitrage, NTAs should sign - or update, as needed - MOUs with other regulators that have sectoral but similar remit over components of the DFS ecosystem. NTAs should also augment and provide appropriate technical assistance to the other authorities where needed.

To catalyze DFS services, NTAs could also provide incentives for providing critical infrastructure used in service provision. This may include lowering taxes – in conjunction with the fiscus – or type approval costs on mobile infrastructure, as well as scrapping taxes on handsets that could be used exclusively by merchants as replacements for expensive dedicated POS equipment.

Coordinating these responses in relation to the specific DFS-related technical and regulatory needs requires identification of the issues and a strategy for dealing with them: this, we suggest could fall under a specific financial inclusion strategy of the NTA or contribution by the NTA to a national financial inclusion strategy if one exists.

This strategy should include the NTA providing an enabling regulatory and environment for DFS that promotes the widest possible provision of DFS, including allowing MNOs to directly participate in the DFS ecosystem and not just be restricted to acting as a bearer network or provider of an agent network for banks or third party DFSP.

And while there are cogent financial inclusion reasons for extending the universe of entities able to legally provide DFS, the corollary is that the NTA should not attempt to extend their remit to DFSPs - as has been done in some countries - where there is no jurisdictional basis for doing so. Any overreach may have the effect of hindering financial inclusion. Nor should the NTA's remit unilaterally be extended to matters of financial interoperability and integration into a national payment system, unless undertaken as part of a national strategy alongside other authorities.

An important component of properly regulating the DFS ecosystem is the importance of collaboration between for example, central banks, NTAs and competition authorities for them to understand each other's markets and their feedback loop effects. While an MOU is critical to connecting them and ensuring certainty in remits, collaboration required must be more than an MOU. It should include exchanges of data and analysis on the regulators' respective markets where data can be legally shared as well as coordinating on specific aspects of the DFS ecosystem.

It is clear though that increasing complexities offered through the emergence of DFS, that any expansion or clarification of the NTA's DFS-related remit requires reviewing not only of its existing internal capacity but also its ability undertake capacity building where necessary to properly and efficiently interact with market participants and other authorities.

Annex A: **Example of an MOU Between a NTA and Central Bank**

Establishment page from the MOU between the Malawian NTA, MACRA and the central bank, the Reserve Bank of Malawi on regulating DFS in Malawi.[417]

Dated this ..16th.. day of ..December..2013

**THIS MEMORANDUM OF UNDERSTANDING** (MOU) is made this 16th day of December 2013 **BETWEEN RESERVE BANK OF MALAWI,** Post Office Box 30063, Lilongwe 3, having its office along Convention Drive, City Centre, Lilongwe, hereinafter referred to as 'the Bank' AND **THE MALAWI COMMUNICATIONS AND REGULATORY AUTHORITY**, Private Bag 261, Blantyre, having its registered office at MACRA House , Salmin Armour Road in Blantyre (hereinafter referred to as 'MACRA').

**WHEREAS:**

1. The Bank is established under the Reserve Bank Act , Cap 44 : 02 of the Laws of Malawi in order to , inter alia , regulate , oversee, monitor payment systems in Malawi ;

   MACRA is established under the Communications Act Cap 68:01 of the Laws of Malawi in order to, inter alia, regulate the communication sector including licensing and oversight of mobile network operators (MNOs) who are also mobile money transfer service operators;

**AND WHEREAS-**

There exist a potential overlap between the functions of the Bank and MACRA in mobile payment transactions, as the Bank has general powers in relation to financial transactions, whilst MACRA has general powers on provision of mobile communication services.

**NOW THEREFORE,** the parties agree to conclude this Agreement as follows:

2

[417] RBM & MACRA (2013) *Memorandum of Understanding Between the Reserve Bank of Malawi (RBM) and The Malawi Communications Regulatory Authority (MACRA)*, available at https://bit.ly/2ILIVs8

