International Telecommunication Union

ITU-T Technical Report

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(05/2019)

DSTR-DFSREG

Digital financial services – Regulation in the digital financial services ecosystem

Summary

Regulations may enable or thwart a healthy digital financial services ecosystem and therefore the potential to realize the goals of financial inclusion. Moreover, given the complexity of the DFS regulatory environment, it remains imperative that the two sector authorities involved in these efforts – financial services and telecommunication – collaborate to address these issues.

This Technical Report outlines the categories of regulation, defines the corresponding sub-issues or topics and highlights the financial inclusion of each topic. Key categories include

1) agents,
2) consumer protection,
3) market access,
4) payments systems,
5) risk management and
6) other related issues.

This Technical Report also addresses key issues related to managing the regulatory environment. It outlines a survey of how regulators currently work together, provides a draft memorandum of understanding template for Authorities in a given country to formally outline joint goals and methods of working together, and outlines considerations if regulators are interested in formalizing cross-border collaborations.

Keywords

Ecosystem, digital financial services, regulation.

Change Log

This document contains the ITU-T Technical Report on "*Digital Financial Services – Regulation in the Digital Financial Services Ecosystem"* which was agreed by the ITU-T Study Group 3 meeting held in Geneva, 23 April - 2 May 2019.

CONTENTS

Technical Report ITU-T DSTR-DFSREG

Digital financial services – Regulation in the digital financial services ecosystem

1 Scope

See Summary.

2 References

None.

3 Terms and definitions

3.1 Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

None.

3.2 Terms defined here

This Technical Report defines the following terms:

None.

4 Abbreviations

AML Anti-Money Laundering

CFT Combatting the Financing of Terrorism

DFS Digital Financial Services

KYC Know Your Customer

MNO Mobile Network Operator

MOU Memorandum of Understanding

5 Introduction

The Ecosystem Working Group of the ITU DFS Focus Group was tasked with providing a comprehensive listing of the regulatory issues in the ecosystem. This is a very important part of the ecosystem, as regulations may enable or thwart a healthy digital financial services ecosystem and therefore the potential to realize the goals of financial inclusion.

This Technical Report categorizes the issues and highlights the financial inclusion perspectives of each topic. The group also considered the issues of managing the regulatory environment, particularly given the intersecting domains of financial and telecommunications regulation.

Note that the interconnections and effects of one regulation on another were considered outside of scope but should be considered within a country context. Furthermore, the effects of specific country contexts or conditions were not considered in this Technical Report.

6 Categories of regulation

Regulations have been categorized related to digital financial services and financial inclusion across 6 categories, including: agents, consumer protection, market access, payment systems, risk management, other.

6.1 Category 1: agents

- Governing agent exclusivity (across all digital financial service providers)
  - Financial inclusion perspective: exclusivity may create barriers to access, vis-à-vis non-interoperable networks. However, allowing exclusivity, for a short period of time, may serve as an incentive to first movers.
- Authorization of agents by the financial services regulatory authority/ies
  - Financial inclusion perspective: authorization can be burdensome and may limit agent network development. However, guidelines may need to be issued for proper identification and notification of agents to the regulatory authority to help enable appropriate tracking and monitoring.
- Identifying requirements and restrictions around who can operate and serve as an agent, including security requirements
  - Financial inclusion perspective: if few limitations are placed on who can serve as an agent, it may allow greater access of services by the unbanked.

6.2 Category 2: consumer protection

- Governing the ease of switching between alternative service providers
  - Financial inclusion perspective: promoting ease of switching may allow end users, particularly the unbanked, and the power of choice. Heavy termination fees should likely be avoided.
- Outlining end user privacy of payments and transactions, including governing the use of end user data by entities (both formal and informal) other than the end user
  - Financial inclusion perspective: allowing access to end user data may allow for improved products/services, but may be used incorrectly, resulting in invasive advertising (e.g. spamming) and aggressive selling. These trade-offs should be top of mind as regulators determine the appropriate level of privacy.
- Determining information transparency, including those related to fees
  - Financial Inclusion Perspective: it is in the end user's best interest to have a strong understanding of how digital financial services may or may not impact them and their behaviour. This transparency is particularly valuable as it relates to fees applied to a transaction. Ideally, fees are communicated before the transaction is submitted.

