ITU FOCUS GROUP DIGITAL FINANCIAL SERVICES: MAIN RECOMMENDATIONS

ITU-T FOCUS GROUP ON DIGITAL FINANCIAL SERVICES

International Telecommunication Union

ITU-T FG-DFS

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(03/2017)

ITU-T Focus Group Digital Financial Services

Main recommendations

Focus Group Technical Report

International Telecommunication Union

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The procedures for establishment of focus groups are defined in Recommendation ITU-T A.7. TSAG set up the ITU-T Focus Group Digital Financial Services (FG DFS) at its meeting in June 2014. TSAG is the parent group of FG DFS.

Deliverables of focus groups can take the form of technical reports, specifications, etc., and aim to provide material for consideration by the parent group in its standardization activities. Deliverables of focus groups are not ITU-T Recommendations.

Main recommendations

About this Report

This report outlines the recommendations of the Focus Group and identifies key areas where intervention by regulators, DFS operators and policymakers are needed to create a conducive environment for digital financial services.

The recommendations are grouped under the following main headings of each working group:

- Ecosystem
- Interoperability
- Technology, Innovation and Competition (TIC)
- Consumer Experience and Protection (CEP)

If you would like to provide any additional information, please contact Vijay Mauree at tsbfgdfs@itu.int

Table of Contents

1. Introduction

The ITU Focus Group Digital Financial Services has prepared a set of recommendations for consideration by in-country regulators, policy makers, and other stakeholders in the ecosystem. These recommendations will support a DFS ecosystem that enables financial inclusion through the delivery of affordable, accessible, secure, transparent, and robust DFS to end users.

The Focus Group members recognize that financial inclusion contributes to the development goals of poverty reduction, economic growth and jobs, greater food security and agricultural production, and women's economic empowerment and health protection.

The recommendations assume a willingness by in-country regulatory bodies and authorities, including financial service authorities, central banks, telecommunications authorities, competition authorities, consumer protection authorities and joint bodies to collaborate to enable a DFS ecosystem to support financial inclusion. It is also noted that the ecosystem, and the ways in which different regulators are involved with the ecosystem, are evolving. The incremental costs and other burdens of regulation are noted: The allocation of these costs to various stakeholders needs to be determined.

The Focus Group recommendations have been informed by the G20 High Level Principles for Digital Financial Inclusion, the Guiding Principles stated in the CPMI/World Bank PAFI report, and the FATF Principles.

The work of the Focus Group included mapping out key roles in the DFS ecosystem. These definitions and the related DFS glossary are provided in the published Focus Group report, "The Digital Financial Services Ecosystem". It is recommended that the Glossary be a "live" document within the ITU, with ongoing additions and amendments.

2. DFS Ecosystem recommendations

Title of recommendation	Regulations promoting an open ecosystem of DFS providers
Working Group	Ecosystem
Audience for recommendation	DFS regulators

Policy makers and regulators should support the growth of an open ecosystem for DFS that promotes innovation and ensures robust competition.

- Regulators should enable multiple regulated financial services providers (banks and non-banks alike) to compete or partner to offer a range of responsible, secure financial services. Openness of access by many providers will encourage competition, promote innovation, and reduce prices. Regulators must keep in mind the need to ensure the safety and soundness of the ecosystem.
- Policy makers and regulators are encouraged to take a proactive approach to establishing clear goals and regulations related to the DFS marketplace, and to recognize the limitations in market actions, given the need for players to cooperate with each other in order to achieve the goals of financial inclusion. Policy makers are further encouraged to use a broad range of tools, including formal and informal convenings, and work with industry bodies and financial inclusion policy groups to achieve their goals. In the likely event that multiple regulatory authorities in a country are involved in some way in the regulation of DFS, regulators are encouraged to collaborate by establishing memoranda of understanding (MOU) between and among these groups or through a National Payments Council or like body, to ensure clarity on responsibilities. This approach and a template for an MOU are included in the Focus Group published report, "Regulation in the Digital Financial Services Ecosystem".
- Regulators should cooperate to ensure a service-based approach to DFS regulation, so that bank and non-bank regulated DFS providers are subject to similar regulations and therefore similar rights and obligations as other DFS providers, while recognizing the challenges of managing different channels.
- Regulators should take actions to ensure adequate market oversight of DFS providers. Regulators should require companies under their regulatory jurisdiction to report on activities, transaction volumes, fraud, and other regulated activities, and should use analyses of this data to guide future actions. Active monitoring of regulatory compliance is specifically encouraged to enable a broader and more open DFS ecosystem. The use of electronic reporting mechanisms is strongly encouraged.
- Policy makers and regulators should consider actions to make it easier for consumers to switch DFS providers without incurring undue costs or difficulties.
- Policy makers and regulators should encourage DFS providers and DFS provider support services (including processors, aggregators, payments switches, etc.) to make use of standards-based APIs to encourage the development of the open ecosystem.
- Regulators are encouraged to require that DFS providers, particularly those not from a traditional financial services sector, to manage risks with a dedicated focus on that task, and to hire skilled and experienced employees to manage risk.

Title of recommendation	Consumer pricing and fees
Working Group	Ecosystem
Audience for recommendation	DFS regulators

Relevant regulatory bodies should maintain accurate and timely information about the direct and indirect prices consumers must pay to access DFS to ensure that market prices do not create significant barriers to use.

- Regulators are encouraged to use a variety of techniques, including mandating transparency in charging of fees and "moral suasion" to ensure the consumer prices are reasonable. The use of mandates over the amount of fees is not recommended, although it may be advisable in some exceptional situations. It is important when considering the question of consumer fees to make note of the use case involved. Consumer fees may be warranted, for example, for person-to-person remittances, particularly when electronic remittances are substantially safer or less expensive than manual cash transfers. In other use cases, such as bill payment or merchant payments, having any consumer fee at all may represent an insurmountable barrier to use, with consumers continuing to use cash for such payments rather than incurring a fee.
- Regulators should take steps to ensure that pricing information is publically available in a meaningful way, and that consumers are aware of where this information is.
- Policy makers should consider measures to ensure that economic barriers do not make large value (including government and employer) "bulk" payments impractical, that DFS providers supporting the receipt of consumer payments are appropriately compensated, and that charges to consumers for government to person (G2P) payments (including cash-out fees) are not excessive.
- If payments system interchange reimbursement fees are employed, financial regulators should monitor these fees and revisit any cost and market assumptions every 2-3 years to determine if the fees are still necessary, and if so, at what level. If put in place, interchange fees should be specific to a use case, and be used to compensate one DFS provider for unavoidable costs associated with providing services to the customer of another DFS provider. For example, if a DFS provider is enabling its consumer to make bill payments, and these bill payments require ongoing customer service and problem resolution procedures on the part of that provider, it may be reasonable to use interchange as a mechanism to transfer value from the biller's DFS provider to the consumer's DFS provider. The assumption here is that the biller's DFS provider would pass these interchange costs on to the biller, who is receiving the benefit of the electronic transactions. Another example relates to the use of agent services for cash-out by a consumer, where the consumer is using an agent who is not a representative of their DFS provider. Interchange compensation within an interoperable scheme from the consumer's DFS provider to the agent's DFS provider is reasonable (assuming the consumer is not charged by the agent directly) and in keeping with long-standing practices in ATM network interoperability.
- Financial regulators and competition authorities should resist the use of interchange to compensate for revenue reductions experienced by one "side" of the transaction: doing so can lock-in outdated compensation structures; subsidize inefficient processes and cost structures; and retard incentives to innovate. Altogether, this can create a barrier to true low cost payments.

Title of recommendation	Fostering acceptance of electronic payments
Working Group	Ecosystem
Audience for recommendation	DFS stakeholders

Policy makers should promote initiatives and incentives that encourage merchants and other payment acceptors (e.g. billers, farmers, government entities) to accept electronic payments.

- Stakeholders agree on the benefits of reducing cash in the ecosystem. To achieve this, it is critical to give consumers avenues to spend money received electronically. Merchant acceptance of electronic payments from consumers and other businesses can increase the velocity of money in the ecosystem, therefore reducing the costs and risks associated with "cash-in, cash out".
- The DFS Focus Group has published a series of reports on electronic payments acceptance. "Enabling Merchant Acceptance in the DFS Ecosystem" describes the value chain and segmentation; four other reports look at particular aspects of acceptance: B2B Payments and the DFS Ecosystem (if a merchant can buy their inventory electronically, they will be more willing to accept consumer payments); Merchant Data and Lending (merchant transaction history can lead to credit extension); The Impact of Social Networks on Digital Liquidity (social networks may enable small merchant eCommerce); and The Impact of Agricultural Platforms on Digital Liquidity (agricultural platforms should integrate with consumer wallets).
- While recognizing the importance of the topic, policy makers should be aware that there is no single "killer app or factor" to enable electronic acceptance. A combination of the factors below should be used to create incentives for small merchants.
- DFS providers and other stakeholders should cooperate to ensure that merchants are educated about the benefits of accepting electronic payments: customer convenience and preferences, safety/reduced theft of funds, easier and/or cheaper access to credit, new revenue streams, enriched data/information about customers, customer relationship management, etc. Policy makers should recognize that merchants of different sizes and in different segments have varying needs.
- Policy makers should consider tax incentive policies to encourage merchants and other payments acceptors to take electronic payments. Measures should be considered to ensure that small merchants which are today accepting only cash are not subject to immediate taxation upon moving to electronic payments. Charging tax on mobile money is quite common where there are difficulties in collecting tax revenue. Tax authorities need to research the possible impacts of taxation first and then decide on the taxation on a case by case basis.
- DFS providers extending payment acceptance services to very small merchants may not be profitable from transaction fees alone, and are therefore likely to extend their offering to include a variety of services. The most critical of these is the provision of credit to merchants (and in some situations to their customers). Regulators should be open to allowing DFS providers to extend this credit, with appropriate safeguards on lending.
- Commercial value chains should leverage general purpose payment instruments/transaction accounts (rather than proprietary/single-purpose solutions such as e-vouchers) as much as possible in order to improve efficiency and better targeting of subsidies within the DFS.
- As rapidly emerging person to person (P2P) payment and merchant commerce platforms, social networks can bring significant value to the small merchants and their customers. Policy makers should consider policies that encourage adoption and use of social networks for commercial transactions. That said, social networks are tremendously powerful and regulators should monitor and manage them judiciously with

adequate safeguards, as well as implement policies that protect consumers from potentially harmful effects (e.g., data privacy, pricing discrimination, identity theft, etc.)

- Policy makers should take steps to encourage electronic B2B payments (merchants paying suppliers electronically, for example). This could help the DFS ecosystem as a whole achieve digital liquidity and improve the ability of governments to collect taxes. For example, this could make it easier for informal businesses to make digital business to business (B2B) payments by taking a risk-based/tiered approach to regulating those payments, supporting interoperable B2B payment systems, and encouraging/mandating e-invoicing in certain situations as it is implemented in Chile, Brazil, Mexico, and Argentina, for example.
- Encourage the development of alternative credit decisioning (ACD) that includes merchants' payments history, in a system open to a wide range of participants – banks, mobile network operators (MNOs), alternative lenders, etc. Importantly, policy makers should address a range of issues surrounding consumer and merchant consent, collection, usage, securing, ownership, and sharing of ACD data.

Title of recommendation	National identity, eKYC and payments addressing
Working Group	Ecosystem
Audience for recommendation	DFS regulators

Policy makers and regulators are encouraged to use national identity systems, or other market-wide identity systems, to help with opening transaction accounts, addressing payments, and, in some instances, improving transaction security.

- The DFS Focus Group commissioned a study called "Review of National Identity Systems", to: Determine the extent of pervasive national identity systems; understand the extent of the use of biometrics with those systems; and look at the use of these systems in enabling digital financial ecosystems. In general, the study found higher-than-expected pervasively distributed identity systems, and a surprisingly large number of countries using biometric systems. The use of these systems with financial services, however, is still quite limited.
- Countries with a national identity system, or another similar market-wide identity system, should recognize this as a public resource. Access to this directory, and use of it, should be open to all regulated DFS providers at a reasonable cost. Countries without a national identity system are encouraged to develop one.
- DFS Providers and regulators should cooperate to ensure that a uniform addressing directory for payments is established, enabling the addressing of payments using national ID's, mobile phone numbers, or other non-provider specific aliases. Such a directory should enable persistent consumer and enterprise identification numbers that may be made public without compromising the security of transaction accounts.
- Policy makers, including financial regulators, should examine ways to use national identity systems to reduce know your customer (KYC)-related barriers to opening a transaction account, such as by linking account opening to a national identity number system, and/or leveraging SIM registration processing. If possible, the use of biometric data tied to a national ID is strongly encouraged because of the potential of reducing fraud.
- Where national identity systems are not pervasively used, policy makers should consider, where possible, having a "zero KYC tier" for consumers, enabling low value transaction accounts to be opened without identity documents.
- DFS providers are encouraged to create mechanisms for consumers to dispute transactions with fraudulent merchants, and in some specific instances support revocation of funds.

Title of recommendation	Government support of the DFS ecosystem
Working Group	Ecosystem
Audience for recommendation	Governments and other DFS stakeholders

Government support of the DFS ecosystem is necessary for it to flourish. Government agencies are encouraged to support the ecosystem in multiple ways.

- Stakeholders in the DFS ecosystem are encouraged to work with government units to facilitate the digitization of government services - in particular, payment flows between the government and consumers or enterprises (e.g., salaries, social transfers, fees). This includes both government to person (G2P) and person to government (P2G) transactions.
- The specific matter of G2P payments (sometimes generically referred to as "bulk" payments – including payments of salary and non-governmental benefits) has been extensively studied over recent years. The DFS Focus Group concentrated on one particular issue within G2P payments: the question of how payments are addressed, or routed from the paying agency to the consumer's DFS account. The DFS Focus Group published a report, "Bulk Payments and the DFS Ecosystem" that investigated the issue and isolated some best practices. The use of a national identity number to address a payment is beneficial in that it does not require the paying agency to collect, store, and maintain beneficiary account information - doing so is both time and labor intensive and subject to frauds of various types. An interoperable payment scheme, with a directory at its core that maps national identities to consumer transaction account(s), is an elegant and efficient solution to these problems, and regulators are encouraged to promote this. Furthermore, if the national identity scheme has a biometric component, and this biometric is associated with the transaction account, it is possible to substantially reduce fraud from "ghost accounts". Policy makers are urged to look at India as an example. Transaction accounts are associated with a biometric that is accessible by the interoperable payments scheme. Payments into accounts may be made using the identity number. Consumers wishing to withdraw funds from their transaction accounts can do so at any agent whose account is connected to the payments scheme; the consumer identifies themselves to the agent with a biometrically enabled "micro ATM" at the agent's location.
- Governments should play an active role in working with DFS providers to educate consumers and promote the visibility of DFS services.

Title of recommendation	Shared services
Working Group	Ecosystem
Audience for recommendation	Competition authorities

Regulators, including competition authorities, should recognize that the DFS ecosystem will benefit from some services being shared among providers and should encourage this sharing. Shared services, such as fraud management services, can be an important way to achieve success, particularly for those which benefit all participants, require economies of scale, and which are not thought to be sources of competitive differentiation.

- Although policy makers are encouraged in general to promote vigorous competition in the DFS ecosystem, there are areas where cooperation and collaboration make more sense for the development of low-cost financial services. The most obvious area of collaboration is in the development of shared, interoperable payments schemes – that is addressed at length in other papers and recommendations of the DFS Focus Group.
- There are other areas where policy makers and regulators should allow, and even promote, a collaborative approach. Payments fraud management relies on the use of data and algorithms to detect anomalies that might be fraudulent, and to detect "bad actors" who are using the ecosystem through a variety of DFS providers. Allowing or even mandating DFS providers to share data (while protecting the confidentiality of this data, at both the consumer and the DFS provider level) is strongly recommended. Having a larger pool of data simply makes fraud detection easier and better - no single DFS provider can have the data that all DFS providers together have. Furthermore, a shared investment in fraud algorithms, and even the use of those algorithms to stop fraud, can be equally beneficial.
- There are multiple examples of the use of collaboration in fraud management in the U.S. payments card market. Visa and MasterCard cooperatively manage an Issuer's Clearinghouse which require issuers to report: All credit card applications; all fraudulent applications; and all accounts that have experienced unauthorized usage. From this data the card networks provide reports and tools to allow issuers to manage account application fraud. Multiple other services, including early warning services, ID analytics, and Experian's National Fraud Database, support similar payments related fraud management capabilities using shared data. Although many of these services are now commercial, in the early days of the development of the systems they were managed by bank-owned entities and operated on a cost recovery basis.

Title of recommendation	Over the counter (OTC) services
Working Group	Ecosystem
Audience for recommendation	DFS stakeholders

"OTC" transactions may be useful in some markets for effecting a transition from purely cash to digital payments between transaction accounts.