## Annex B: **Radio Frequencies In Use In DFS-focused Countries**[418]

| Frequency | Type of use | Region used |
|---|---|---|
| 450 MHz | Superior propagation characteristics but substantially less capacity. Originally 1G analog telephone service in Scandinavia, Saudi Arabia, ultimately 30 countries. Used sparsely for public 4G LTE 450 (Band 31) mobile networks. LTE-450 promoted in Brazil since 2012 but currently unsuccessful. | Used in Russia, Scandinavia, limited usage in continental Europe (excluding the UK) and Southeast Asia. Used in smaller countries, Aland Islands, Armenia, Indonesia and the Philippines. |
| 700 MHz | Primarily being deployed for 4G.<br>Caribbean (Belize, Bahamas, Antigua and Barbuda, Cayman Islands, Turks and Caicos Islands) Kiribati, Papua New Guinea, Bolivia, Chile, Guam. *Other:* US, Canada, Caribbean, South America, Australia, New Zealand. Taiwan, France. | 700 MHz is planned for worldwide deployment but most common is in ITU Region 2 (North America, LATAM) |
| 850 MHz | 2G is still ubiquitous. When re-farmed, primarily for 3G with some 4G LTE. All deployments 2G and 3G unless otherwise noted.<br>American Samoa, Bhutan, Bolivia, Brazil, Chile, Costa Rica, British Virgin Islands, Curacao (3G), Dominica, Dominican Republic, Ecuador, El Salvador, Guam, Suriname, Venezuela, Virgin Islands, Guatemala (3G/4G), Honduras, Indonesia (4G), Malaysia(4G), Mexico, Panama, Pakistan (4G), Paraguay, Peru, Nicaragua, Montserrat, Northern Mariana Islands, Anguilla, Antigua and Barbuda, Bahamas (3G), Argentina, Belize (3G), Bermuda (3G), Haiti, Jamaica, St. Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Turks and Caicos, Philippines (3G,4G), Bonaire Islands; *Other:* Australia (4G), United States (4G), Canada, South Korea (4G), Kazakhstan. | 850 MHz most common deployment in ITU Region 2 (North America, LATAM) |
| 900 MHz | 2G coverage still ubiquitous in region. 900 MHz has and is being re-farmed for 3G and 4G uses in many countries. ***(3G):*** Angola, Myanmar, Chile, Djibouti, Dominican Republic, Fiji, Ghana, Macau, Macedonia, Malta, Sao Tome and Príncipe, Samoa, South Africa, Tunisia, Vanuatu, etc.) Indonesia (4G) | 900 MHz band most common deployment in ITU Regions 1 and 3 (Africa, Europe, Middle East, Asia) |
| 1700 MHz | Primarily used for 3G, 4G in Canada, Chile, Colombia (4G), Dominican Republic (4G), Ecuador (4G), Guam (4G), Mexico (4G), Paraguay (4G), Peru (4G), Puerto Rico (both), US (both), Uruguay (4G),Venezuela (4G) | |
| 1800 MHz | 2G coverage still ubiquitous in region. When re-farmed, 1800 MHz is primary deployed for 4G use (in addition to 2G) and noted where only 4G implemented.<br>***(4G):*** Venezuela (4G only), Afghanistan, Angola, Aruba (4G only) Bahrain (4G only), Belarus (4G only), Bhutan, Brazil, Costa Rica (4G only), Ivory Coast, Croatia, Dominican Republic, Estonia, Fiji, Guinea-Bissau, Indonesia, Isle of Man, Jordan, Kazakhstan (4G only) Kenya, Latvia, Malaysia, Mauritius, Montenegro, Pakistan, Philippines, Slovenia, Slovakia, South Africa, Sri Lanka, Tajikistan, Venezuela. | 1800 MHz band most common deployment in ITU Regions 1 and 3 (Africa, Europe, Middle East, Asia) |
| 1900 MHz | 2G coverage still ubiquitous in region. Primarily used for 3G and sometimes 4G.<br>***(3G and 4G):*** Afghanistan (3G) Anguilla (3G), Bermuda (3G), Brazil (2G and 3G), Colombia (2G and 3G), Burundi (3G), El Salvador (2G and 3G), Guatemala (2G and 3G), Honduras (2G and 3G), India (3G), Moldova (3G), Mongolia (3G), Nicaragua (2G and 3G), Paraguay (4G), Peru (4G), Argentina (3G), Armenia | 1900 MHz most common deployment in ITU Region 2 (North America, LATAM) |
| 2100 MHz | Substantially used worldwide to provide 3G service and 4G in developed countries.<br>***(3G):*** Afghanistan, Albania, Algeria, Andorra, Angola, Antigua and Barbuda, Aruba, Azerbaijan, Bahrain, Bangladesh, Barbados, Belarus, Benin, Bhutan, Bonaire Islands, Brazil, British Virgin Islands, Myanmar, Burundi, Cambodia, Cameroon, Cape Verde, Cuba, Curacao, Djibouti, Dominica, Ecuador, Egypt, Estonia, Ethiopia, Faroe Islands, Fiji, Ghana, Guinea, Guyana, Haiti, India, Indonesia, Iran, Iraq, Jamaica, Malaysia, Mali, Malta, Mauritania, Mauritius, Mexico, Moldova, Mongolia, Montenegro, Mozambique, Namibia, Nauru, Nepal, Nigeria, Pakistan, Panama, Philippines, Rwanda, Saint Kitts and Nevis, Saint Vincent and the Grenadines, Samoa, San Marino, Sao Tome and Principe, Senegal, Seychelles, Sierra Leone, Sri Lanka, Sudan, Suriname, Syria, Tanzania, Thailand, Trinidad and Tobago, Tonga, Uganda, Uruguay, Venezuela (4G), West Bank, Zambia, Zimbabwe. | Primarily used for providing 3G (worldwide) and sometimes 4G (US, Central and South America, Caribbean) |
| 2300, 2600 MHz | Primarily used for providing 4G worldwide including Austria, India, Indonesia, Mozambique, Nigeria, Oman, Russia, Saudi Arabia, Sri Lanka | |

[418] Data from Perlman, L & Wechsler, M (2018) *The Role of Mobile Coverage on Digital Financial Services*, available at www.dfsobservatory.com