6.3 Category 3: market access

- Specifying the types of entities that can hold a mobile money license or offer digital financial services
  - Financial inclusion perspective: an open system is beneficial to lower income end users as it likely increases access and drives prices down through increased competition.
- Cross-border money transfer
  - Financial inclusion perspective: recognizing that many unbanked end users may migrate to support themselves and their families, regulations should also aim to support open, low-value cross border payments.

- Outlining entry and exit controls of digital financial service providers and other entities participating in the scheme
  - Financial inclusion perspective: increasing entry and exit controls is likely to decrease access, which may limit competition and innovation. However, fragmented markets can be difficult to properly supervise. As a result, regulators should aim for lower entry and exit controls assuming supervision does not suffer.

6.4 Category 4: payment systems

- Identifying requirements for e-float to non-bank DFS providers
  - Financial inclusion perspective: providers should be required to keep 100% of float in liquid assets to ensure refund or redemption by the end users.
- Interest accrued on trust accounts
  - Financial inclusion perspective: the custodian bank should be required to pay interest on float. Ideally, the providers pass on interest earned on their trust accounts to end users.
- Defining or limiting payment scheme interchange (between providers)
  - Financial inclusion perspective: low or no fees are preferred for the unbanked. Interchange can create upward pressure on end user pricing. In instances where interchange from one DFS provider to *another* is required or makes sense, providing a sunset period (where interchange is at first limited than phased in) may avoid higher retail prices in the long run.
- Requiring interoperability of digital financial services providers and schemes
  - Financial inclusion perspective: fragmented markets may limit access and usability for end users. *Regulators* should aim to achieve full interoperability across all DFS providers and schemes.

6.5 Category 5: risk management

- Specifying Know Your Customer (KYC) requirements for digital financial services providers
  - Financial inclusion perspective: restrictive KYC prevents undocumented end users from opening accounts; tiered access is preferred. Additionally, connecting to a national identity scheme, if one is in place, may prove beneficial to the unbanked who may otherwise have few forms of identification. National identity scheme with biometric components have a powerful potential for avoiding payments to "ghost" recipients.
- Requiring anti-money laundering (AML) /combatting the financing of terrorism (CFT) *monitoring* of suspicious activity
  - Financial inclusion perspective: overly tight AML/CFT monitoring can either discourage usage or *make* the cost of operating a system high; leading to prices unsupportable for poor populations. Regulators should aim to achieve risk-proportionate AML/CFT monitoring.
- Requiring AML/CFT *reporting* of suspicious activity
  - Financial inclusion perspective: reporting of suspicious activity should be required even for lower-risk *accounts*.
- The appropriate identification and registration of end users by agents
  - Financial inclusion perspective: agents should be properly trained and monitored to ensure they follow all *required* customer due diligence procedures upon account opening (and as required for cash-in, cash-out, bill payment, etc.)

6.6 Category 6: other

- Telecommunication regulations setting minimum quality of service requirements
  - Financial inclusion perspective: end users must feel that digital financial services are as reliable and available as cash. High quality of service is likely to help meet that standard. A minimum standard may encourage that perception.
- Regulations relevant to labour laws around agent banking
  - Financial inclusion perspective: agents play a critical role in supplying digital financial services, particularly to those who may have previously been unbanked. However, their services may not be commercially viable if the cost to serve becomes too high. Regulators should be aware of this balance and how it may intersect with labour laws.
- Tax policies on merchant sales using digital financial services
  - Financial inclusion perspective: merchants may be dissuaded to use digital financial services if suddenly they are taxed on gains that, when using cash, went unnoticed and untaxed. Regulators should be cautious of how to implement and message tax policies to merchants who serve lower income end users. Consideration should be given to creating new tax policies that actively encourage merchant participation in the DFS ecosystem.