- Several markets are characterised by extensive use of OTC transactions. The ITU Focus Group on Digital Financial Services has published a report titled "Over The Counter Transactions: A Threat To Or Facilitator For Digital Financial Ecosystems?" that describes the various forms of OTC in place and analyses some of the challenges arising from them.
- Regulators are understandably concerned about problems associated with payment transactions conducted between unidentified individuals. In some countries, programs are being put into place to ensure that identity information (sometimes biometrically established) are collected for both parties in the transaction. Regulators should require that risk-proportional identification of both the sending and the receiving parties are recorded.
- However, regulators are encouraged to consider the broader question of whether or not transactions are paid out of – and into – transaction accounts. From the standpoint of financial inclusion, it is beneficial for consumers to open and use transaction accounts, which can, over time, provide the base – and the data – necessary for access to other financial services, including credit, savings, etc. Stakeholders in markets with extensive use of OTC transactions should cooperate in order to create a path towards fully electronic account-based payments, and thus, ultimately, to a range of DFS. Regulators should work with DFS providers to implement education programs to promote the transition to a digital system, and consider provisions to incent providers and consumers to use transaction accounts.
- Regulators should also consider the question of agent assistance as a separate question from the use of non-account based payments transfers. Agent assistance can be of value in helping consumers understand and become familiar with electronic payments. Agents often provide assistance with account-based transfers, and this should not necessarily be discouraged by regulators.
- The economics of OTC transactions are problematic in several countries where the fee and commission structure among DFS providers, agents, and consumers may together encourage the ongoing use of OTC transactions. Regulators are encouraged to study this issue closely, and consider actions to reduce this problem.
- Some countries have considered the question of banning OTC transactions altogether. Given that OTC can create a transition path for the consumer to the full use of digital payments, it is recommended that OTC be allowed to continue in markets where it currently exists – subject to efforts to create a path to broader financial inclusion highlighted above.

Title of recommendation	Postal Networks
Working Group	Ecosystem
Audience for recommendation	DFS regulators

Policy makers and other stakeholders are encouraged to leverage existing infrastructures and capabilities within their countries, in an effort to avoid duplication of costs. In particular, policy makers are encouraged to consider ways to use postal networks to support the DFS ecosystem.

Postal networks represent a considerable asset in emerging economies, and regulators and policy makers should consider ways in which these assets can be deployed in support of the full DFS ecosystem in a country. The ITU Focus Group on Digital Financial Services has published a report titled "The Role of Postal Networks in Digital Financial Services" which describes these assets and the various ways in which postal networks are today providing or supporting financial services.

Consideration should be given to the postal network's positioning as a public good, especially in light of the challenging business models for commercial providers of DFS in some markets. This applies both to the provision of transaction accounts, and to supporting cash-in, cash-out services.

Where postal networks are providing either transaction accounts (savings or current accounts), or remittances or other payments services, these services should either be regulated by financial services regulators or, where this is not possible, every effort should be made to ensure that regulations concerning these accounts and services be closely aligned with those applied to banks and other licensed providers of such services in the country. Inter-regulator MOU's are encouraged to ensure clarity of responsibility and to provide a mechanism to ensure regular meetings among regulators aimed at achieving alignment of regulation.

Transaction accounts in postal networks should be interoperable with other payments networks in the country. Preferably, the postal network should be a direct participant in the payment network, rather than accessing it through a bank. Consumers holding a postal network transaction account should be able to transfer money to other postal network accounts, but also to bank accounts and to eMoney transaction accounts offered by other licensed DFS providers in the country. Consumers, businesses, and government entities holding bank accounts or eMoney transaction accounts should be able to transfer money into a postal network transaction account.

As noted in the report, postal networks are upgrading their electronic access capabilities. As they come fully online, they may be able to play a useful role in eCommerce and mobile commerce in the country, by managing the physical pick-up or delivery of goods and/or providing escrow services to manage risks with such transactions. Regulators should support and encourage this.

3. Interoperability recommendations

Title of recommendation	Interoperability mission
Working Group	Interoperability
Audience for recommendation	Authorities, DFS Providers

Interoperability should enable users to make electronic payment transactions with any other user in a convenient, affordable, fast, seamless and secure way, even with a single transaction account.

At the core of this vision lies the "transaction account". A transaction account can be a deposit (current account, checking account, card account, savings account) or an e-money account (prepaid account, online money, mobile money), issued by a bank or a non-bank. These types of accounts share the characteristics of allowing user to make and receive payment transactions. The need to hold different accounts (including for closed-loop systems like transit cards) especially affects poor users, since for them it is more difficult to afford idle balances in those accounts. Therefore, if a user wishes to hold only one transaction account, he/she should be able to initiate and receive his/her payments via this single transaction account.

Payment transactions are made in order to settle an obligation or send money to someone else, without underlying economic transaction. Payments are often considered a friction to that end objective. Users must be able to access transaction accounts and initiate payment transactions in an overarching or ubiquitous manner, independent of their location, this implies 24/7 availability. In that sense payments should be convenient, with minimum effort for end users as possible.

Payments between customers of two different DFS providers should not be perceived users as being different from payments between two customers of the same service provider. This seamless experience should include commercial conditions that should not be different between transactions within the same provider (on-net or on-us) and comparable payment transactions across different providers (off-net or off-us). Payment transactions, including those between customers of different payment providers, must be affordable, as a way to foster usage, value deposits and drive financial inclusion.

Payment transaction should be fast, meaning that the final receiver of the transaction should have the certainty of availability of funds instantly. Certainty of availability of funds on an instant basis is fundamental to meet the aim of substituting cash transactions.

Another required feature is safety. Payment services are only viable if they are perceived as safe by final users. As a store of value, transaction accounts must be perceived at least as safe as holding, carrying and handling cash. If users see a transaction account and the associated payment instruments as being susceptible to fraudulent access and use they will not adopt it.

Making payments with any other user refers to the possibility to make payment transactions between users in-person or remotely, i.e. if they are geographically separated within or across borders. Often innovative solutions that offer global reach do so within closed or limited interoperable schemes only or still rely on complex correspondent banking relationships.

Title of recommendation	Interoperability strategy and policy
Working Group	Interoperability
Audience for recommendation	Authorities, DFS Providers

Interoperability, reflected in strategies and policies of relevant authorities and market participants, should meet the needs of participating DFS providers and the markets they serve by also aiming at increased efficiency, effectiveness and affordability.

Interoperability should be consistent with the objective to improve payment system efficiency and effectiveness. Interoperability is effective if it supports the reliable and timely exchange of payments and supports the public policy goals of safety and efficiency. In the context of payment system oversight, interoperability effectiveness requires meeting service and security requirements. To facilitate the assessment of effectiveness, interoperability arrangements should have clearly defined goals and objectives.

Choices of financial regulators and other authorities, very often in consultation with the industry, are increasingly reflected and communicated in strategy documents. But not only authorities should be transparent on their interoperability strategy, also service providers involved in an interoperability arrangement should formulate a clear strategy, which should be disclosed to relevant authorities, users and, at a more general level, to other service providers.

The establishment of interoperability should support the relevant public policies. Among these public policies can be to aim to facilitate the exchange of payments domestically and/or internationally, improving the reachability of the providers and their customers, and increasing affordability. Rules and solutions to establish interoperability should take into account market practices and technology and/or accommodate internationally accepted communication procedures and standards adhered to by participating service providers.

In order to ensure efficiency for its users, interoperability should be designed having in mind the users' current and future needs. Interoperable systems should provide users with practical services. In order to do so, the size of the users' activity (number of payments), the efficiency of the channels currently used for clearing payments, and the jurisdictions within which they exchange payments need to be considered. The decision on whether to establish interoperability should be based on a cost-benefit analysis.

The efficiency and effectiveness of interoperability should be measurable. Mechanisms for the regular review of interoperability efficiency and effectiveness, such as periodic measurement of its progress against its goals and objectives, should be established.

Title of recommendation	Role of authorities in interoperability
Working Group	Interoperability
Audience for recommendation	Authorities

Authorities should publicly disclose interoperability strategies and policies. The lead role in DFS interoperability should be played by the financial regulator. In doing so, the financial regulator should cooperate with other authorities as needed.

Policies that promote/favor interoperability should be clearly stated in order to provide guidance to the industry and other market participants. Having stated clearly their policies concerning interoperability, authorities should engage market participants, in order to catalyze market participants' discussions and turn policies into reality. Engagement should be in the development of the policies and on an ongoing basis as soon as policies are published. This should allow market participants to internalize the policies into their goals and develop the best way to realize these policies by implementing interoperability.

DFS interoperability will require strong cooperation between relevant authorities. As DFS interoperability involves several related dimensions (including legal, financial, operational, technical, procedural, and business aspects), different institutions bearing oversight, supervisory, and regulatory responsibilities – not just in the financial area – may need to be involved (on a regular or an ad hoc basis) to make sure that interoperability is established and sustained in a way that is consistent with overall payment system efficiency and safety. Authorities should cooperate with each other, both domestically and internationally, as needed, with a view to fostering efficient and effective communication and consultation in order to support each other in fulfilling their respective mandates. Cooperation needs to be effective in normal circumstances and should be adequately flexible to facilitate communication, consultation, or coordination, as appropriate, especially during crisis situations.

The role of different authorities when it comes to interoperability should ideally be clarified and agreed upon, e.g. in form of a memorandum of understanding. Central banks are heavily involved in the operation, regulation and oversight, and reforming of payment systems as operators, overseers and regulators and facilitators/catalysts. Telecom regulators may play a role as regulators for certain specific components and/or participants of the national payments system, though they will not normally have primary responsibility for payments or the payment systems as such.

Title of recommendation	Role of authorities in interoperability
Working Group	Interoperability
Audience for recommendation	Authorities

Authorities, acting in their catalyst role, should engage market participants and other stakeholders in order to promote discussions and guidance over the path towards interoperability. Scope, extent and timing of regulatory interventions, if any, need to be carefully considered and take into consideration the views of market participants and key stakeholders.

Authorities should provide an enabling environment that balances the legitimate interest of the providers in capitalizing their investments as first movers against the overall public policy objectives. It is imperative that regulatory interventions are carefully considered so as to support the overall policy objective and avoid market distortion. Mandating interoperability at an early stage may reduce the incentives for firms to enter a new market and compete. On the other hand offering a proprietary solution can help innovative service providers to exploit their first-mover advantage, but might create path dependence and lock users into their service. Therefore, the absence of moral suasion or regulatory intervention may lead to inefficiencies and may leave some communities unserved.

Market participants and key stakeholders must be heard before regulation is imposed, to avoid that regulation has the unintended side effect of adversely affecting market development. Regulation should be limited in those aspects the market cannot agree on and/or realize, since authorities as neutral entities can mediate between various, often competing interests of different market participants.

Where the regulators and market is unable to establish interoperability from the beginning at minimum the focus should be on ensuring that interoperability is technologically feasible. At the same time regulators should ensure that they have both the necessary information and regulatory power to intervene when there is evidence that a dominant position is being exploited. To make such interoperability feasible, there need to be effective oversight arrangements that look at system-wide, cross-system, and infrastructure-level interoperability. Requiring infrastructure-level and system-wide interoperability and disallowing exclusivity arrangements can set the stage for cross-system interoperability in the future.

Title of recommendation	Interoperability stakeholder coordination
Working Group	Interoperability
Audience for recommendation	Authorities, DFS providers.

The roles of public authorities and private sector stakeholders in achieving interoperability should be clearly defined and agreed upon. The involvement of all relevant stakeholders, be they incumbent providers or new, authorized/regulated entrants, should be ensured throughout the process. The implementation of interoperability should leverage to the extent possible existing coordination structures. If coordination structures are not yet in place or existing ones are not suitable, alternative coordination structures should be established.

Interoperability, like other major payments reforms, requires the active and often continuous involvement of a broad range of stakeholders from the public sector and the private sector. A collaborative approach to payment system modernization is essential. On one hand, relevant changes in any area of the payments industry will most likely have an impact on all of its participants. Moreover, as a network industry, some of the challenges to improve efficiency, safety or security can only be overcome by the industry as a whole. Another crucial reason for cooperation is that no single individual or entity possesses all the knowledge needed to address payment system reforms. Different mechanisms can be used for these purposes.

In many countries, central banks have established and usually chair a payments council and/or a financial inclusion council that serves as a forum for multi-stakeholder consultations. A National Payments Council (NPC) or National Payments Committee is one of the most commonly used coordination mechanism for payment reforms, especially in countries that have engaged in larger or more significant reforms. It consists of a rather structured and, in many cases, formal mechanism with leadership from the central bank.

If interoperability is a market wide-approach, as opposed to the establishment of interoperability between selected market participants, existing coordination structures can be used for that purpose. In the absence of these structures and/or if not all market participants are (yet) interested in interoperability, a task force among the market participants can be formed, involving authorities as observers.

Title of recommendation	Legal aspects of interoperability
Working Group	Interoperability
Audience for recommendation	DFS providers

Interoperability arrangements should be compliant with the legal and regulatory frameworks within all the functional and/or geographic jurisdictions they are implemented in. Interoperability rules should be enforceable within as well as across all these relevant jurisdictions. Conflicts of laws should be identified upfront and mitigated in the interoperability arrangements.

The legal framework (laws, regulations, rules and procedures) applicable to interoperability should provide a high degree of certainty for every aspect relating to interoperability. The rules, procedures and contracts governing interoperability should be clear, understandable and consistent with relevant laws and regulations. They should be readily available as appropriate for all parties with a legitimate interest.

The rules, procedures and contracts governing interoperability should be complete, valid and enforceable in all relevant jurisdictions. There should be a high degree of certainty that actions taken under such rules and procedures will not be stayed, voided or reversed.

Interoperability should be consistent with the applicable regulatory frameworks. In cross-border interoperable systems, risks arising from any potential conflicts of laws across jurisdictions should be identified and mitigated.

An unclear and/or inconsistent regulatory framework may result in payments processed via interoperability arrangements being subject to higher legal risks, compared with those processed in a single and/or proprietary system. In particular, conflicts may arise if it is not clear which are the specific laws, regulations, rules or procedures applicable to payments processed via interoperable arrangements. In exceptional circumstances (e.g., the default of a participant), uncertainties or conflicts could arise if the rules governing interoperability do not clearly specify the procedures to be followed.

Conflicts may also arise when the legal basis, and in particular the contracts, do not clearly define the rights and obligations of the entities participating in interoperability arrangements. Conflicts could stem from differences in laws and regulations defining rights and obligations, finality and irrevocability, and settlement finality. In order to safeguard the protection of customers' assets, market participants should determine appropriate liability regimes to minimize the potential loss for their customers. Legal risks should also be mitigated in case interoperability involves a settlement agent that temporarily holds the funds transferred between one market participant and another in a transitional account.

Title of recommendation	Interoperability scheme access and governance
Working Group	Interoperability
Audience for recommendation	Authorities, DFS providers

Access criteria for interoperability schemes should be clear, objective, publicly disclosed and allow for new participants, banks and authorized/regulated non-banks, to join. Equal representation of participants (irrespective of market size) in the scheme governance is encouraged. The governance process should foresee effective dispute resolution and the orderly exit of scheme participants without unreasonably disrupting the interoperability scheme, and an appeal mechanism.

Governance should ensure whether a decision to establish an interoperability arrangement appropriately reflects the objectives and interests of the relevant stakeholders and, if so, how. Market participants involved in an arrangement should preferably implement formalized mechanisms for sharing relevant information with the relevant stakeholders and consult them when needed.

Access criteria to interoperability arrangements should ensure a level playing field among market participants. If market participants are foreclosed or inhibited from joining existing interoperability arrangements, the result may be substantial inefficiencies that limit growth and/or reduces the benefits for end users. Access criteria should be justified in terms of the safety and efficiency of the system, as well as the broader financial markets. From a risk mitigation perspective, the access criteria should aim at minimizing legal, financial and operational risks. Participating market participants in an interoperability arrangement have the requisite operational capacity, financial resources, legal foundation and risk-management expertise so that risks are adequately mitigated and managed. From an efficiency viewpoint, the access criteria may be based on the business case. The access criteria should have the least restrictive impact on access that circumstances permit.

Access criteria should be commensurate with the risks generated by interoperability and those to which participating market participants may be exposed. If access to interoperable systems is refused by the system owners or operators to an applicant market participant, the reasons should be explained to the applicant in writing on the basis of the access criteria adopted.

When access criteria constitute terms and conditions for maintaining interoperability, they have to be continuously applied. Market participants should monitor compliance with participation requirements on an ongoing basis through the receipt of timely and accurate information. If conditions for maintaining interoperability are no longer met, rules and procedures should be legally set either for the termination of the non-compliant market participant or for dismantling an interoperability agreement depending on the extent of the problem.

Title of recommendation	Interoperability scheme provisions
Working Group	Interoperability
Audience for recommendation	DFS providers

DFS providers should ensure that their client contracts make the interoperability scheme rules transparent. Interoperability schemes should specify rules on payment and settlement finality and not put off-net transactions at a disadvantage as compared to on-net transactions.

DFS providers should be transparent in their customer relationship when it comes to interoperability. While the notion of "seamless" transactions is a key characteristic of the interoperability mission, customers should be able to take informed decisions when it comes to interoperable DFS and any specific rules that might result from the interoperability scheme.

A DFS providers participating in interoperable systems should be able to meet in a timely manner all of its obligations to the other participating entities. Furthermore, a provider's participation in interoperable systems should not compromise its ability to meet in a timely manner its obligations toward its own customers.

DFS providers and/or payment infrastructure providers participating in interoperable arrangements might be exposed to additional credit and liquidity risks and they should have access to all the information necessary to conduct an assessment of credit and liquidity risks associated with interoperability. A risk can materialize if a participating entity defaults causing liquidity pressures on other DFS providers and/or payment infrastructure providers. This risk may increase when a netting process takes place. Also, interoperability causes an additional exposure if a participating DFS providers and/or payment infrastructure providers temporarily holds the funds transferred between one retail payment entity and the other in a transitional account. Moreover, interoperability may create significant credit and liquidity interdependencies between systems.