7 Managing the regulatory environment

Given the complexity of the DFS regulatory environment, it remains imperative that the two sector authorities involved in these efforts – financial services and telecommunications – collaborate to address these issues. Below, the Ecosystem Working Group outlines a survey of how regulators currently work together, provide a draft memorandum of understanding template for Authorities in a given country to formally outline joint goals and methods of working together, and outline considerations if regulators are interested in formalizing cross-border collaborations.

7.1 Survey of regulators

Below, the results of a recent study conducted by ITU with telecommunication regulators on collaborative efforts has been outlined. As can be seen, various approaches exist to working together, but many have recognized and actualized this need.

Figure 1 depicts the digital financial services ecosystem.

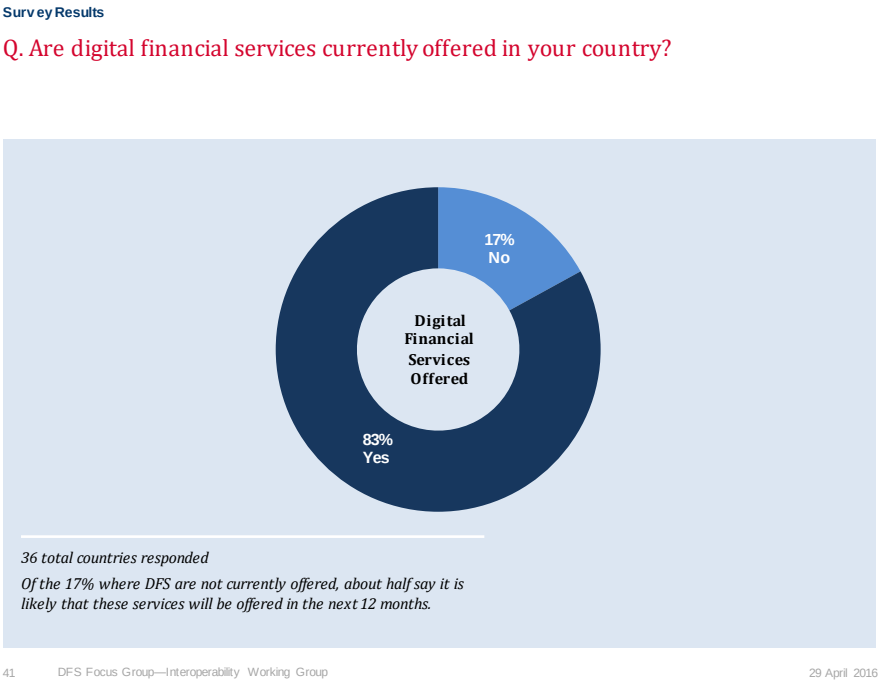

Figure 1 – Digital financial services ecosystem

Figure 2 depicts the ways in which mobile network operators provide digital financial services in different countries.