Interoperability arrangements should specify rules on payment finality. Participating entities should state in their rulebooks that payments are final once they are confirmed as successful to the remitting entity. In other words, when the remitting DFS providers receives a positive confirmation from the beneficiary provider via the inter-provider system, payment finality has been achieved and the payment may not be recalled by the payer without the consent of the beneficiary. In addition, settlement should be guaranteed to ensure there is no settlement risk and that settlement is assured in the event of the insolvency and exclusion of an entity, particularly where settlement is based on a deferred model. The system of guarantees used will require agreement with the relevant national central bank(s).

Where interoperability involves more than one payment infrastructure, interoperability agreements should include rules for settlement finality. Guaranteed finality should apply to each step in the chain, i.e., where a payment flows from one payment infrastructure to another, the payment will be guaranteed in the first system before being passed to the second system. There are a variety of strategies for guaranteeing settlement. All such strategies require the remitting provider in some way guaranteeing payment to the beneficiary provider in a way that would not be affected by insolvency or provider failure. Some of the options are as follows: (i) cash prefunding (either periodic deferred net settlement or settlement in real time), (ii) pledging non cash collateral to the central bank, (iii) bilateral guarantees between banks, (iv) loss sharing agreements, or (v) trust lines.

Title of recommendation	Interoperability risk management
Working Group	Interoperability
Audience for recommendation	DFS providers

DFS providers that establish interoperability should identify, monitor, manage and mitigate its related risks, such as legal, operational and financial risks, before entering into an interoperability agreement and on an ongoing basis once the agreement is established. Interoperability schemes should assess the additional risks new participants might introduce, in order to maintain the integrity of the interoperability scheme, and ensure that scheme rules address accountability for risks appropriately.

Albeit being an important feature of payment system efficiency, interoperability may also be a significant source of risk. For this reason, pursuing it requires DFS providers to implement adequate standards addressing those risks.

DFS providers should conduct an initial risk assessment to evaluate the potential sources of risks arising from interoperability before entering into interoperability agreements. The type and degree of risk varies according to the design and complexity of interoperability arrangements and depending on whether one or more jurisdictions are involved. Interoperability should be designed in such a way that risks are adequately mitigated.

DFS providers should assess their risk management procedures to ensure that they can effectively manage the risks that may arise from interoperability. In particular, DFS providers should have robust risk management procedures to manage the legal, financial and operational risks they are exposed to through other entities, as well as those it poses to other entities. These procedures should include business continuity plans allowing for a rapid recovery and resumption of critical activities, or alternative channels for processing cross-system payments.

Furthermore, DFS providers that participate in interoperable systems should ensure that the risks generated in one system do not spill over and affect the soundness of the other systems. Particular attention should be placed on the links connecting the systems and the risks that could be transmitted through such links.

A DFS provider could use another provider to achieve interoperability (e.g. via a switch platform or a service provider such us a financial intermediary or a network operator). The DFS provider seeking to achieve interoperability should measure, monitor and manage the risks related to the other provider on an ongoing basis and provide evidence to the oversight authority that adequate measures have been implemented to limit and monitor these risks.

The management of risks should be commensurate to the number of parties involved in interoperable systems. As a result, the risks should be assessed, monitored and mitigated taking into consideration the number of entities involved in interoperable systems. The payment infrastructure provider should provide participants with the information necessary to conduct an assessment of the risks associated with the entity via which interoperability has been established.

Title of recommendation	Oversight aspects of interoperability
Working Group	Interoperability
Audience for recommendation	Authorities

Authorities should recognize that the responsibility for managing the risks associated with interoperability lies first and foremost with the operators of and the participants in interoperable systems. Authorities in their role as payment system overseer should address interoperability in their oversight frameworks and when they conduct oversight. The oversight principles should build on international best practices and take into consideration international technical standards.

An interoperable payment system and the effective management of risks associated with interoperability should be a key objective of payment system oversight. It is important to have a clear understanding of how and to what extent current international oversight standards provide for effective means to promote safe and efficient interoperability. It will then be possible to consider ways to strengthen the oversight policy framework, including identifying expectations specifically tailored for interoperability, against which payment system operators and PSPs should be held accountable.

Interoperability is addressed by the Principles of financial market infrastructures (PFMIs). As one of the different forms of interdependencies among financial market infrastructures (FMIs), interoperability is addressed in the PFMIs report under various principles. While the PFMIs address interoperability in several contexts, it should be recognized that they have not been designed specifically to cover the risks associated with interoperability in RPS.

While the risks associated with interoperability lies first and foremost with the operators of and the participants in interoperable systems, payment system overseers should define the requirements for them. The requirements should principles build on international best practices and cover risks associated with the legal, financial, and operational aspects of interoperability, as well as issues relating to their governance, access, efficiency, and effectiveness. Importantly, any sound oversight framework for managing risks relating to DFS interoperability will require strong cooperation between relevant authorities.

Title of recommendation	Payment infrastructure access & governance
Working Group	Interoperability
Audience for recommendation	Payment infrastructure providers

Payment infrastructures should have objective, risk-based participation requirements that permit fair and open access to their services. This can enable authorized and/or regulated DFS providers – including authorized/regulated non-banks – to establish interoperability among each other. The payment infrastructure governance should reflect the relevance of all DFS providers (banks and non-banks) appropriately.

Being able to make effective use of key payment infrastructures is an important element underlying a competitive payments market. Access to these payment infrastructures can enable interoperability among DFS providers thereby promoting competition, reducing fixed costs, enabling economies of scale that help in ensuring the financial viability of the service offered by individual DFS providers, and at the same time enhancing convenience for users of payment services.

Gaining access to clearing and settlement services is of capital importance for the ultimate success of new entrants into the market. In the absence of appropriate governance arrangements or safeguards, participants with a dominant position in a payments infrastructure may establish strategic barriers to prevent new entrants to the system. These barriers could be explicit or implicit in terms of higher pricing and access requirements. Certain payments infrastructure pricing and access policies can negatively affect interoperability and consequently competition.

Authorized/regulated non-banks are having an increasing role in payments in general, and in retail payments in particular, including for the continued development of digital financial services. Despite this increasing role, many authorized/regulated non-banks that provide payment services are still not accepted as direct participants in many payment infrastructures, either of a retail nature or a large-value nature. This often results in fragmentation of payment services and/or of DFS providers, which leads to their limited or null interoperability.

Title of recommendation	Telecommunication infrastructure access & governance
Working Group	Interoperability
Audience for recommendation	Authorities, Telecommunication infrastructure providers

Telecommunication infrastructure providers should not restrict access to their telecommunication services, impact service quality and/or discriminate among DFS providers. Telecommunication infrastructure providers should commit to creating an open and level playing field for the provision of DFS.

In some markets it has been observed that certain mobile network operators that are also DFS providers have restricted access to the mobile telecommunications network that they themselves operate and which is used by other DFS providers. Although different from restricting access to payment infrastructures, restricting access to the mobile telecommunications network is likely to have similar overall effects in terms of limiting interoperability and competition in the market place.

Telecommunication providers that compete with other DFS providers, but also own key communications infrastructure required to provide these DFS, might not only deny other providers access, they can also provide access at a high price and/or with poor quality affecting the customer experience, trust, and effective price. Telecommunication providers offering DFS should be able to prove that there is no discrimination among own DFS those offered by other DFS providers upon request by the telecommunication and/or financial regulator.

Telecommunication infrastructure providers, especially those who are also providing DFS, should commit to create an open and level playing field for the provision of DFS services. In this context, where telecommunication infrastructure providers or their subsidiaries are permitted to provide DFS, access to the telecommunications channel should be provided on a competitive, commercially viable basis.

Title of recommendation	Business aspects of interoperability
Working Group	Interoperability
Audience for recommendation	DFS providers

The implementation of interoperability arrangements should leverage the experience in establishing interoperability from other countries and/or other sectors. If available, international best practices and technical standards should be used. Shared infrastructures, within and across countries, should be considered for the processing of interoperable transactions.

Many markets are looking at varied ways of implementing interoperability arrangements and this presents the risk that all the domestic deployments operate on different principles and standards creating domestic anomalies for providers and making cross border transactions challenging. Interoperability can mean different things in different markets, but certain elements need to be addressed by all interoperability schemes/operating rules.

Interoperability agreements should cover a broad range of aspects of how participants agree to work with each other and cover aspects such as business models, settlement models, dispute rules, risk, governance and more. Promoting the use of existing rules as example may not only avoid duplication in effort and potential unnecessary domestic anomalies, but will also support regional and global harmonization enabling standardized and efficient future cross border transactions.

Infrastructure-level interoperability, whereby the same infrastructure can be used to support multiple payment mechanisms, is especially relevant for innovative payment products, since without some basic interoperability with more traditional payment instruments and systems their acceptance and/or usefulness for consumers might be very limited. In the absence of interoperability among payment infrastructures, a sizeable cross-membership combined with system-wide interoperability would enable achievement of de-facto cross-system interoperability.

Title of recommendation	Access point interoperability
Working Group	Interoperability
Audience for recommendation	Authorities and DFS providers

Access point interoperability should be encouraged and implemented. A common interoperability brand at access point level, such as agent, POS, or ATM, may ensure customer awareness of access point interoperability. Effective interoperability of agents by initiating transactions via the agent account to any transaction account should be aimed for to expand the effective size of service points/access channel networks.

Close proximity to bank branches, mobile money agents other points of access and channels is, generally, insufficient if there is limited or no interoperability between those points of access. In fact, at present, most innovative payment solutions are based on proprietary payment schemes that are not interoperable and as such can only be used at a limited number of access points.

The usefulness of transaction accounts is augmented with a broad network of access points that also achieves wide geographical coverage, and by offering a variety of interoperable access channels. The consequences of low interoperability are overlapping or limited coverage, sunken investment costs and inefficiency. For example, a proprietary payments infrastructure, such as a bank's own ATM or POS network that is not interoperable with other similar networks has limited impact on financial inclusion due to its limited network size.

Interoperability can play a critical role in expanding the effective size of service points/access channel networks. In contrast, exclusivity agreements limit the interoperability of service/access points that are otherwise interoperable. Non-exclusive agent arrangements promote competition within the ecosystem between DFS providers for both customers and agents.

If agent accounts can be used to initiate transactions to transaction accounts in other interoperable schemes, this could result in agent level interoperability without the need for the agent to open accounts in different schemes. The user of one mobile money scheme could cash-in at the agent of another mobile money scheme and the agent in turn transfers the corresponding amount from its mobile money account to the user's mobile money account at the other (interoperable) scheme.

Despite many markets having mandated non-exclusive agency arrangements, exclusive arrangements continue in practice. It is therefore important to implement cost effective mechanisms to monitor compliance.

4. Technology, Innovation and Competition recommendations

The recommendations here are further categorized under different streams:

1) Security
2) Identity and authentication
3) Mobile handsets use
4) Competition
5) Distributed Ledger Technology
6) DFS Vendor Platform

The recommendations are detailed below.

Title of recommendation	Cooperation and MOUs
Working Group	Technology, Innovation and Competition
Workstream	Security
Audience for recommendation	DFS Providers, MNOs, regulators

MOUs between the central bank and the telecommunications regulator should clearly delineate the need for the telecommunications regulator to undertake – with or without the cooperation of the telecommunications infrastructure licensee – monitoring of vulnerabilities in the telecommunications infrastructure, particularly in areas where there is a high volume of DFS transactions.

Cooperation should be strengthened between MNOs providing DFS services, the Central Bank, telecommunication regulators, payment service providers (PSP), and banks to assess and mitigate many of these security risks.

Title of recommendation	Mobile Devices
Working Group	Technology, Innovation and Competition
Workstream	Security
Audience for recommendation	Mobile Device Manufacturers, MNOs

The use of mobile devices that allow for the use of strong authentication mechanisms to demonstrate ownership of the device is recommended.

DFS Providers should recommend the use of mobile devices that support such strong authentication mechanisms. Because the key space of PINs allows them to be brute-forced, consider the use of longer PINs or alphanumeric PINs, such as easily remembered passphrases as arbitrarily long random sequences can lead to password information being written down. However, caution should be exercised before mandating complex PINs and ensure that any such adoption goes hand-in-hand with user education, as overly complex PINs are likely to be written down or entered by others, thus degrading their security.

Also consider how biometrics may aid with authentication and provide a second factor if they are stored securely within the device. Additionally, back-end analytics systems providing services such as IP velocity, geolocation, and time-of day access expectations, can act as authentication factors for the mobile device user.

Device manufacturers and MNOs should ensure that regular security updates are pushed to devices. Because security updates are critical to ensuring that mobile operating systems running on mobile devices are properly functioning and secure against exploits, potentially rendering DFS applications vulnerable, there should be mechanisms in place to ensure that security patches are made easily accessible to user devices.

Device manufacturers and MNOs should ensure that the handset operating system is configured in a way that reduces the size of the trusted computing base and the attack surface. Hardware and software mechanisms within mobile devices, such as secure elements and trusted execution environments can aid in the reduction of the TCB and help to ensure device integrity. Mobile devices that are so equipped should be promoted for use in DFS.

Title of recommendation	DFS application security
Working Group	Technology, Innovation and Competition
Workstream	Security
Audience for recommendation	App developers, DFS providers

App developers should ensure that DFS applications are designed and implemented in accordance with industry and Standards Setting Bodies (SSB) best practices for secure software development, including encrypted and authenticated communication and secure coding practices.

DFS app developers should make use of hardware and software features within mobile devices that enhance security such as secure elements and trusted execution environments for ensuring device integrity. While such mechanisms are made available at the level of the operating system and may provide APIs for usage, it is often the responsibility of the app developer to ensure that the apps themselves leverage these features.

The use of best practices should additionally extend to software embedded in third party systems and web pages for communication with mobile money systems. Strong encryption should be employed for both data protection within the app and for communication with back-end services, and it is important that such mechanisms are used in all appropriate locations within the app. Such apps should also be designed to be resilient against denial-of-service attacks.

DFS providers should ensure that DFS apps are subject to external security review and penetration testing, and any recommendations should be acted upon. Applications should be designed to be robust against phishing software, and should guide customers to access and download applications through official channels to mitigate the risk of running code that is infected with malware.

App developers should ensure that apps securely manage customer credentials, and should use strong authentication mechanisms to protect against unauthorized access. Default usernames and passwords should be removed or reset so that an adversary cannot easily guess credentials.

Title of recommendation	Network Access and Fake Base Stations
Working Group	Technology, Innovation and Competition
Workstream	Security
Audience for recommendation	DFS providers, MNOs

Mobile Network Operators should implement security policies that maintain the integrity of their networks and prevent unauthorized access to customer accounts.

DFS providers should consider transitioning away from mobile applications that leverage unencrypted access technologies such as unencrypted SMS and USSD. Instead, solutions that use public cryptography and end-to-end security, that employ standardized and up-to-date cryptographic algorithms and ciphersuites, are strongly recommended. Such algorithms should be reviewed to ensure they remain robust against new security vulnerabilities. While existing architectures may be in place for the near-term future and it will likely take years for smartphones to become widespread enough to supplant feature phones, and hence to decommission SMS- and USSD-based DFS services, transitioning high-value and high-volume accounts (e.g., business and merchants) to smartphones that support end-to-end security can protect those accounts while ensuring that risk mitigation strategies are in place for feature phones.

MNOs in co-operation with national telecommunications regulators should install devices to identify fake base stations designed to capture clear-text SMS and USSD session data and customer credentials, and software should be installed to find these fake base stations. So-called "IMSI-catcher-catcher" devices can be used to identify and isolate these fake base stations or IMSI catchers.

MNOs should be required to report to the relevant authorities any intrusions to their base station infrastructure through SS7 exploits and fake base station attacks. Any evidence of "man-in-the-middle" attacks where data is being intercepted should be reported, as a centralized view of such activity can provide better resources to determine the scope of such activity and means of eliminating it.

Title of recommendation	Trusted Phone Number Spoofing
Working Group	Technology, Innovation and Competition
Workstream	Security
Audience for recommendation	MNOs, regulators.

MNOs and regulators should undertake active customer awareness campaigns to educate consumers about malicious messages, phishing, and spoofing attacks.

Market participants and regulators should encourage consumers and victims of such attacks to report the mobile number of malicious attackers to MNOs. This can allow MNOs to send warning messages throughout their network and to ensure that such mobile numbers are permanently blocked from the system, as well as providing a means of investigating and prosecuting the perpetrators of these actions.

MNOs should monitor incoming calls from interconnect carriers and undertake fake caller line ID analysis. A blacklist or whitelist of known bad (or good, respectively) caller line IDs, as well as other security mechanisms, should be implemented in order to mitigate the risks of attackers attempting to steal customer credentials.

Title of recommendation	SIM cards security issues
Working Group	Technology, Innovation and Competition
Workstream	Security
Audience for recommendation	MNOs

MNOs and DFS agents should be made aware of the risk of SIM swap operations and ensure that mechanisms are in place to ensure that the legal, verified owner of the SIM is being provided with a new card.

Systems should be made available by MNOs to ensure that PSPs can determine in real time whether a SIM has recently been swapped before high value transactions and payments to new beneficiaries are allowed. Having these controls in place can help to mitigate the effects of SIM swap fraud, a type of phishing fraud where attackers pose as MNOs to unsuspecting customers in order to steal their credentials.

MNOs should track any occurrence of SIM swap attacks. Customer service agents should implement processes for detecting potentially fraudulent activity, and MNOs can use data such as tracking device type and location to detect these SIM swaps.

Title of recommendation	Infrastructure security
Working Group	Technology, Innovation and Competition
Workstream	Security
Audience for recommendation	MNOs, DFS Providers

MNOs should be discouraged from using weak encryption ciphers and switching off encryption on their networks.

Where practical, MNOs should discontinue use of the GSM A5/0, A5/1, and A5/2 ciphers. These ciphers are known to be vulnerable to attack, and in the case of A5/0, no actual encryption is occurring.

Encryption should not be switched off in order to enhance data spends on mobile networks. Doing so can lead to data intrusions on the mobile handset and through the MNO's network.

MNOs should implement security policies that maintain the integrity of their networks and prevent unauthorized access to customer accounts. This includes logical and physical access controls, including ensuring there is no unauthorized access to and any use of Signaling System 7 (SS7) core components of the MNO's infrastructure.

MNOs should undertake, as may be required, continuous testing, intrusion filtering, and monitoring of their core networks, base station infrastructure, and licensed mobile phone frequency bands to ensure that there is no unauthorized access, disruption, or misuse. Testing and monitoring includes not only mechanisms to detect SS7-based attacks but also detection, where technically possible, of unauthorized radio frequency devices.

DFS providers and MNOs should develop security benchmark assessments and regular testing of defenses to protect against new attacks as part of a risk management framework. This is necessary to assure the continued security of stored data within these systems.

MNOs should install hardware and software solutions that filter rogue SS7 messages emanating from potential attackers. A significant number of attacks over SS7 can be prevented if ingress and egress filtering is performed by network providers.

Telecom and central bank regulators should jointly ensure that PSPs and MNOs undertake penetration testing of systems and networks. These testing, using either internal or third-party resources, should check for vulnerabilities within the provider networks. The results of these tests should be reported to regulators.

PSPs and MNOs should implement disaster recovery systems and processes to ensure that any intrusions into their networks do not result in loss of customer data and funds. The same resilience and best practices for IT security should optimally be followed by all stakeholders within the DFS ecosystem who are responsible for processing and storing critical data.

Title of recommendation	Third-party providers
Working Group	Technology, Innovation and Competition
Workstream	Security
Audience for recommendation	External providers

DFS and external service providers should employ strong cryptography practices to assure the confidentiality and integrity of data as it enters the provider network and as it is processed and stored within this environment, with a goal of end-to-end encryption.

DFS and external providers should keep systems up to date and monitored against malicious threats from outside code. While maintaining a robust perimeter against outside attack is important, providers should also ensure strong internal controls are in place to mitigate insider threats. Robust input validation routines on external and internal-facing services should be deployed. Ensuring that data is encrypted as it enters the network mitigates external threats to confidentiality, while ensuring that all sensitive consumer data such as PINs and passwords are encrypted within the internal network and while at rest mitigates internal threats against this data.

All PSPs should maintain a trustworthy supply chain via third-party providers of technical services. A trustworthy supply chain is necessary to assure the integrity of the PSP's infrastructure and data.

Title of recommendation	Companion Cards
Working Group	Technology, Innovation and Competition
Workstream	Security
Audience for recommendation	PSPs

PSPs should ensure that companion General Purpose Reloadable cards linked to DFS accounts require the use of cardholder verification.

PSPs should ensure that companion cards use EMV chips. These cards should also support strong verification mechanisms such as PINs or biometrics where practical.

PSPs should ensure that all card transactions result in an alert to customers. This is necessary to ensure that customers are protected against unauthorized use of their cards.

Title of recommendation	Liability in case of MNO infrastructure exploitation
Working Group	Technology, Innovation and Competition
Workstream	Security
Audience for recommendation	Device manufacturers, DFS providers

Terms and Conditions of DFS customer contracts should be modified to acknowledge liability shift in loss of consumer funds, through the possibility of the MNO infrastructure being exploited.

In addition, device distributors should ensure that new devices do not contain any factory-installed malware of similar software that could compromise DFS accounts. The use of hardware-backed security mechanisms on mobile devices, and the assurance of only essential programs that have been evaluated for security loaded onto these devices by MNOs can mitigate the spread of malware onto these devices.

Title of recommendation	Secure transactions
Working Group	Technology, Innovation and Competition
Workstream	Security
Audience for recommendation	DFS Ecosystem stakeholders

It is clear that the security of all transactions within the DFS ecosystem rests upon the safe and secure transmission of data between users and service providers. We thus strongly recommend the development and implementation of end-to-end security techniques employing standardized and up-to-date cryptographic algorithms and ciphersuites to ensure data stays confidential and has integrity protection from the time it leaves the user's handset until it is delivered to its destination. The response from the provider to the user should be similarly protected.

Mobile devices increasingly contain additional hardware to improve data security; we recommend that DFS provides make use of these technologies to assure the security of information on the mobile device platform.

Best practices for data handling within DFS provider systems and network, such as the maintenance of audit logs, the use of least privilege, assuring data confidentiality, and premises security, are essential to ensuring the security of data and increasing its resistance to data breach attacks. The development of security benchmark assessments and regular testing of defenses to protect against new attacks is vital to assuring the continued security of stored data in these environments.

Title of recommendation	Creation of digital identity at registration
Working Group	Technology, Innovation and Competition
Workstream	Identity and authentication
Audience for recommendation	DFS operators

At time of registration, A DFS operator should create a digital identity for its customers, for use in both DFS transactions and (where relevant) in identity assertion with external service providers.

This transactional identity should be derived from a state-issued foundational identity to ensure reliability, flexibility and control. The transactional identity should be authenticated locally, not remotely, to ensure maximum security and the authentication (local) should be separate from authorisation (centralised). Provision should be made for periodic re-verification of identity attributes.

Title of recommendation	Issuance of a dynamic, self-asserted digital identity
Working Group	Technology, Innovation and Competition
Workstream	Identity and authentication
Audience for recommendation	DFS Operators

Where a customer is unable to provide a foundational document of digital identity, issue a dynamic, self-asserted digital identity.

The level of assurance of this digital identity should be developed over time, by measures such as:

- Associating a strong form of authentication, such as biometrics, with the identity, so that the service provider can be assured that the same person is accessing the service on each occasion;
- Attaching an attribute noting sponsorship/endorsement from someone who *does* have the necessary documentation/state-issued digital identity;
- Verifying the 2FA opportunity presented by a self-asserted mobile phone number;
- Adding additional attributes as further documentation becomes available;
- Noting repeated/consistent usage of the digital identity over a period of months.
- The nature of the financial services that can be delivered to the customer can then be linked to this level of assurance, rather than the initial lack of documentation

Title of recommendation	Standardization of digital identity registration
Working Group	Technology, Innovation and Competition
Workstream	Identity and authentication
Audience for recommendation	DFS Operators

Regulators should standardize digital identity registration, and ensure interoperability between DFS operators and service providers relying on the digital identity.

Relying parties need confidence that a digital identity is standardised (in format, reliability, and confidence) across DFS operators.

Title of recommendation	Streamlining of ID registration & subsequent authentication
Working Group	Technology, Innovation and Competition
Workstream	Identity and authentication
Audience for recommendation	DFS Operators

DFS Operators should ensure an intuitive and straightforward customer experience for registration and subsequent authentication.

Easy to use identification (registration) and authentication mechanisms and associated UE flows are an essential strategy for overcoming barriers to adoption presented by low literacy rates and complexity.

Title of recommendation	Build in customer privacy measures
Working Group	Technology, Innovation and Competition
Workstream	Identity and authentication
Audience for recommendation	Regulators in DFS ecosystem

DFS operators should build in customer privacy measures, compliant with national legislation either current or anticipated.

Citizen data protection and privacy measures are becoming increasingly common – so DFS operators should build them in even if the legislation is not yet in place, and ensure that any parties they provide with identity and attribute data (relying parties) take the same approach.

Title of recommendation	Availability of high speed mobile data access on smartphones
Working Group	Technology, Innovation and Competition
Workstream	Mobile handsets use
Audience for recommendation	Market participants in DFS

Market participants should encourage the distribution of smartphone devices that have high speed mobile data access.

Many of the devices currently being seeded into DFS markets are of low specification compared to marquee brands. While very affordable, they are often characterized by:

- Batteries that are mostly of low power capacity;
- Touchscreen displays that are of low resolution and relatively fragile;
- A minimum amount of RAM, just enough to run a few applications efficiently; and
- Insufficient internal storage to store more than just a few applications.

Some Android smartphones being sold by private-label distributors in the developing world markets do not have 3G (or higher) mobile data connectivity. The retail packaging for these devices often does not identity these devices as lacking this high-speed access.

Market participants thus should encourage:

- Distribution of smartphone devices that have high speed mobile data access, and
- Accurate descriptions of their features on retailing packaging and in marketing materials

Title of recommendation	Availability of high speed mobile data access at national level
Working Group	Technology, Innovation and Competition
Workstream	Mobile handsets use
Audience for recommendation	Regulators and market participants in the DFS ecosystem

Regulators should interact with industry to encourage national high speed mobile coverage. To make this cost effective, this coverage could be facilitated through national roaming and infrastructure sharing.

Not all MNOs have 3G/4G coverage overlaid over their 2G coverage. This gap in provision of high speed mobile coverage mainly affects rural areas.

This may the result of high spectrum fees imposed by authorities, and/or the uneconomical cost to providers of installation and maintenance of new base station infrastructure. One or both of these factors – and others - could discourage MNOs from providing national high speed mobile data coverage, and could discourage the downstream adoption of smartphone-based DFS-apps that require high-speed access to provide an acceptable user experience.

Regulators should interact with industry to encourage the provision of national high speed mobile coverage and also take proactive steps to make spectrum available where required.

To ensure that high-speed national mobile coverage is cost effective, this could also be facilitated through national roaming and infrastructure sharing where possible.

Title of recommendation	USSD access and regulatory focus
Working Group	Technology, Innovation and Competition
Workstream	Mobile handsets use
Audience for recommendation	Regulators in the DFS ecosystem

Despite the increase in alternative access mechanisms, the continuity of feature phone penetration and growth means that access to DFS services is likely to continue to be via USSD and STK, and therefore regulatory focus on these access mechanisms should persist.

Basic and feature phones currently constitute the majority of the phones used in DFS ecosystems worldwide. They are likely to dominate for the next few years.

A move to a more smartphone-centric ecosystem using app-based DFS access may be circumscribed by the lack of national high speed 3G/4G mobile data coverage in many of the countries where DFS is provided. The lack of high speed mobile data coverage mainly affects rural areas, where USSD & STK dominate.

The sub-optimal user experience of having to run relatively higher bandwidth-requiring smartphone apps in a 2G/2G+ environment, suggests that the current basic USSD and STK bearer access types for DFS services as used on basic and feature phones are likely to persist.

Existing concerns in some markets on Fair, Reasonable and Non Discriminatory terms for access to these basic 2G/2G+ USSD and STK bearer services is likely to require continued regulatory focus on these access mechanisms.

Title of recommendation	Strengthening competition law through institutions
Working Group	Technology, Innovation and Competition
Workstream	Competition
Audience for recommendation	Member States and regulators in the DFS ecosystem

As DFS market(s) are prone to market concentration and potential anticompetitive practices due to the intrinsic market characteristics of financial services and telecoms, governments and regulators in nations wishing to enable DFS should make competition law a policy priority. In this respect, they should strengthen relevant institutions.

- DFS market(s) implicate at least two industries – financial services and telecommunications - whose characteristics (significant fixed costs and sunk investments, economies of scale and scope, essential facilities and bottlenecks of network industries) make the sector more prone to market concentration and potential anticompetitive practices such exclusionary and/or cartelistic behaviour.[1]
- Given these specific market attributes, Member States should strengthen the application of competition law to the DFS ecosystem, by strengthening existing institutions themselves and their enforcement.
- To strengthen the competition institutional capacity, there are several principles that have been distilled from best practice, which governments and regulators may wish to consider:
    - The passage of a national competition law, if none currently exists. A separate framework for competition matters, rather than piece-meal sectorial legislation, ensures that there is a homogenized treatment of competition issues across all industries, which benefits players in cross-industry markets such as DFS.
    - Ensuring national competition regulation does not provide for any exclusions for specific sectors or state entities. This prevents the discriminatory and/or privileged treatment such entities operating in market sectors.
    - Where resources are available, the creation of a separate national competition authority, with a clear demarcation of jurisdictional competence between the competition authority and other sector-specific regulators in its founding legislation.
    - Where a competition authority exists, rendering the competition authority as an independent administrative body. Substantial autonomy for the regulator ensures effective implementation of competition law in DFS.
    - Appointment of the competition authority members by parliament or a national assembly to further ensure independence of the regulator.
    - Ensure that the competition authority is free from any government veto, though this does not exclude the possibility that the authority's decisions may be appealed to higher bodies, or within the legal system.

[1] The World Bank Group (2016) *ibid*

Title of recommendation	Regulatory collaboration
Working Group	Technology, Innovation and Competition
Workstream	Competition
Audience for recommendation	Member States and regulators in the DFS ecosystem

To ensure effective implementation of competition law, governments should clearly define which authority(ies) is/are responsible for which specific competition law issues. Where a competition authority co-exists with sector regulators who also have competition competence, all regulators should coordinate jurisdiction and competence between themselves, potentially through formalized MOUs. Where there is no established competition authority, other domestic sector-specific regulators, either on a national or regional level, should be empowered and encouraged to lead and define a coordinated way forward on competition issues.

Given that DFS are cross-industry products, it is not always clearly defined who the competent authority(ties) is/are for completion law issues, which can create jurisdictional conflicts between authorities, result in double jeopardy for regulated firms, and incentivize forum shopping.

Collaboration on a national level may also include the creation of a national forum to discuss a coordinated strategy, if such collaboration is not prescribed in the legislation itself.[2] The key to such coordination will be the will of stronger, more established authorities, such as central banks, to support those who are still developing their capacity, such as recently established competition authorities.[3]

Further, given that useful lessons can be gleamed from the experience of other countries as well, especially for countries with a nascent competition culture, participation by regulators in international forums should be a corollary priority.

Where such regional blocs (such as COMESA) have antitrust or merger control provisions, it should be noted that close coordination with national authorities with overlapping jurisdiction should be ensured to prevent jurisdictional conflicts.[4]

[2] Sitbon (2015) *ibid*
[3] As was the case in Kenya. See Mazer and Rowan (2016)
[4] Sitbon (2015) *ibid*

Title of recommendation	Competition authority expertise in DFS
Working Group	Technology, Innovation and Competition
Workstream	Competition
Audience for recommendation	Regulators in DFS ecosystem

Given the complex nature of DFS, competition authorities or sector-specific regulators, where relevant, should, to the extent possible, be staffed with specific expertise relating to DFS, financial inclusion and its adjacencies.

One reason why competition issues are often identified at a late stage in market evolution is the lack of institutional expertise on a regulatory level in many DFS nations. Regulators may lack expertise in sophisticated economic competition analysis or in the subject matter itself, DFS, which is extremely complex. This may be due to resources, but also to limited sectoral experience, especially for newly created entities.

To ensure timely identification of competition issues, the allocation of sufficient financial and human resources (including both overall number of staff and technical staff with economic and/or legal skills) and the development of DFS expertise should be the focal points, thus allowing the authority to ensure competent handling of DFS investigations.

In this respect, the national and international financial inclusion experts (often found at the financial regulator, but also available from international organizations, NGOs and consultancies) as well as competition law experts and economists can play a large role in helping to build permanent in-house capacity.[5]

[5] Sitbon (2015) ibid

Title of recommendation	Strengthening competition law through enforcement
Working Group	Technology, Innovation and Competition
Latest Revision Date	6/12/2016
Audience for recommendation	Member States in the DFS

As a corollary to the need to strengthen relevant institutions, to ensure a fair playing field in DFS markets, governments should equally strengthen the enforcement powers of the bodies responsible for compliance with competition law.

To ensure that DFS markets function fairly and to guarantee an equal playing field for all stakeholders in the ecosystem, especially given the large number of entrenched interests that can be found in DFS markets, competition authorities or their counterparts in sector regulators need to have real powers to prevent anti-competitive behaviour, as well as to sanction ex post abuses.

To this end, competition authorities should have the concrete ability to detect and sanction anti-competitive behaviour. Such tools include fines that ensure adequate deterrence, the ability to impose injunctions and structural (such as the break-up of entities with Significant Market Power (SMP) who abuse their dominance) as well as behavioural remedies, search and seizure powers (including dawn raids), the establishment of a leniency program, the ability to compel disclosure of relevant information and the promotion of settlements.

Competition authorities should equally have the concrete power to preempt future market distortions through the implementation of effective merger control. To ensure that such control is most effective, pre-notification of mergers should be mandatory, allowing fast track procedures or a two phase review process to prioritize the more complex and/ or problematic cases (in which DFS cases are more likely to fall) while concurrently imposing notification thresholds to reduce the administrative burdens on both the market players and the authority.[6] Further, due process, such as oral hearings, technical discussions with case handlers, access to statements of objections and to case files, publication of annual reports, and publication of decisions issued, ensures a fair and transparent process, and strengthens the reputation of the competition authority or sector regulator, especially in a market such as DFS where there may be several powerful and connected players.[7] Lastly, rules regarding conflicts of interest and the separation of the investigation, prosecution and decisional functions in case handling further support the independence and reputational strength of the authority.[8]

Competition authorities should balance their actions with other government interventions to minimize restrictions on competition in those areas. This may be through the provision of opinions and statements on policy and legal reforms and/or the conduction of sectoral studies and issuance of recommendations to other government bodies[9], even when such opinions are not formally foreseen in the legislation.

[6] *ibid*
[7] *ibid*
[8] *ibid*
[9] *ibid*

Title of recommendation	Capacity building for distributed ledger technologies
Working Group	Technology, Innovation and Competition
Workstream	Distributed Ledger Technology
Audience for recommendation	Member States in the DFS

Regulatory (and legal) capacity to understand the technology, engage with industry, design policy around Distributed Ledger Technologies (DLTs), and properly regulate where needed, is critical to DLT use for financial inclusion. Thereto, regulators should undertake capacity building exercises with other regulators, ministries, academia, and industry.