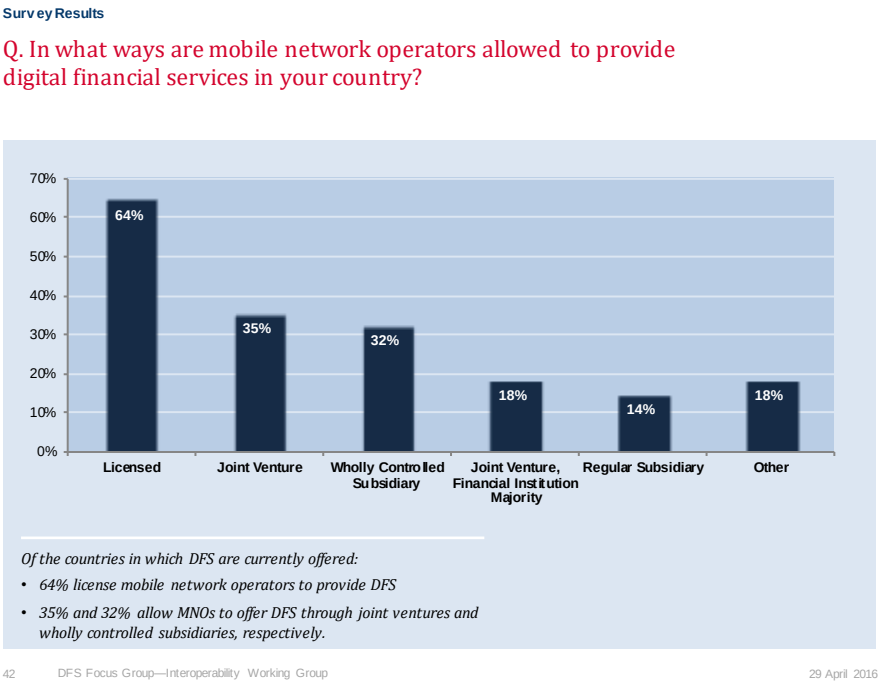

Figure 2 – Mobile network operators and DFS

Figure 3 shows the areas related specifically to digital financial services, denoting whether organizations currently mandate or expect to mandate for regulation and supervision.

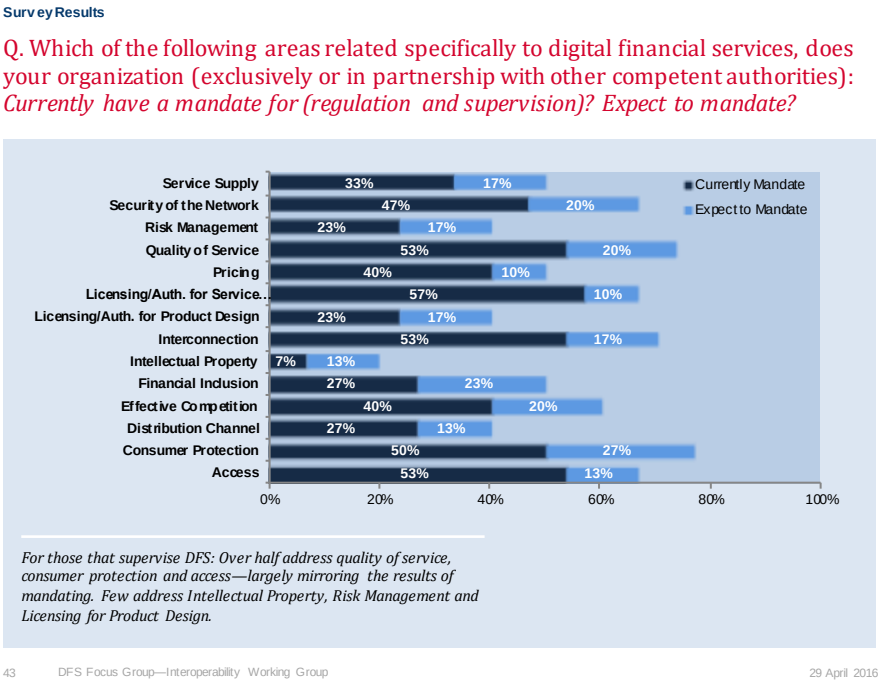

Figure 3 – Digital financial services and mandates

Figure 4 depicts the areas related to digital financial services that organizations supervise.