Distributed Ledger Technology (DLT) represents an evolving technology shift that may potentially usher in a new way of storing and accessing information across the world, as well as disintermediate guarantors, authenticators, and trusted third parties.

This has the potential to replace many of the established procedures and mechanisms in *inter alia* finance, rights managements, and identity management.

There are already commercial implementations of DLTs, for example, the cryptocurrency Bitcoin. Other are being tested in limited scale by commercial actors and governments. The momentum though is towards large-scale launches of DLT.

Regulators need to understand the implications of DLT in their markets and should undertake capacity building exercises with other regulators, government ministries, academia, and industry to understand the permutations of DLTs and the impact of its emergence. In particular, any effects of DLTs on financial inclusion should be explored.

Title of recommendation	Use of functional approach to implement laws and regulations
Working Group	Technology, Innovation and Competition
Workstream	Distributed Ledger Technology
Audience for recommendation	Regulators in DFS

Any changes to laws and regulations across multiple sectors should use a functional approach to ensure that there are no technology-specific constraints to implementation of new technologies.

Often regulations are technology-specific, be they for various payment instruments or automation. This silo'd regulatory approach and associated laws and regulation is challenged in this multi-sectoral environment.

Distributed Ledger Technologies may expand this universe of potential regulators by linking multiple sectors and requiring regulatory coordination. This has been evident in multi-regulator approaches to the emergence of the Bitcoin DLT.

In anticipation of the emergence of DLTs in their market at scale, regulators and legislators should plan for using a functional - rather than an institutional or technology-specific - approach to regulation and amendments to existing legislation.

This would avoid situations of institutional- and technology-specific laws and regulations that could potentially constrain innovation and implementation of new technologies.

Title of recommendation	Provision of no-action relief, or interpretive guidance for Distributed Ledger Technologies implementations
Working Group	Technology, Innovation and Competition
Workstream	Distributed Ledger Technology
Audience for recommendation	Regulators in the DFS ecosystem

As it may not always be possible to use existing financial laws and regulations for Distributed Ledger Technologies (DLTs), changes to laws or regulations, no-action relief, or interpretive guidance from regulators may be necessary.

As DLTs implementations spread across the globe, regulators, policy marker and legislators may find that it is not always be possible to fit the use of DLT into existing financial laws and regulations.

To encourage innovation, no-action relief or interpretive guidance from regulators who have remit over implementations of DLTs may thus be necessary.

This approach may be accompanied by the use of regulatory sandboxes that allow DLTs to be tested in markets in a familiar form to that of the 'test and learn' regulatory philosophy of forbearance that bootstrapped the emergence and global success of DFS transactional platforms.

Title of recommendation	Use of regulatory sandboxes to encourage DLT and Fintech innovation
Working Group	Technology, Innovation and Competition
Workstream	Distributed Ledger Technology
Audience for recommendation	Regulators in the DFS ecosystem

Regulatory sandboxes that allow DLTs to be tested in markets should be embraced by regulators in a familiar form to that of the 'test and learn' regulatory philosophy used for the first DFS implementations.

An emerging tool being used by some regulators are so-called regulatory sandboxes that allow new technology and financial innovations.

These allow financial technology (FinTech) companies and new technologies to get the benefit of temporarily avoiding the full regulatory process to which a FinTech product or service launch would typically be subject. The intent is to encourage and enable experimentation of solutions that leverages technology innovatively to deliver improved financial products and services to both consumers and businesses. Normal consumer protection rules still apply during the testing phases, and usually these technologies must later obtain all the necessary regulatory permissions, when the sandbox scheme has come to an end.

In a DFS context, the sandbox concept is of a familiar form to the 'test and learn' regulatory philosophy of forbearance that bootstrapped the emergence - and huge global success - of DFS transactional platforms.

The concept could be 'formalised' by regulators in terms of sandboxes and extended to broader range of services that can be enabled through DLTs.

Title of recommendation	Identification & bolstering of vendor platform feature sets
Working Group	Technology, Innovation, and Competition
Workstream	DFS vendor platform
Audience for recommendation	Regulators and DFS vendor platform providers

DFS platforms could leverage the features and functions from multiple vendor platforms and include multiple access options on the side of customers in different countries and for different electrical devices (e.g. computer, laptop, feature mobile phone, and smart mobile phone), the interaction with the third-parties (e.g. bank, mobile operators, interoperability) and the popular and normal service function and system function.

The vendor platform features expected of a typical DFS deployment should include access options, cooperation with third-party partners, interoperability, key service functions, and system features. A reference instance of an architecture for a DFS vendor platform to support a variety of services is present within the report.

By identifying the common and general functions of the platform, regulators can focus their efforts on the services already adopted, given clear guidance for security and data controls, but also prepare for new services that may be deployed as the ecosystem matures.

Regulators need to consider the advancement of future services – many services will be combined to create new services. By providing clear guidance on the controls and mechanisms required in the relevant data sets and access channels, a vendor can advance their platform with confidence that the platform will meet developing market needs within a robust regulatory framework. A good example is identity capture – many current regulatory processes require capture of physical paperwork, however digital techniques and processes can overcome the weaknesses in such a process.

5. Consumer experience and protection recommendations

The recommendations here are further categorized under different themes:

1) General framework
2) Contracts/Disclosures
3) Fraud
4) Agents
5) Recourse
6) Revocability
7) Protection of funds
8) Payment and use of interest on customer funds
9) Data protection
10) Digital credit
11) Quality of service

Title of recommendation	Regulatory harmonization for all financial products
Working Group	Consumer Experience and Protection
Theme	General framework
Audience for recommendation	Regulators

Regulators should work individually and in collaboration with one another to harmonize coverage of different DFS provider types, and ensure consumer protection provisions apply to all financial products provided digitally. Regulations should require that consumer protection for DFS consumers is not inferior to that of consumers in the traditional banking sector.

Regulators should consider the unique characteristics of DFS – such as the use of agents, reliance on a technology interface, and longer and more complex value chains – in their approach to consumer protection. According to Consultative Group to Assist the Poor (CGAP)[10], key DFS consumer risks include: Trouble completing a transaction due to network/service downtime; insufficient agent liquidity or float, which also affects ability to transact; complex or confusing user interfaces; digital recourse issues; lack of transparent fees and other terms; fraud; and data privacy and protection concerns.

The increased number of entities involved in delivering DFS may elevate these risks and create gaps in oversight and accountability. For example, liability for the loss of customer funds due to fraud or mishandling may be unclear due to the involvement of several parties (including agents) delivering the service. New players and partnerships that deliver DFS may be subject to diverse forms of regulation and supervision, such as those governing banking, payments, telecommunications, and insurance.

Consumer protection rules need to specifically address DFS risks and be harmonized across different DFS provider types to avoid gaps and inferior treatment for digital versus non-DFS. Guidelines for E-Money Issuers in Ghana[11] obligate e-money issuers to fully adhere to any rules issued by the Bank of Ghana pertaining to consumer protection as well as such basic principles of consumer protection as: Equitable, honest, and fair treatment of all customers; transparency and disclosure of clear, sufficient, and timely information on the fundamental benefits, risks, and terms of any product or service offered in an objective and accessible form; sufficient and accessible information to customers on their rights and responsibilities; protection of customers' privacy; responsible business conduct of all staff and agents; and adequate systems and processes for complaints handling and redress.

Regulators' licensing procedures should ensure that DFS providers are subject to clear and enforceable rules that protect customer funds from loss due to a provider's insolvency, fraud, or other operational risks. One option is to require DFS providers to operate under the license of one regulator even if some services fall under the purview of more than one authority, an approach recommended[12] by the Alliance for Financial Inclusion (AFI). Regardless of how regulation and oversight are allocated, the roles, responsibilities, and information sharing rights and obligations of all participants should be clearly defined in regulations and interagency memorandums of understanding. This is in line with the G20 High-Level Principles[13] on Financial Consumer

[10] McKee, K., Kaffenberger, M., and Zimmerman, J.M. (2015), *Doing Digital Finance Right: The Case for Stronger Mitigation of Customer Risks*. http://www.cgap.org/sites/default/files/Focus-Note-Doing-Digital-Finance-Right-Jun-2015.pdf
[11] *Guidelines for E-Money Issuers in Ghana* (2015) https://www.bog.gov.gh/privatecontent/Banking/E-MONEY%20GUIDELINES-29-06-2015-UPDATED5.pdf
[12] *Mobile Financial Services Consumer Protection in Mobile Financial* Services (2014), http://www.afi-global.org/sites/default/files/publications/mfswg_guideline_note_7_consumer_protection_in_mfs.pdf
[13] *G20 High-Level Principles on Financial Consumer Protection* (2011) https://www.oecd.org/g20/topics/financial-sector-reform/48892010.pdf

Protection, which emphasize the need for cooperation by regulators of different segments of the financial and non-financial (e.g., telecommunications) sectors.

To enhance coordination and cooperation between various regulators, Jordan has established a "DFS Council" representing all types of DFS providers and super agents, along with other financial service providers such as microfinance institutions, insurance companies, governmental institutes, and money transmitters. This set up was created to help fill gaps and ensure adequate coverage of consumer protection and more customer-centric services and conduct across diverse providers.

Title of recommendation	Appropriate supervision & market monitoring measures
Working Group	Consumer Experience and Protection
Theme	General framework
Audience for recommendation	Regulators

Regulators should have in place appropriate supervision and market monitoring measures to hold DFS providers accountable for consumer protection outcomes. These should include standardized, electronic reporting requirements for fraud, complaints, products, etc. Regulators should also consider using consumer research, such as mystery shopping and SMS or IVR surveys, and other consumer engagement.

In order to adequately supervise and monitor their markets, regulators should require DFS providers to regularly report data related to complaints, fraud, types of product, and other relevant issues, segmented by channel, product, and service. Review of this information allows regulators to verify provider compliance with existing laws and regulations, and allows regulators to spot new issues, trends, and potential problems. The AFI notes[12] that as quantitative and qualitative data is collected and analyzed over time, regulators can use this information to make necessary adjustments to consumer protection and market conduct regulations and guidelines. The State Bank of Pakistan, for example, requires monthly reports on customer complaints of fraud and forgery incidents related to agent banking and actions taken.

Regulators should require DFS providers to submit reports using a standard template to facilitate offsite review, statistical analysis, and comparison across providers and products. Where practicable, providers should upload this report electronically. G20 High-Level Principles[13] on Financial Consumer Protection also recommend that aggregated complaints data and their resolution be made public, which would further enhance accountability and transparency.

Regulators should also use consumer research for supervision and market monitoring. Such research can be used to measure compliance with existing regulations and identify new problems that need to be addressed. For example, mystery shopping can identify how well agents comply with requirements to display fee charts, and how common it is for agents to overcharge. A mystery shopping study conducted for the ITU found that only 66 percent of agents visited in Zambia had fee charts displayed.

Other methodologies, such as SMS or IVR surveys, can give larger-scale, market-level indicators of consumer protection issues. A SMS survey conducted for the ITU, for example, found that 17 per cent of mobile money users in both Tanzania and the Philippines have lost money to a mobile money fraud or a scam. Such surveys can also assess consumer attitudes and perceptions on newer consumer protection issues. For example, the same survey for the ITU found that mobile money users in Ghana and the Philippines are most concerned about data privacy, while Tanzanians are less concerned. Regulators can also apply behavioural insights gathered from consumer research to inform their regulations. Finally, findings from consumer research can be triangulated with other data sources, such as complaints data from providers, to better understand the market and enforce regulations.

Title of recommendation	Demarcation of provider liability
Working Group/Work Stream	Consumer Experience and Protection
Theme	General
Audience for recommendation	Regulators

Regulators should delineate situations in which DFS providers are liable for outcomes that negatively affect consumers, including, but not limited to: Acts and omissions of agents, employees, and third-party service providers (e.g. agent network managers), including cases of fraud; loss or harm due to network issues such as network downtime; and fraud related to DFS systems/platform, including system or data breaches.

To promote an enabling DFS environment, regulators should clearly define and enforce provider liability for negative outcomes that affect consumers, including losses due to fraud, staff, or agent misconduct, and network and security issues. This is emphasized in the G20 High-Level Principles[13] on Financial Consumer Protection, which cite the need for strong and effective legal, judicial and/or supervisory mechanisms to protect consumers from fraud, abuse, errors, and enforce sanctions for such misconduct.

Customers may sustain losses from agent misconduct, such as agents charging extra "informal" fees, and from employee misconduct, such as unauthorized access to account data and identity theft. Quality of service (QoS) issues such as network downtime also open the door to losses due to fraud and erroneous transactions. For example, when a network is down, a customer may leave money with an agent to complete the transaction later, increasing the risk of agent mishandling. Less sophisticated or secure systems and equipment also present QoS issues with the potential for loss, for example, inadequate encryption standards may expose users to identity theft.

Regulators should hold DFS providers liable for losses due to acts or omissions of their agents, employees, network quality, and third-party service providers they engage with. For example, when DFS providers are liable for agent wrongdoing, they will have increased incentives to monitor their actions. Agents in turn will have incentives to act appropriately if they will be held accountable to the provider for losses due to their misconduct. Where multiple players are involved in different aspects of a DFS transaction, regulators should ensure that the primary service provider is liable for customer losses, and that service provider may work out alternative liabilities with third parties with whom they contract.

Bangladesh Bank's agent banking guidance[14], for example, spells out various technical and data security requirements (e.g., real-time processing, end-to-end encryption) for agent banking transactions to help ensure secure and reliable QoS. The guidance requires banks to submit copies of agreements signed between banks and their agents before launching a new product and specifies that banks must bear all the liabilities that arise from any improper action on the part of their engaged agents.

[14] *Guidelines on Agent Banking for the Banks* https://www.bb.org.bd/aboutus/regulationguideline/psd/agentbanking_banks_v13.pdf

Title of recommendation	Regulatory review of DFS provider contracts with customers
Working Group	Consumer Experience and Protection
Theme	Contracts/Disclosures
Audience for recommendation	Regulators

Regulators should review DFS providers' contracts with customers on a regular basis, such as every six months, and as informed by consumer complaints. Regulators should verify that contracts are in compliance with domestic laws and require that terms in violation of laws and regulations shall be void and removed. To the extent their legal mandate permits, regulators should also disallow unconscionable or unfair terms or practices such as limiting access to recourse, misleading terms, or omitting information about pricing or other key terms of service. Regulators should publish, in multiple channels likely to be seen by consumers, a list of examples of unconscionable and unfair terms and practices for DFS providers and public awareness.

DFS industry user agreements are considered contracts of adhesion or standard forms which do not allow consumers to negotiate changes to the agreement should consumers not agree with the specifics of the offer. Essentially, a consumer has two options: Adhere to the provider's terms and conditions or elect not to use the service. It is possible that this lack of real choice could contribute to consumers not reading user agreements, and/or simply clicking boxes, indicating acceptance without a true comprehension of the provider's obligations to offer a quality service, nor an understanding of the consumer's own obligations, such as a keeping one's PIN private or repaying credit installments on time.

ITU research on DFS user agreements illustrated that user agreements may contain clauses that are unfair to consumers. The research also highlighted that several of the DFS user agreements reviewed contained potentially illegal clauses when the substance of the user agreement was compared to the domestic legal framework. For example, two Kenyan DFS provider contracts mandate arbitration as the sole method of dispute resolution for consumers, even though Kenya's Consumer Protection Act, in section 88(1), states that requiring a consumer to submit to arbitration is invalid as it prevents a consumer from exercising a right to commence an action in the High Court.

In an example from Tanzania, the provider's user agreement states that it may change its charges and tariffs at its own discretion and without notice to the subscriber. This clause may contravene Tanzania's E-Money Regulations of 2015, section 44(2), which state that an E-Money issuer shall notify its customers of fees and charges before they are imposed. Arguably, if a DFS provider changes the tariffs without any notice to the consumer, this could be viewed as violating the E-Money regulations.

To enforce existing regulations and identify areas in potential need of new rules, regulators should review DFS user agreements on a regular basis. Regulators should indicate to DFS providers that any clauses deemed unfair will not be upheld and that they should be removed from the contract.

Regulators may also wish to publish examples of unfair terms and practices so that providers and consumers are on notice of what is considered unacceptable. For example, in 2015, the UK Competition and Markets Authority published an unfair contract terms guide explaining which terms and practices are considered blacklisted and which were on the gray list (i.e., suspect and unlikely to be upheld). Examples of gray-listed practices included binding consumers to hidden terms, disproportionate cancellation fees, or financial penalties and restrictions on consumer remedies.

In other countries, and even other industries, a regulatory review of standard form financial agreements is common. For example, in the U.S. insurance and real estate markets, a regulator must approve consumer contracts. In Peru, the banking superintendent conducts a review of financial services agreements for consumer financial products.

Title of recommendation	Accessibility of contracts to customers
Working Group	Consumer Experience and Protection
Theme	Contracts/Disclosures
Audience for recommendation	Regulators/Providers

Regulators should require providers make customer contracts available to consumers in readily and easily accessible ways, including in languages commonly spoken in the jurisdiction and via multiple means, including both digital and print versions available at agent and customer care locations. Regulators should also encourage DFS providers to keep contracts as short and precise as feasible, and to use simple wording that is easy for consumers to understand.

Uganda has 41 living languages[15], and its two official languages are English and Swahili. In Nigeria, there are 527 living languages spoken, with 10 of the languages considered the most commonly spoken in the country. Yet, the Consumer Experience and Protection Working Group's review of DFS provider contracts from those two countries (as well as 6 other African countries), found that consumer user agreements were only available in English. Only in Tanzania did the review find a single DFS provider contract that was available in Kiswahili, as well as English. If consumers are expected to understand and comply with contract terms, contracts should be in commonly spoken languages in the consumer's jurisdiction.