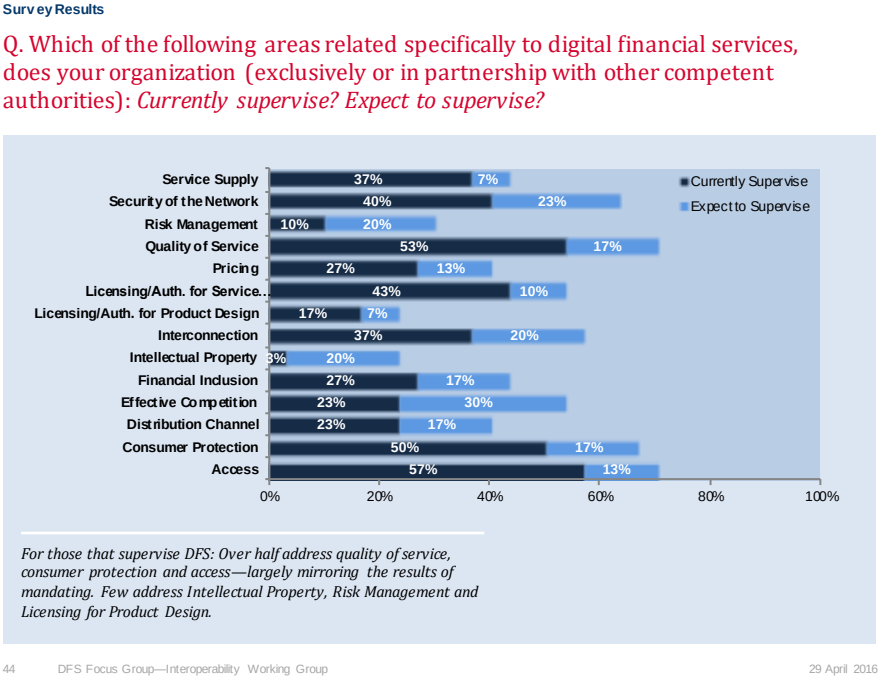

Figure 4 – Digital financial services and organization supervision

Figure 5 describes the ways in which organizations work with counterparties with financial regulators, relating to digital financial services.

Figure 5 – Organizations and financial regulators as relates to DFS

Figure 6 depicts the ways in which organizations work with counterparties with financial regulators as it relates to financial inclusion.

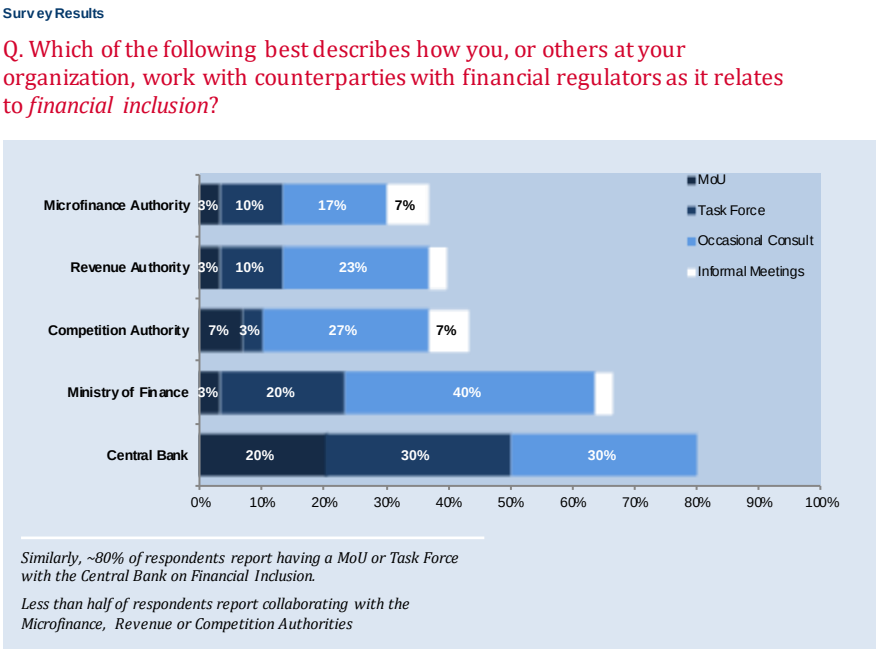

Figure 6 – Organizations, financial regulators and financial inclusion

7.2 Survey conclusions

83% of respondents (telecommunications regulators) say that digital financial services (DFS) are currently offered in their country. Of the 17% where DFS are not currently offered, about half say it is likely that these services will be offered in the next 12 months.

Of the countries in which DFS are currently offered, 64% license MNOs to provide DFS, 35% and 32% allow MNOs to offer DFS through joint ventures and wholly controlled subsidiaries, respectively.

For those that mandate DFS, over half address 'quality of service', 'interconnection', 'consumer protection' and 'access'. Few address 'intellectual property', 'risk management' and 'licensing for product design'. For those that supervise DFS, areas of supervision largely mirror the results of mandating.