In addition to a population's spoken languages, providers also need to take into consideration the varying literacy rates amongst their user base, as well as the fact that consumers may have other obstacles to reading or comprehending a contract, like poor vision, low levels of education, or cognitive impairment. Further, the Working Group's review found that some contracts were not well drafted and the meaning was unclear, even to the lawyers tasked with reviewing them.

For this reason, certain legal frameworks already mandate that contracts be written in plain, simple, and readily understandable language; and that providers read and explain the contents to those consumers who are unable to read and/or who have comprehension difficulty.

For example, Malawi's Consumer Protection Act of 2003, Sec. 26(1) provides:

> Standard form contracts or agreements shall:
>
> (a) be drafted in the official language and in characters readable at single sight by any normal sighted person;
>
> (b) where the contract is entered into locally, have a written translation into the national local language and shall be read and explained to an illiterate, blind, mute, and similarly disabled consumer in a language he/she understands.

[15] Ethnologue https://www.ethnologue.com/

Title of recommendation	Summaries of key terms and conditions of DFS contracts in simple language
Working Group	Consumer Experience and Protection
Theme	Contracts/Disclosures
Audience for recommendation	Regulators

Regulators should require DFS providers to provide summaries of *key terms and conditions* in simple language both at the beginning of the contract and through other means easily accessible to customers, such as via SMS. These summaries should include core information necessary for DFS consumers such as:

i. **all prices and fees, using definitions established by regulator (see separate recommendation)**
ii. **the provider that is ultimately responsible for the service (e.g. if a bank is providing a service via a mobile money channel, then the bank's role is clearly disclosed);**
iii. **limitations, if any, on the consumer's ability to cash out;**
iv. **any explicit obligations of the customers (e.g. to maintain PIN secrecy);**
v. **under which circumstances the consumer bears the risk of loss and the provider not liable (e.g. when fraud results from a consumer giving out PIN);**
vi. **where and how to complain if the consumer has a problem;**
vii. **for credit products, relevant interest rates, as well as all delinquency and default penalties.**

In the CEP Working Group's review of 18 user agreements from nine different countries, key information such as pricing, who bears risk of loss and under which circumstances, and where and how to complain, were often missing from the consumer agreements. If these essential terms and conditions are missing from the user agreement, what will the default protocol be? Consumers are left to wonder, or worse, find out that adverse consequences apply when such an unanticipated event occurs.

The U.S. legislature determined that there are certain key terms and conditions that must not only be communicated to consumers about credit cards, but should be highlighted by displaying it in a box at the outset of the consumer's agreement. This box was named the Schumer Box after the Senator who proposed the legislation and it contains rates, fees, and other key points as required under the U.S. Truth in Lending Act. Further, the font size for these disclosures must be 18-point or greater and remaining terms in at least 12-point type.

DFS regulators should consider which terms and conditions they consider critical and important enough to be highlighted to the consumer prior to contracting and consider ways to make these disclosures prominent. Space constraints on mobile devices may be an issue, but still the most important terms and conditions should be listed in a simple, concise manner.

The working group considered the above seven key facts to be of primary importance such that they should be communicated to the DFS consumer in a prominent summary, set off and distinguished from the full user agreement.

Title of recommendation	Fee disclosure prior to completion of transaction with standard pricing definitions
Working Group	Consumer Experience and Protection
Theme	Contracts/Disclosure
Audience for recommendation	Regulators

Regulators should require disclosure of fees prior to the completion of a transaction, with the option to cancel the transaction after the disclosure. Regulators should also establish standard definitions for costs and fees, and require disclosure in line with these standard definitions to ensure consistency across offerings (e.g., how to calculate and disclose interest and fees for credit products).

The price of a financial service, particularly a credit or insurance product, can be very difficult for a consumer to determine. If the providers use different pricing terminology or varying definitions for their costs and fees, this furthers the confusion and makes it difficult for consumers to compare products, potentially harming competition. For example, for years the microcredit sector made no reference to whether they were charging a flat interest rate for loans or charging interest on a declining balance. The former was much more common in practice, as well as more expensive for the borrower. However, microcredit consumers were generally not aware of the distinction, and were frequently misled as to the true cost of a microloan. An organization called MicroFinance Transparency was established to bring more clarity to the issue of pricing in the microfinance industry and developed an app for the calculation of microcredit interest rates.

Transparency is critical for consumers, and many financial sector regulators globally have rules pertaining to it. In the U.S., the Truth in Lending Act went into effect in 1969 mainly as a response to murky sales tactics in the consumer goods and auto industry with regard to selling on credit. Various ways of obfuscating the true price of financing led Congress to develop the annual percentage rate (APR) as the standard acceptable calculation and means of communicating interest rates to consumers. A review conducted by the University of Washington's Evans School of Policy, Analysis and Research Group (EPAR) for ITU concluded that 18 of 22 countries reviewed had enacted regulations which mandate the transparent communication of costs of DFS. As an example, recently the Competition Authority of Kenya directed that by the end of 2016, DFS cost disclosures must be a priori, and that costs for all transactions, including loans, must be displayed on the consumer's mobile screen before the consumer hits 'accept.'

Rules for transparency and disclosure in other sectors also provide apt examples. The U.S. Federal Communication Commission's (FCC's) recent transparency rule on internet privacy mandates that U.S. providers of fixed and mobile broadband internet publicly disclose accurate information regarding network management practices, performance, and commercial terms of their services sufficient for consumers to make informed choices. The FCC highlights what substantive information must be conveyed to the consumer and further requires that communications be accurate. The FCC also specifies that all the provider's consumer-facing communications, including advertising mailings, advertisements on buses, web banners, as well as information available in their retail stores, must match what actually occurs during services provision. Violations of this rule are subject to significant fines ranging from USD 16 000 to USD 1.575 million per single violation by a provider.

Similar to an APR as a standard way to disclosure the price of credit, regulators should establish standard definitions for other DFS transactions, including for money transfers, loans, insurance, fees associated with savings accounts (such as withdrawal fees), and any others relevant in a market. Regulators should then require providers to provide meaningful disclosure and true transparency, including accurate, consistent information

to the consumer at the time when the consumer can best utilize the information (i.e., prior to making a financial commitment).

Title of recommendation	Liability for fraud
Working Group	Consumer Experience and Protection
Theme	Fraud
Audience for recommendation	Regulators

Regulators should establish that providers are liable for loss or harm due to fraud related to DFS systems/platforms, staff, agents, and third-party service providers, while consumers are generally responsible for fraud resulting from their negligence (such as negligence in sharing their PIN). Liability for third-party fraud could follow a similar approach to existing regulations, such as banking/agency rules.

Fraud leads not only to customer losses, but damage to the reputation of the provider and the industry as well, according to GSMA[16]. Research conducted for the ITU found that 83 per cent of mobile money users in the Philippines, 56 per cent in Ghana, and 27 per cent in Tanzania have received a fraudulent or scam SMS. In both Tanzania and the Philippines, 17 per cent of mobile money users have lost money to a fraud or a scam, and in Ghana 12 per cent have.

Consumers, especially those who are unfamiliar with formal financial services, may not be aware of the rights they have in the case of fraud, or find rules governing the liability of providers and customers confusing. The consumer may not even realize who the actual service provider is in cases where DFS are provided through agents or partnerships between multiple providers.

Regulators should clearly define and enforce provider liability for losses due to fraud that is related to the DFS system/platforms, staff, agents, and/or third-party service providers. Liability for third-party fraud, such as fraudsters sending randomly generated phishing messages, may align with existing rules in a market, such as banking or agency banking rules. Finally, consumers shall generally be liable for fraud resulting from their own negligence, such as when they share their PIN with an agent. The G20 High-Level Principles[13] on Financial Consumer Protection emphasize the need for strong and effective legal, judicial, and/or supervisory mechanisms to protect consumers from fraud, abuse, and errors and for regulators to enforce sanctions for such misconduct.

Better than Cash Alliance (BTCA)[17] guidelines state that customers should be promptly informed of suspected fraud and compensated for losses due to fraud by the provider's agents, employees, and third-party service providers, including third-party fraud caused by a reasonably preventable security breach. In Rwanda, banks are liable for, and have insurance to cover, third-party fraud. When multiple players (e.g., provider, agents, outsourced B2B service providers, or business partners) are involved in a transaction, regulators could review and/or approve governing contracts at licensing of the main provider and on an ongoing basis when new contracts are developed, to ensure that contracts and other agreements clearly define the responsibilities and liabilities of all participants. Regulations should provide guidelines as to what each agreement should cover.

Managing fraud risk requires DFS providers to have a good knowledge of consumers' potential vulnerabilities (e.g., phones with weak security features, low literacy, or customer reliance on third parties to help perform transactions) and to design their business processes and technical interfaces accordingly. CGAP notes that DFS providers in Uganda and Rwanda have identified their top consumer-facing fraud concerns as SIM swaps

[16] Gilman, Lara, Joyce, Michael. (2012) GSMA, *Managing the Risk of Fraud in Mobile Money*, http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/10/2012_MMU_Managing-the-risk-of-fraud-in-mobile-money.pdf

[17] Better than Cash Alliance. *Responsible Digital Payments Guidelines.* (2016) https://btca-prod.s3.amazonaws.com/documents/212/english_attachments/BTCA-Responsible_Digital_Payments_Guidelines_and_Background.pdf?1469034383

leading to identity theft; provider impersonation by fraudsters; false promotions, phishing or social engineering scams; network down time that creates openings for fraud; agents asking for a customer's PIN, increasing vulnerability to fraud; and agents overcharging for transactions, such as deposits that are supposed to be free.

The G20 High-Level Principles[13] on Financial Consumer Protection also state that consumers' rights come with responsibilities, which include avoiding opportunities for fraud by protecting their security credentials and following secure procedures. To that end, GSMA's Code of Conduct for Mobile Money Providers[18] states that DFS providers shall "educate customers on how to use mobile money services safely". Regulators should require clear disclosures regarding customer liability for certain actions along with education and awareness programs to communicate and reinforce these rules.

Regulators should also require that providers regularly update customers (either through the media or by text) on fraud trends that may impact them, with prevention tips (PIN controls, promotional scams, fake money transfer messages, etc.).

[18] GSMA *Code of Conduct for Mobile Money Providers* http://www.gsma.com/mobilefordevelopment/programmes/mobile-money/policy-and-regulation/code-of-conduct

Title of recommendation	Robust security and fraud mitigation systems
Working Group	Consumer Experience and Protection
Theme	Fraud
Audience for recommendation	Regulators

Regulators should ensure that DFS providers have in place robust system security and fraud detection, management, and mitigation measures and procedures at the time of licensing and on an ongoing basis, and regulators and providers should jointly conduct consumer and agent awareness efforts to prevent fraud.

Opportunities for fraud arise at numerous points during a DFS transaction, including network downtime, agent or staff misconduct, and risky behaviour by customers, such as sharing a PIN. In addition, customers may be subject to third-party fraud, such as phishing SMSs requesting money transfers. As such, regulators should ensure DSF providers have robust security and fraud detection programs. GSMA's Code of Conduct for Mobile Money Providers[18], for example, provides a list of important security and fraud management principles. Providers should also take into account the level of technology used in the market, such as less sophisticated equipment (e.g., basic handsets with inadequate encryption standards) that are more likely to expose users to identity theft.

ITU Focus Group's document, Commonly Identified Consumer Protection Themes for Digital Financial Services,[19] recommends that DFS are provided only by licensed entities that are regulated by a financial regulator. This is in line with an AFI[12] recommendation that regulators license and supervise DFS providers under an enforceable regulatory framework. Formal licensing standards should require regulators to assess a proposed DFS provider's understanding of its target market and relevant operational and security risks. Providers should be required to establish and maintain adequate: Policies; procedures; controls; audit programs; information systems; governance and reporting lines; and hiring standards, including background checks for agents and employees.

AFI[12] also recommends that DFS providers be licensed by one regulator, even though some providers may offer services that fall under the purview of more than one regulator. A single licensing framework will help to ensure consistency for consumers related to a DFS providers': financial and technical resources; internal controls; operational risk framework, including security controls; and account segregation requirements for customer funds.

Once licensed, the DFS provider should be required to adhere to these standards at all times and be subject to inspection to confirm their compliance. CGAP's paper on Supervision of Banks and Nonbanks Operating through Agents[20] highlights various approaches to monitoring and reporting agent activities. Good recourse systems are helpful for monitoring complaints related to fraud. Regulators could also assess the extent to which providers have an effective feedback loop between their AML-CFT and financial crime monitoring, complaints handling, and customer/agent awareness/education efforts to ensure fraudsters and fraud schemes are quickly identified and addressed, and customers are quickly made aware of schemes to avoid.

GSMA's Code of Conduct for Mobile Money Providers[18] states that mobile money providers shall educate customers on how to use mobile money services safely. These communications could occur using a variety of

[19] ITU-T FG-DFS – (2016), *Commonly Identified Consumer Protection Themes for Digital Financial Services* https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/09_2016/ConsumerProtectionThemesForBestPractices.pdf
[20] Dias, D., Staschen, S., and Noor, W. (2015), CGAP, *Supervision of Banks and Nonbanks Operating through Agents* https://www.cgap.org/sites/default/files/Working-Paper-Supervision-of-Banks-and-Nonbanks-Operating-through-Agents-August-2015.pdf

methods. For example, CGAP[10] reports that Kenya's Safaricom M-PESA uses SMS alerts, radio announcements in different local dialects, and newspaper ads to update customers on various fraud schemes, and Banco WWB in Colombia requires product security tips be given to customers when they open an account.

AFI[12] recommends that government agencies, including regulators, play a more active role in financial education programs for base of pyramid customers. FinCoNet [21] research provides several examples. Armenia's national strategy on financial education includes risk of fraud and forgery in online and mobile payments, and has a special section on security risks in online shopping and payment on the Central Bank's financial education website. The Indonesia Financial Services Authority has publications on its website for consumers on safety issues for online and mobile payments and launched a mobile app for internet and smartphone users on financial education matters. In South Africa, the consumer education department of the Financial Services Board has activities to inform consumers about scams and keeping their money and identity safe, which include workshops and exhibitions via a website, a call center, and face-to-face presentations.

[21] FinCoNet International Financial Consumer Protection Organisation. (2016), *Online and mobile payments: Supervisory challenges to mitigate security risks* http://www.finconet.org/FinCoNet_Report_Online_Mobile_Payments.pdf

Title of recommendation	Require fraud reporting per standardized fraud definitions
Working Group	Consumer Experience and Protection
Theme	Fraud
Audience for recommendation	Regulators

Regulators should standardize definitions of fraud types and require standardized, electronic, timely fraud reporting from providers. Regulators should use this and other information to monitor fraud types and trends in the market and determine whether and what type of additional fraud detection and mitigation measures are necessary and feasible.

Fraud is a key DFS security issue and its frequency is increasing, according to research by FinCoNet[21]. To monitor and control fraud, regulators need access to regular, timely, and standardized data. Although monitoring and circulating data on frauds and scams is essential to the health of the DFS sector, providers may be averse to reporting fraud incidents due to a perceived risk to their reputations. Regulators should mandate reporting of all DFS-related fraud and other criminal activity, and provide confidential mechanisms for sharing information.

Providers should submit fraud information electronically using standard templates and definitions to allow regulators to more efficiently aggregate and analyze data and trends and report emerging issues to providers, other regulators, and law enforcement. Analysis should inform additional fraud detection and mitigation measures, and regulators should disseminate aggregate information so that providers have a better understanding of fraud across the market and can take appropriate steps.

FinCoNet provides examples of fraud definitions. FinCoNet[21] also describes some of the main types of DFS fraud as theft of personal data and security credentials; identity theft based on profiling and tracking techniques; malware, phishing, and SIM card swaps (i.e., when a customer's mobile phone is attacked and phone calls and SMS are fraudulently received by a fraudster's SIM card). GSMA[16] lists and defines key fraud risks in terms of where in the process the fraud may occur, including, but not limited to, the following:

Transactional (customer) fraud

- Vishing/Smishing - phone calls or SMS to gather personal details such as account numbers, PINs or personal identification details.
- Advance fee scams – customers are duped to send funds under fake circumstances.
- Payroll fraud – a non-existent employee receiving funds.
- Reversal requests - customer requests to reverse transactions that were in fact successful, or unintended recipient cashes out following an erroneous transaction.
- False transactions - sending fake SMS to make customers believe a transaction was successful. Often accompanied by a reversal request.

Channel (agent) fraud

- Split transactions - agents split cash-in transactions in order to earn multiple commissions in a tiered commission structure.
- False transactions - agents transferring customer funds to a personal account.
- Registration fraud - creation of accounts for false, invalid, or duplicated customers for the purpose of obtaining extra registration commissions.

Internal (employee) fraud

- Internal fraud - employees colluding for unfair personal financial gain.
- Identity theft - employees accessing and exploiting customer information.

Title of recommendation	Coordination of risk management and fraud mitigation
Working Group	Consumer Experience and Protection
Theme	Fraud
Audience for recommendation	Regulators

Regulators overseeing different aspects of the DFS market should coordinate efforts among themselves for risk management and fraud mitigation, and they should coordinate with law enforcement agents such as police, investigative bodies, and the prosecutorial authority. Regulators should also encourage DFS providers to collaborate on fraud detection and mitigation, such as through the establishment of a "Fraud Forum" or other cooperation arrangements.