Over 80% of respondents coordinate with the Central Bank in some form on DFS- over half citing a formal relationship with 20% citing an MOU, and 33% citing a Task Force. Similar results are yielded as it relates to coordinating on financial inclusion. Coordination with the Ministry of Finance also proves common, though more often through occasional consult rather than an MOU or Task Force. Given the frequency through which coordination proves valuable, the Ecosystem Working Group has outlined a template for an In-Country MOU below.

7.3 Template for an in-country Memorandum of Understanding

The purpose of this document is to provide a template, or starting point, for countries interested in drafting a memorandum of understanding (MOU) between the financial services regulatory authority(ies) and telecommunications authority(ies), as it relates to digital financial services and financial inclusion.

Additionally, it may be relevant and/or necessary to include other authorities (e.g. competition authorities, consumer protection authorities) in the agreement.

7.3.1 Parties involved

The <Authority 1> was established to <formal explanation of authority 1 role>

The <Authority 2> was established to <formal explanation of authority 2 role>

<AS NEEDED>The <Authority 3> was established to <formal explanation of authority 3 role>

<AS NEEDED>The <Authority 4> was established to <formal explanation of authority 4 role>

7.3.2 Basis

In recognition of the growing convergence of telecommunications and financial services in what has been identified as digital financial services, the Regulatory Authorities have identified a need for regulatory interaction and collaboration to ensure the integrity, security, stability and protection of participants and end users as these services are rolled out.

7.3.3 Purpose

This MOU is established in respect to the mandate of the statute regulating each entity. The purpose of this memorandum is to provide a framework for the <Authority 1> and <Authority 2> and <**AS NEEDED**: Authority 3 and 4> to collaborate with one another regarding the regulation and supervision of digital financial services in <COUNTRY>. This MOU aims to promote the integrity, efficiency (for better use of public funds/budget) and efficacy of participants by improving effective regulation and enhancing the supervision of digital financial services. This MOU is entered into on the basis of mutual respect, in a spirit of goodwill and does not affect the independence of the parties hereto.

7.3.4 Principles

This collaboration aims to abide by the following principles as allowed by law:

- Digital financial services providers and participants will experience a more coordinated effort through harmonious regulations that are clearly communicated

- End users, particularly the unbanked, will be empowered to use digital financial services, recognizing such services are secure and end users are appropriately protected

This collaboration aims to achieve the following outcomes as allowed by law:

- Implementing effective measures to combat the financing of terrorism, money laundering and fraud, including
    i. Facilitating the discovery of and actions against non-compliance or fraudulent practices
    ii. Conducting training and awareness programs on cyber security for participants and end users
    iii. Ensuring the imposition of effective sanctions
- Fostering competition and promoting a level playing field for all participants of a digital financial services ecosystem including
    i. Enabling equitable access to the telecommunications network
    ii. Preventing anti-competitive practices
- Promoting interoperability and interconnectivity of digital financial services participants
- Ensuring transactional points, including agents, adhere to relevant regulatory and supervisory requirements
- Ensuring appropriate mechanisms are in place to identify, assess, monitor and control risks related to digital financial services
- Fostering consumer protection and creating an enabling framework to ensure
    i. Services are delivered in a fair and transparent manner
    ii. Appropriate mechanisms exist to address end user complaints
    iii. Appropriate financial literacy programs exists
    iv. Participants can accurately track and provide proof of transactions
    v. End user data and identity is protected and kept confidential
    vi. End user mobility (e.g. no minimum barriers for switching products and/or services providers)

7.3.5 Promotion of a coordinated framework

The Authorities agree to work together to promote a coordinated framework for the regulation and supervision of digital financial services in <Country>. Such collaboration will include but not be limited to:

- Regulating and supervising providers to ensure digital financial services are provided in a safe, sound and sustainable manner that promotes financial inclusion.
    i. Collaborating to determine supervision, reporting, research, monitoring and record-keeping requirements
    ii. Establishing appropriate systems and clear procedures for the supervision of digital financial services
    iii. Developing standards and guidelines as deemed necessary
    iv. Implementing strategies and policies aimed at enhancing financial inclusion through digital financial services
    v. Inspecting digital financial services participants and providing technical expertise
    vi. Sharing information <SEE LATER CLAUSE>
    vii. Providing technical opinions and comments on legal and regulatory instruments
    viii. Developing and disseminating materials to participants on the regulations

7.3.6 Ongoing contact and meetings

To enable effective collaboration, each Authority may:

- Nominate at least two senior representatives from within their organization to start and serve on a Steering Committee that will hold meetings at least two times per year and when necessary. The Steering Committee will be responsible for providing strategic and policy guidance on matters covered in this MoU
- Nominate one person as the primary contact person and liaison for the purposes of information sharing related to this understanding. If this person changes over the course of the understanding, the Authority will communicate the change to the other party.
- Nominate two persons to serve on a Technical Working Group aimed at collaborating on technical matters, whose terms of reference shall be defined and approved by the Steering Committee.
- Nominate one person to serve on an External Communications Working Group, aimed at liaising with other regulatory bodies and participants, whose terms of reference shall be defined and approved by the Steering Committee.
- Nominate representatives to serve on other working groups if and when the need is identified by the Steering Committee.

7.3.7 Sharing information

Exchange of information will take place at many levels. Some information available to one regulator (including regularly provided regulatory data) may not be readily available to the other. As a result, the Authorities agree to share information to the extent permitted by law, to enable the regulation and supervision of digital financial services in <COUNTRY>. Such information includes but is not limited to

- Both Authorities will inform each other about an event which has the potential to endanger the stability of digital financial services or a relevant participant operating in the digital financial services ecosystem. This may include complaints data, supervision outputs, risk assessment outputs and enforcement data.
- Both Authorities will consider offering trainings on their expertise to the counterparty as needed to ensure proper understanding.
- The Financial Services Regulatory Authority(ies) will provide the Telecommunications Authority(ies) and <AS NEEDED: Authority 3 and 4>
    i. Information related to the licensing and/or authorization of entities able to provide digital financial services and/or participate in the digital financial services ecosystem
    ii. Information on funds safeguarding, including isolation, liquidity requirements and deposit protection
    iii. Information on emerging business models and services related to digital financial services
- Telecommunications Authority will provide the Financial Services Regulatory Authority and <AS NEEDED: Authority 3 and 4>
    i. Information pertaining to regulation or approvals to provide communication services including updates on licensed/unlicensed operations
    ii. Data on outreach and coverage of the telecommunications network(s), including network performance metrics like quality and reliability
    iii. Data on the security of the telecommunications network and information on relevant security and risk mitigation measures

iv. Information on emerging business models and services related to digital financial services

- Requests for information should be delivered with the following considerations outlined
  i. Accurate description of the information needed and the corresponding purpose
  ii. Conditions attached to the disclosure
  iii. The sensitivity and confidentiality of the information
  iv. The recipient parties of the information, including any third parties
  v. The date by which the information is needed
- Provision of or request for information will be denied if compliance would result in an unlawful act or interfere with an ongoing investigation

7.3.8 Confidentiality

- Information shared or discussed will be used only for lawful purposes
- Information will not be shared or disclosed beyond the recipient parties identified unless first agreed upon by both Authorities
- Information provided will remain the property of the Authority that provided such information
- All documents related to this MOU will include the following in the footer: 'Confidential-provided pursuant to the MOU between the <Authority 1> and <Authority 2> and <AS NEEDED: Authority 3 and 4> on the regulation and supervision of digital financial services.