The World Bank/Bank for International Settlements report on Payment Aspects of Financial Inclusion (PAFI)[22] states that sound risk management, mitigation of fraud and abuse, and protection of consumers are key supervisory and oversight considerations for retail payment services. These objectives are challenged by the fact that DFS providers and their services may be subject to diverse forms of regulation and supervision, such as telecommunications, banking, payments, and insurance. CGAP[10] confirms that the increased number of entities involved in delivering DFS may create gaps in oversight and accountability and elevate risks to customers. For example, liability for the loss of customer funds due to fraud may be unclear due to the participation of several parties (including agents) delivering the service. These risks may be heightened for inexperienced users of financial services.

In light of the issues, regulators should formally coordinate oversight of DFS providers' fraud mitigation and risk management efforts to avoid gaps and inferior treatment for digital versus non-digital financial services. This is in line with the G20 High-Level Principles[13] on Financial Consumer Protection, which emphasize the need for cooperation by regulators of different segments of the financial and non-financial (e.g., telecommunications) sectors. Laws related to fraud and other criminal activities should also be adapted to the use of digital delivery channels. In addition, regulators should seek ways to cooperate in DFS fraud detection and mitigation efforts to develop a more complete picture of risks. This could include both formal information sharing agreements and mechanisms such as working groups, conferences, and newsletters to learn about emerging risks and issues.

DFS providers should be encouraged to collaborate on fraud and security prevention, as well. CGAP[10] reports that Bangladesh, Pakistan, and Tanzania have formal industry discussion and coordination processes, and Kenya holds forums for stakeholders to share and discuss market trends and issues such as fraud. The South Africa Bank Risk Information Centre (SABRIC) is a consortium of four major banks working together to combat bank-related crimes.

Another example of collaborative fraud prevention comes from Tanzania. CGAP[10] reports that to combat SIM card swaps, Tanzanian providers have imposed a quarantine period after switching SIM cards. During this time, the mobile money PIN cannot be changed. Some use "IMSI locking," which locks the SIM and blocks access to the account until the customer has confirmed that the SIM swap was legitimate and has the SIM in hand, at which point the new SIM will be linked to the account.

[22] Committee on Payments and Market Infrastructures World Bank Group, (2015)*: Payment Aspects of Financial Inclusion* https://www.bis.org/cpmi/publ/d144.pdf

Title of recommendation	Establishment of requirements for agents
Working Group	Consumer Experience and Protection
Theme	Agents
Audience for recommendation	Regulators

Financial sector regulators should establish and supervise conditions and requirements for agents engaged in DFS delivery, such as identification requirements and other qualifications. For conduct regulations, there should be no material difference between those applying to agents of banks and agents of nonbanks, so as to allow a consistent supervisory framework, avoid regulatory arbitrage, and create a level playing field that fosters competition and innovation.

Financial sector regulators should establish and supervise the conditions and requirements for agents engaged in DFS delivery, regardless of the type of DFS provider on whose behalf they are acting (e.g., telcos, banks), so as to establish a level playing field for DFS providers and avoid regulatory arbitrage. Regulators should establish conditions and requirements to enable DFS clients to recognize authorized agents. Regulators should also hold DFS providers accountable for meeting agent-related requirements, and establish fines or other repercussions for noncompliance. DFS consumers should be able to trust that the agent they use is indeed empowered to deliver the services, and should know who to turn to in case of recourse. (Refer to recommendations on recourse.)

As CGAP advises, many countries permit a wide range of individuals and legal entities to be DFS agents[23], while others limit the list of eligible agents on the basis of legal form. All agents providing financial services should be held to the same market conduct standards whether they are serving a bank or a non-bank DFS provider. Regardless of what form agents take, *The Model Legal Framework*[24] stipulates that agents and third-party service providers should be compelled to disclose to clients the nature of their relationship with a DFS provider any time they are marketing, selling, or servicing consumer financial products or services, or when they are providing services, including debt collection, in connection with consumer financial products or services. The *SBS of Peru*[25] states that agents shall have signs, plainly visible to the public, indicating clearly that they are a provider of services on behalf of the financial enterprise company with which they sign contracts.

Regulators should require that providers have contracts with agents or other outsourced service providers. AFI[12] states that contract templates for agents, as well as outsourced agent networks, should be reviewed to ensure that standards are in place. The regulator may find it useful to review or approve such standard form contracts. The G20 High-Level Principles[13] on Financial Consumer Protection state that regulators should indicate the conditions under which an agent can be sanctioned or see its license revoked.

[23] Tarazi, M., Breloff, P.. CGAP Regulating Banking Agents (2011) https://www.cgap.org/sites/default/files/CGAP-Focus-Note-Regulating-Banking-Agents-Mar-2011.pdf
[24] Microfinance CEO Working Group (2015) *Client Protection Principles: Model Law and Commentary for Financial Consumer Protection* http://smartcampaign.org/storage/documents/Model_Legislation_-_English.pdf
[25] Resolution S.B.S. Nº 775, *The Superintendent of Banks, Insurance Companies and Private Pension Fund Administrators* (2008) http://www.bu.edu/bucflp/files/2012/01/SBS-Resolution-No.-775-2008-on-Regulation-of-Banking-Agents.pdf

Title of recommendation	Liability of DFS providers for acts/omissions of agents
Working Group	Consumer Experience and Protection
Theme	Agents
Audience for recommendation	Regulators

Regulation should specify explicitly that DFS providers are liable for the acts and omissions of their agents, employees, and third party service providers (e.g., agent network managers, master agents, super agents, or other distributors).

Regulation should stipulate that providers have clear guidelines for what is expected of agents and have adequate monitoring systems to ensure agent compliance with policies. AFI[12] states that DFS providers should ensure that appropriate standards are in place to select, manage, and train their agents. G20 High-Level Principles[13] on Financial Consumer Protection also state that financial service providers should be responsible and accountable for the actions of their authorized agents. While regulation should permit DFS providers to enter into agreements with other entities (e.g., agent network managers, master agents, super agents, etc.) to support their agent networks, the DFS provider itself maintains responsibility for: the actions of agents and other outsourced service providers in delivering DFS; consumer outcomes related to DFS delivery; and ensuring compliance of agents and the agent network with regulatory requirements and DFS provider policies and procedures. The GSMA Code of Conduct for Mobile Money Providers[18] also states that mobile money providers "shall assume responsibility for actions taken on their behalf by their agents (and any sub-agents) under the provider-agent contract."

Bangladesh, Brazil, Colombia, DRC, Ghana, India, Indonesia, Kenya, Nigeria, Pakistan, Peru, Rwanda, South Africa, Tanzania, Uganda, and Zambia all have language that explicitly states that providers are either responsible or liable for agent actions. Ghana, Kenya, Rwanda, and Tanzania also include more extensive language specifying that providers are even responsible for actions that the provider may have specified as off limits in a contract. For instance, Bank of Ghana's Agent Guidelines[26] read: "A standard agency agreement shall, at a minimum…specify that the principal is wholly responsible and liable for all actions or omissions of agents providing services on its behalf, even If said actions have not been authorized in the contract, as long as they relate to agency business or matters connected therewith". More commonly, regulations assign liability to both providers and agents. For example, in South Africa[27] regulations state, "If an employee or agent of a person is liable in terms of this Act …, the employer or principal is jointly and severally liable with that person".

DFS providers should conduct regular or periodic checks on agents and conduct corrective actions as needed. Regulations in Bangladesh, Ghana, India, Kenya, Lesotho, Malaysia, Nigeria, and Tanzania indicate that regular or periodic checks on agents to ensure compliance with legal/regulatory requirements must occur. In Bangladesh[14], for example, "The banks must formulate internal audit policy to monitor and control agents. They should visit the agent's outlets at a regular interval to ensure that the agents are working in accordance with the terms and conditions of the agreement and following the rules, regulations and guidelines issued by the regulators." However, beyond saying that they should be regular or periodic, none of the regulations specify how often these checks should take place. Brazil, Colombia, Indonesia, Pakistan, Rwanda, Sierra Leone, South Africa, and Uganda mandate that monitoring should take place, but regulations do not specifically require

[26] Bank of Ghana, *Agent Guidelines* https://www.bog.gov.gh/privatecontent/Banking/AGENT%20GUIDELINES%20UPDATED3.pdf
[27] Republic of South Africa, *Consumer Protection Act* (2008) http://www.wipo.int/edocs/lexdocs/laws/en/za/za054en.pdf

regular checks. For instance, the Bank of Uganda[28] states: "In its dealings with mobile money agents, a mobile money service provider must… put in place mechanisms for supervising the mobile money agents to ensure agents conduct business in accordance with these Guidelines and any other relevant regulatory provisions".

DFS providers' corrective actions should be informed by issues identified during internal audits and through client complaints. As agents who are treated poorly are less likely to deliver acceptable and safe services to customers, regulators should require that DFS providers monitor agent complaints as well as client complaints. The Smart Campaign[29] highlights the multiple problems and complaints that agents also have with their DFS providers. In addition to a system that allows for the monitoring and addressing of complaints from clients to agents, agents should also have access to a recourse mechanism(s) in order to address complaints against their DFS providers. (Refer to recommendations on recourse.)

[28] Bank of Uganda, *Mobile Money Guidelines* (2013) https://www.bou.or.ug/opencms/bou/bou-downloads/Financial_Inclusion/Mobile-Money-Guidelines-2013.pdf

[29] Bansal, H., Caruso, C., Kumari, T., Rizzi, A., Shrivastava, P., Yaworsky, K. (2016) The Smart Campaign, *Protecting Clients and Earning Trust, Exploring Responsible Agent Management in India* *http://smartcampaign.org/storage/documents/Responsible_Agent_Management_Final_2016_08_09.pdf*

Title of recommendation	Requirements for onboarding and training of agents
Working Group	Consumer Experience and Protection
Theme	Agents
Audience for recommendation	Regulators

Regulators should require that DFS providers: Conduct adequate compulsory onboarding and ongoing training of agents; require agents to display relevant information for consumers, such as prices and fees, in a visible manner; provide a toll free complaints channel for agents to contact the DFS provider; conduct regular monitoring of agents to ensure they offer safe and reliable services and comply with all relevant operational, legal, and conduct requirements; and maintain an adequate framework for agent liquidity and float management.

DFS providers should carefully select and onboard agents, to ensure understanding of their policies and processes, and should provide on-going training for reinforcement of these policies and processes. The GSMA Code of Conduct for Mobile Money Providers[18] states that providers shall "screen, train, and monitor staff [and] agents…to ensure that they offer safe and reliable services and comply with all relevant operational and legal requirements."

DFS providers should provide appropriate training to agents and ensure that their authorized agents act in the best interest of consumers. Numerous references point to this recommendation including: The G20[13], World Bank Global Practices [30], AFI[12], and The Smart Campaign [31]. Training should include guidelines on impermissible conduct with respect to customers, including integrity and non-discrimination, as well as issues of complaints handling and fraud detection. Bangladesh, Brazil, DRC, Kenya, Nigeria, Peru, Sierra Leone, Tanzania, Uganda, and Zambia have regulations that mandate training for agents. For example, Kenya[32] and Nigeria's[33] central banks direct that agents have to be trained on proper identification of customers, customer service, confidentiality of information, cash security, record keeping, and financial education. Peru[34] requires training on "identification of and service to clients, confidentiality, and banking secrecy", while Uganda[29] mandates training on how to receive complaints and handle their resolution and escalation.

Regulators should mandate that providers require their agents to clearly display all prices and fees for DFS services at their agent location. Providers should also require agents to provide full, transparent, and relevant information about products and services through other means, such as verbally. Agents should also be required to provide clients with information about the client's rights and responsibilities, as well as about mechanisms for redress. As a reference point, mystery shopping conducted by the ITU showed that only 66 per cent of agents visited in Zambia had fee charts displayed, and only a fifth had printed brochures that clients could take with them. In addition, when quoting fees verbally, more agents quoted incorrect fees than quoted correct fees.

[30] The World Bank, *Good Practices for Financial Consumer Protection* (2012) http://siteresources.worldbank.org/EXTFINANCIALSECTOR/Resources/Good_Practices_for_Financial_CP.pdf
[31] The Smart Campaign *Client Protection Certification Standards* (2016) http://www.smartcampaign.org/storage/documents/Standards_2.0_English_Final.pdf
[32] Guideline on Agent Banking – CBK/PG/15 (2012) http://www.bu.edu/bucflp/files/2012/01/Guideline-on-Agent-Banking-CBKPG15.pdf
[33] Central Bank of Nigeria, *Guidelines for the Regulation of Agent Banking and Agent Banking Relationships in Nigeria (2013)* http://www.cbn.gov.ng/Out/2013/CCD/GUIDELINES%20FOR%20THE%20REGULATION%20OF%20AGENT%20BANKING%20AND%20AGENT%20BANKING%20RELATIONSHIPS%20IN%20NIGERIA.pdf
[34] Resolución S.B.S. Nº 6285, El Superintendente de Banca, *Seguros y, Administradoras Privadas de Fondos de Pensiones* (2013) https://intranet2.sbs.gob.pe/intranet/INT_CN/DV_INT_CN/714/v1.0/Adjuntos/6285-2013.r.pdf

This indicates the need for strict disclosure and training requirements to ensure customers receive needed, accurate information.

Regulation should create clear expectations that DFS providers will ensure that agents do not coerce clients into using products that do not meet their needs and would be harmful to them. Agents should not use aggressive sales and marketing techniques or intimidate clients.

Agents should not charge clients additional fees than those agreed to by the DFS provider, and the DFS providers should be required to monitor agents for compliance. Many countries prohibit agents from charging additional fees in cash to consumers for DFS services. Bangladesh, Brazil, Colombia, Egypt, Ghana, India, Kenya, Pakistan, Peru, Rwanda, Sierra Leone, Tanzania, and Uganda have regulations on DFS consumer fees. For example, Bangladesh Bank's Guidelines on Agent Banking for the Banks[14] states: "Customers should not be charged directly by the agents for providing services to them".

DFS providers should put in place appropriate management systems to monitor and verify the conduct of agents, and put in place corrective measures if and as needed. GSMA[35] and the Smart Campaign[31] state that providers shall develop policies and processes for ongoing management and oversight of agents and entities providing outsourced services.

Providers should monitor and assess their agents' needs and put in place a toll-free complaints line and other agent redress mechanisms. Providers should also put in place a framework to ensure adequate liquidity and float management, so that transactions can be done in real time and without delays. Insufficient agent liquidity can cause serious harm to consumers. As highlighted by CGAP[10], it can either prevent clients' access to their funds, or result in extra costs or risks of fraud for consumers (due to split transactions, waiting time, sharing of PINs and other personal information, etc.). According to the Helix Institute of Digital Finance Agent Network Accelerator (ANA) surveys[36], lack of liquidity in Tanzania results in denial of an average 14 per cent of daily transactions in Tanzania and ten per cent in Uganda. We do not find any regulations that set minimum liquidity requirements at the agent level. Bank of Lesotho[37], Central Bank of Malaysia[38], and Superintendencia de Banca, Seguros, Y AFP of Peru[34], place loose prescriptions on agent liquidity with language indicating that agents should have "sufficient" liquidity, while others mention that providers should be aware of liquidity concerns. While no liquidity requirements are specified in regulation, we do find evidence that Ecuador sets minimum liquidity requirements for "macro" agents.

Agents are the stewards of client funds and data, and should not conduct transactions if there is a risk of loss of client funds due to service downtime, and should have appropriate policies in place to counter fraud. To prevent fraud and loss of funds, DFS providers thus should ideally prohibit agents or employees from conducting transactions in situations where conducting in real time is not possible. Bangladesh, Colombia, Ghana, India, Kenya, Nigeria, Rwanda, Sierra Leone, Tanzania, and Uganda have such regulations. For example, the Bank of Ghana[26] mandates that, "*Agents are not permitted to… [transact] when there is communication failure or when the issuance of physical or electronic receipt is not possible*". The Central Bank of Kenya[32] takes this prescription a step further by also requiring the disclosure of this prohibition: "*An agent shall disclose to the institution's customers in a conspicuous place on the agent's premises… a written notice to the effect that if the electronic system is down, no transaction shall be carried out*". AFI[12] also

[35] GSMA, *Code of Conduct for Mobile Money Providers,* (2015) http://www.gsma.com/mobilefordevelopment/programmes/mobile-money/policy-and-regulation/code-of-conduct
[36] Helix Institute of Digital Finance, *Digital Finance Data & Insights* http://www.helix-institute.com/data-and-insights
[37] Central Bank of Lesotho, *National Payment System Division Guidelines on Mobile Money* https://view.officeapps.live.com/op/view.aspx?src=http://www.centralbank.org.ls/NPS/_vti_cnf/Mobile_Money_Guideline_2013.DOC.doc
[38] General Payment Guidelines http://www.bnm.gov.my/guidelines/00_general/payment/guidelines/gl_016_3.pdf

recommends that real-time transaction services are in place and used. (Refer to recommendations on Fraud and Revocability.)

Title of recommendation	Standardized reporting on agents
Working Group	Consumer Experience and Protection
Theme	Agents
Audience for recommendation	Regulators

Regulators should require DFS providers to submit standardized electronic reports on agent onboarding, trends, sanctions, and bans that will enable the regulator to spot trends in the development of the agent business and emerging risks that could be subject to supervisory action. Data from such reports (with appropriate accuracy and privacy safeguards) can serve as the basis for a negative registry of blacklisted agents or similar report compiled by the regulator and distributed periodically or accessible to DFS providers. Regulators should also conduct regular checks on provider oversight procedures (e.g., field audit, mystery shopping).