7.3.9 Commencement, duration and termination

- This understanding comes into effect on the date signed by the represented Authorities.
- This understanding shall remain in effect until one Authority notifies the other in writing of its wish to revise, amend or terminate from the understanding. <X> days notice of any action will be required. Revisions and amendments must be agreed upon by both Authorities
- An Authority may terminate its participation in this understanding by providing written notice to the other Authority, assuming the termination will not affect the obligations and rights of either Authority with respect to confidential information shared over the course the MOU was active
- This MOU will not affect the rights and obligations of the Authorities under applicable laws and regulations

7.3.10 Other considerations for establishing an MOU

When drafting an MOU, the Authorities may want to consider additional sections beyond what was outlined above. Those may include

- Dispute resolution: how to manage dispute between the two Authorities
- Manage inconsistencies: what to do if there are inconsistencies between the MOU and other laws or regulations
- Distribution of costs: how to divide costs related to actualizing this MOU including information sharing
- Governing law and legislation: how to ensure the recognition and intersections of law and legislation including banking secrecy, protection of personal information and confidentiality of communication
- Communications to the public: how to manage external communications to parties outside of this understanding

- Intersections with other authorities: how to properly engage and interact with the competition authorities and consumer protection authorities

7.4 Cross country considerations for a memorandum of understanding

As national digital payment systems develop and cross-border low-value digital payments scale, regulators may consider drafting an agreement (in the form of a memorandum of understanding) to foster this potential and promote collaboration. If and when this occurs, the following sections should be included:

- **Introduction:** the introduction outlines the background to the current situation, describes the need and rationale for an MOU, outlines the players or authorities that are involved, and the implications of such an agreement.
- **Purpose**: the purpose is intended to be a concise statement that describes the intention of the MOU, how those involved will use the new capability, including the circumstances.
- **Scope**: the scope section of the MOU should include when the policies described in the agreement do and do not apply and whom the policies do and do not implicate.
- **Policy**: this section explains the policies that the players involved have agreed upon. Definitions tend to be beneficial to ensure clarity.
- **Structure**: the structure of the agreement outlines how players intend to work together, including who will be the key points of contact, how often to meet, what the workflow looks like and how to communicate with one another.
- **Obligations**: as its name implies, this section includes obligations of those included in the agreement. For example, the training that needs to be completed, the party that is financially responsible for different aspects of the agreement, how maintenance and oversight will occur, and how to update the MOU.

Bibliography

[1] Bank of Uganda: Mobile Money Guideline, 2013

[2] Central Bank of Liberia: Mobile Money Regulations, 2014

[3] CGAP, GPFI: Global Standard-Setting Bodies and Financial Inclusion for the Poor

[4] CGAP: Update on Regulation of Branchless Banking in Brazil, 2010

[5] Homeland Security: Writing Guidelines for a Memorandum of Understanding

[6] NIST, U.S. Department of Commerce: Writing Guidelines to Develop a Memorandum of Understanding for Interoperable Automated Fingerprint Identification Systems, 2013

[7] European Securities and Market Authority: Memorandum of Understanding, 2014

[8] Federal Reserve: Protocol for the Cooperative Oversight Arrangement of CLS, 2015

[9] Central Banks of Sweden and Finland: Memorandum of Understanding on Cooperation in the Oversight of the Central Securities Depositories VPC AB and Suomen Arvopaperikeskus Oy, 2006

[10] Central Bank of the Russian Federation and The Commission of the Republic of Latvia: Memorandum of Understanding in the Field of Banking Supervision

[11] Central Bank of Jordan and the Qatar Financial Regulatory Authority: Memorandum of Understanding in the Field of Banking Supervision, 2005

[12] Bank of England: Memoranda of Understanding between the PRA and the Central Bank of Brazil, 2015

[13] Oliver Wyman: The Digital Disruption Battlefield

[14] GSMA: Mobile Money- Enabling regulatory solutions, 2013

[15] GSMA: Proportional risk-based AML/CFT regimes for mobile money- a framework for assessing risk factors and mitigation measures, 2015

[16] Coase-Sandor Institute for Law and Economics Working Paper: An Empirical Examination of Why Mobile Money Schemes Ignite in Some Developing Countries but Flounder in Most, 2015

[17] Center for Global Development: Enabling Digital Financial Inclusion through Improvements in Competition and Interoperability: What Works and What Doesn't?, 2015