Having regular reports on agent performance and practices is necessary to ascertain the current state of the market, and determine whether additional guidelines are necessary to protect clients on an ongoing basis. Supervisors should establish a standardised reporting framework that, while not overburdening the provider, enables the supervisor to fulfil specific and clearly articulated purposes, such as: identifying agent-related consumer issues; DFS provider-related agent issues (i.e., lack of support and training); monitoring the relative importance of agents in the eco-system; and spotting trends in the development of the agent business and emerging risks that could be subject to supervisory action. The G20 High-Level Principles[13] on Financial Consumer Protection state that there should be reporting requirements to allow the supervisor to monitor potential trouble spots or poorly performing DFS providers in the market.

Regulators should require DFS providers to submit standardised electronic reports on agent onboarding, recurrent agent training conducted by the provider or third-parties, trends related to agents, client and agent complaints, sanctions, and bans. Data from such reports can help supervisors assess whether an agent network is operating well, including agent conduct towards clients, and whether the agents are receiving adequate support from the provider and/or other parties to whom the provider has outsourced certain support and oversight functions. Indeed, agents depend on the support of DFS providers and a recent study by the Smart Campaign[29] highlights the gap between policies and application, as well as the lack of support from DFS providers to address systems and service issues. Agents reported frequent problems with bank servers and lack of response/engagement/consistent treatment from bank staff. Agents also complained of lack of back-end support from the agent network managers.

Data from reports (with appropriate accuracy and privacy safeguards) can serve as the basis for a negative registry of blacklisted agents or similar report compiled by the regulator and distributed periodically or accessible to DFS providers, to ease agent KYC. Where feasible, the register should utilize advanced identification technology, such as biometrics, for identifying agents.

Regulators should also conduct regular checks on provider oversight procedures (e.g., field audit, mystery shopping), to evaluate challenges faced by agents (and agent networks) and take them into account when reviewing agent performance. For example, a mystery shopping study conducted by the ITU showed that agents were inconsistent in checking customer identification, in displaying fee charts, and in enforcing transaction limits.

Title of recommendation	Require adequate internal complaints handling units
Working Group	Consumer Experience and Protection
Theme	Recourse
Audience for recommendation	DFS providers

DFS providers should establish an adequately staffed internal DFS complaints handling function which is accountable to the corporate governance. Regulators should require that DFS providers' complaints handling units or functions: Provide services in all languages commonly spoken in the jurisdiction, are free of charge, and allow customers to file with or without supporting documentation. Regulators should also set minimum standards for the efficiency and efficacy of the complaint resolution process (e.g., procedures and time parameters for receiving, tracking, and resolving complaints, communicating decisions, and escalating complaints).

The ability to ask questions and resolve issues is necessary for consumer acceptance and use of DFS. Reaching out to customer care is common among DFS customers; research commissioned by the ITU showed that 62 per cent of Tanzanian, 39 per cent of Ghanaian, and 29 per cent of Filipino DFS users have called a DFS customer care line. Research by CGAP[14] has found that customers are less willing to trust DFS when there are negative perceptions of available recourse if something goes wrong. Therefore, regulators should establish a robust recourse framework with well-defined rules and responsibilities for all participants, including: consumers; DFS providers; consumer and industry associations; and alternative dispute resolution bodies, if they exist in the market.

The first and most critical step in the dispute resolution process is the customer contacting the DFS provider. The correct provider to contact should be made clear to the customer, especially in situations where multiple providers, such as an MNO and bank, have partnered to offer a product. Each provider's governance must ensure that there are soundly written procedures, clear reporting lines, and adequately trained staff assigned to handle complaints. Because DFS and telecommunications are uniquely different services, staff assigned to deal with DFS concerns should have specialized training on issues related to the mobile phone service itself.

In line with the World Bank's Good Practices for Financial Consumer Protection[39], G20 High-Level Principles[13] on Financial Consumer Protection , and CGAP research[40], complaints handling and redress should not impose unreasonable cost, delay, or burden on consumers. The DFS complaints handling function should be offered using easy-to-understand terminology in a language appropriate to the customer, including local dialects and speaking or hearing impaired persons. Access to complaints handling should be free and easily accessible. Customers should be permitted to provide supporting documentation of their complaint, but not required to do so, as a requirement for documentation is a barrier to many customers, especially low-income, from having complaints resolved. Additional good practices[39] include providing a dedicated hotline for agents, training agents to deal with common and/or basic problems, and providing digital mechanisms to file a complaint, such as via SMS or social media.

[39] World Bank, *Good Practices for Financial Consumer* Protection, (2016) http://documents.worldbank.org/curated/en/583191468246041829/Good-practices-for-financial-consumer-protection

[40] CGAP, *Recourse in Digital Financial Services: Opportunities for Innovation* (2015) http://www.cgap.org/sites/default/files/Brief-Recourse-in-Digital-Financial-Services-Dec-2015.pdf

As described in the World Bank Good Practices for Financial Consumer Protection[39], providers should log and acknowledge receipt of all complaints. For example, the Central Bank of Nigeria[41] requires DFS providers to maintain a dispute and complaints resolution desk to receive and acknowledge complaints with a case identifier within 24 hours. Calls to the dispute and complaint resolution desk are required to be recorded and personal visits logged with the customer's name and signature or thumbprint.

Regulators could also require that DFS providers establish and follow maximum processing and response times so that there is consistency and accountability across providers. Extensions may be permitted for good cause to facilitate the best possible resolution for the customer. Regulatory requirements for response times vary by country, from a few days to a few weeks. In any case, response times must be as short as possible and DFS providers should provide regular updates to customers while the case is under review. Interim contacts and official responses should be documented and retained.

[41] Regulatory Framework for Mobile Payments Services in Nigeria (2009) https://www.cbn.gov.ng/OUT/CIRCULARS/BOD/2009/REGULATORY%20FRAMEWORK%20%20FOR%20MOBILE%20PAYMENTS%20SERVICES%20IN%20NIGERIA.PDF

Title of recommendation	Informing consumers of their right to complain and how to do so
Working Group	Consumer Experience and Protection
Theme	Recourse
Audience for recommendation	Regulators

Regulators should require that DFS providers inform consumers through multiple channels (e.g., print, SMS, etc.) of their right to complain and the process to complain, including all external complaints, filing options, and procedures in the event that the consumer is not satisfied with the outcome of the recourse process with the provider (e.g. regulators, ombudsman, industry mediator, consumer advocacy body, or the judiciary).

Regulators should require providers to use multiple channels to provide information on recourse, such as in written contracts, pre-contractual disclosures, electronic and print media, statements and receipts, and posted notices at branches and agents. GSMA's Code of Conduct for Mobile Money Providers[18] states that mobile money providers should, "inform customers of the existance of complaint policies and procedures." Some countries, such as Armenia[42], require staff to provide this information verbally, recognizing that illiterate customers will be unable to read written materials. Depending on the nature of the product, SMS may be an effective way to provide this notification.

Customers who interact primarily or exclusively with an agent may not know how to contact the DFS provider directly (e.g., at a call center or branch office) or feel confident doing so and thus first go to agents for assistance. According to CGAP[42] research, agents may not always be adequately trained or incentivized to serve in the dispute resolution role. Further, where the dispute or issue regards the agent itself, this can create serious problems. For this reason, signage, brochures, and other materials that provide clear instructions on contacting the DFS provider with a complaint or concern should be prominently displayed at the agent's location.

In situations where internal recourse fails, providers should specify how disputes can be resolved, as stated in Principle 7 of the GSMA's Code of Conduct[18]. For example, if the result of the investigation regarding the complaint is not in the customer's favor, the customer should be advised of available third-party alternative dispute resolution (ADR) options. Such alternatives may include an external ombudsman, mediator, consumer advocacy body, or judiciary. Regulators should do all in their authority to require providers to conduct internal recourse well, even though dealing with complaints can present a significant burden, particularly to low-capacity regulators.

In countries where an appeal to the court system is not financially or logistically feasible for low-income or illiterate customers, alternatives should be provided. The AFI recommends[12] that a consumer generally should not be expected to visit multiple third parties to seek redress when the DFS provider did not resolve a complaint to the customer's satisfaction; instead sufficient, appropriate options should be available so that a consumer only needs to visit one. Indonesia, for example, provides a single point of contact for customer care and referral to the correct governmental ombudsman. South Africa is also working to have a single contact for its multiple ombudsman schemes.

Banco Central do Brasil[43] requires financial institutions to disclose the existence of internal complaints mechanisms, and how to access them, at the distribution channels. Access to internal complaints must be freely

[42] Central Bank of the Republic of Armenia, Board Resolution 229-N (2009) https://www.cba.am/EN/laregulations/Regulation%208_05_eng.pdf
[43] Banco Central Do Brasil Resolucao No 4.433, DE 23 DE Julho De 2015 http://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/48509/Res_4433_v1_O.pdf

available through effective channels, including: a hotline that should be disclosed at branches; agents; on the provider's website; statements; receipts; agreements; advertisements; and any other documents given to the public.

Regulators may lack the resources to directly respond to all customer disputes, but in the absence of other third-party alternatives may need to take a more active role in providing assistance. As a general good practice, regulators should have visible and reliable procedures to advise customers on the proper steps needed to resolve concerns with regulated entities, including DFS providers. This could start by communicating contact information, such as a phone number and email address, for consumer inquiries in fliers posted in providers' offices, and through local media (e.g., newspaper, radio). Regulators could consider establishing a single phone number to call for DFS recourse. In some countries, consumers can call a single number and be auto-routed to the call center associated with the SIM card.

Title of recommendation	Multiple channels to complain
Working Group	Consumer Experience and Protection
Theme	Recourse
Audience for recommendation	Regulators

Regulators should require DFS providers to allow customers to submit complaints through a minimum of two channels (e.g., via agents, in branches, call center hotlines, SMS).

To promote ease of access, DFS providers should provide multiple means through which customers can submit complaints. There should be options to submit complaints through a channel similar to the delivery channel[40]; for example, a mobile phone-based service should have the means of lodging a complaint or inquiry via mobile phone. Providers that offer other services in addition to DFS, such as telecommunications, should ideally provide a dedicated team to deal with DFS complaints, as well as a dedicated hotline for DFS customers. Because technologies and product offerings mature and evolve, regulators should require that recourse channels evolve with them.

DFS providers should consider the unique needs of their customers when selecting the appropriate channels to offer. For example, walk-in complaints might be feasible for customers living and working in an urban area, but this would be less accessible for those in rural areas where the costs of travel and time away from work could be prohibitive. In markets where toll-free phone numbers are not available, recourse should be adapted so the cost is borne by the provider. For example, a customer could initiate a call, and then the provider could call back, thus incurring the cost.

Issues of trust may determine which channel a customer is most comfortable using, such as a local agent instead of the main office of the provider. While a minimum of two channels is recommended, DFS providers should also consider additional channels to facilitate different customer preferences, without creating so many levels or touchpoints that there is a risk that complaints will get lost.

Current rules on the number and types of required channels vary by country. Bangladesh Bank[14] requires providers to have a call center to receive and process disputes by telephone, SMS, IVR, and mail. Central Bank of Nigeria[41] requires providers to maintain a functional dispute and complaint resolution desk that is equipped to receive complaints through phone calls, e-mails, and personal visits or contact from the user.

Regulators should ensure that customers who are illiterate are not effectively barred from accessing recourse systems because DFS providers require the complaints to be filed in writing, consistent with the World Bank's Good Practices for Financial Consumer Protection[39]. The DFS provider's frontline staff or agents should be available to assist these customers in formulating and processing their complaints while ensuring that a written record is maintained.

The AFI recommends[12] that providers have a clearly defined process for escalating unresolved complaints. Good practice also suggests that the complaints function includes a method to escalate more serious or complicated issues. For example, CGAP reports[44] that some providers have specialized teams to address issues such as lost SIMs and forgotten personal identification numbers (PINs). Dedicated or specially-trained teams can also be used to address fraud and erroneous transactions, as resolution of both is particularly time-sensitive.

[44]Mazer, R., Garg, N., CGAP, *Recourse in Digital Financial Services* (2016) http://www.cgap.org/publications/recourse-digital-financial-services

Title of recommendation	Standardized & regular complaints reporting by DFS providers
Working Group	Consumer Experience and Protection
Theme	Recourse
Audience for recommendation	Regulators

Regulators should require standardized, electronic, and regular reports such as quarterly complaints reporting from DFS providers.

Regulatory review of complaints data can provide a check on the quantity and type of complaints providers receive, and on providers' compliance with the required response times and other standards. Through independent analysis, regulators may be able to spot issues and trends earlier. DFS providers should also make complaint data and supporting documentation available to regulators for review during onsite inspections.

Analysis of complaints data gives regulators a wealth of information on individual providers, new products, and the overall health of the industry. It can be used for market-monitoring, risk-based supervision, and identifying emerging risks and gaps requiring regulatory or other attention. The AFI notes[12] that as quantitative and qualitative data is collected and analyzed over time, regulators may be able to use this information to make necessary adjustments to consumer protection and market conduct regulations and guidelines.

General reporting requirements should include the type of complaint, segmented into category, such as product and delivery channel, to aid in analyzing: trends and problem areas; response times; final resolution (e.g.; in favor of customer or provider, sent to ADR or other third party); unresolved complaints; and the reason for delay. Regulators should require DFS providers to provide this information using a standard template to facilitate offsite review, statistical analysis, and comparison across providers and products. Where practicable, providers should upload this report electronically.

Complaint reporting should be done on a regular basis, both to the DFS providers' governance and to the regulator. Depending on the volume and trends, regulators may want to require complaint information every three or six months. The supervisor should have the authority to require providers to provide more frequent updates when circumstances necessitate. G20 High-Level Principles[13] on Financial Consumer Protection also recommend that aggregated complaints data and their resolution be made public, which would further enhance accountability and transparency. The Central Bank of Brazil, for example, publishes complaint statistics.

DFS providers should also be expected to assess their complaint data to identify and correct systemic issues. The Bank of Uganda[45] requires that a financial services provider have in place arrangements to ensure that, when handling complaints, it identifies and remedies any recurring or systemic problems by: (a) analyzing the causes of individual complaints in order to identify any failings in processes, products, or services; and (b) correcting any such failings.

[45] Bank of Uganda Financial Consumer Protection Guidelines (2011) https://www.bou.or.ug/bou/bou-downloads/Financial_Literacy/Guidelines/2011/Jun/Consumer_Protection_Guidelines_June_2011.pdf

Title of recommendation	Minimum standards for transaction verification
Working Group	Consumer Experience and Protection
Theme	Revocability
Audience for recommendation	Regulators

Regulators should establish minimum client protective measures which providers must put in place for transaction verification to help prevent mistaken transactions.

Research shows that poor user interfaces commonly cause transaction errors, and that these errors are difficult for customers to reverse or resolve. Errors occur when customers do not understand the menu, have difficulty navigating through multiple steps, and hurry to avoid being timed out. AFI also confirms that many customers' lack of technological literacy produces erroneous transactions such as sending money to the wrong account or paying the wrong bill. These errors are more common if menus do not display the recipient's name when the account or phone number is entered. Mystery shopping conducted by the ITU supports the finding that customers often have difficulty resolving mistakes. These problems can reduce customer trust and confidence in DFS and limit their usage due to fear of loss.

To reduce the risk of mistaken transactions, the BTCA Responsible Digital Payments Guidelines recommend that DFS interfaces be clear and easy-to-use. CGAP identifies DFS providers that have designed interfaces and processes to reduce keystroke errors by incorporating triggers to help customers confirm they are sending money where they intended, such as a "check digit" or integration with address book to display the recipient's name before sending. DBBL in Bangladesh creates a customer's account number by adding a check digit to the end of the mobile number. Airtel Money in Uganda displays the recipient's name when the customer inputs the phone number.

To protect consumers and improve the reliability of DFS services, regulators should require providers to have minimum standards for transaction verification built into their product design. The BTCA guidelines recommend that a client receive proof of each transaction and have ready access to clear and understandable transaction and account records. These records should ideally be provided digitally and in a form the client can keep or access, such as a digital transaction history.

The GSMA Code of Conduct states that, "where feasible, providers shall only authorize customer transactions in which the debiting and crediting of mobile money accounts is processed in real time." This requirement for real time transactions could also facilitate instant confirmation of whether the transaction went to the correct recipient.

Title of recommendation	Specialized staff for transaction errors
Working Group/Work Stream	Consumer Experience and Protection
Theme	Revocability
Audience for recommendation	DFS Providers

Customers calling customer care to report a mistaken transaction should be directed to a specially trained team at the call center to speed resolution (e.g., before recipient of an erroneous transaction withdraws the funds).

Research shows[10] that sending transfers to the incorrect recipient is one of the most common problems experienced by DFS users. Resolving incorrect transactions is also time sensitive, as in many markets, once the incorrect recipient has withdrawn the money, the sender no longer has recourse to retrieve the funds. For these reasons, providers' customer care should prioritize resolving incorrect transfers.

In order to ensure rapid responses, providers should have escalation procedures and a specially trained call center team where calls related to incorrect transactions are routed. This team should be trained in the providers' policies and procedures for resolution of reported incorrect transactions and be able to act quickly to resolve the transaction before the incorrect recipient has a chance to withdraw the funds.

Providers should also ensure that customers are well-informed about how to reach customer care. The Better Than Cash Alliance[46] guidelines recommend that customers be given contact details for a 24-hour hotline to notify the DFS provider about a mistaken or unauthorized transaction.

[46] Better Than Cash Alliance, *Responsible Digital Payments Guidelines* (2016) http://www.uncdf.org/sites/default/files/Documents/btca-responsible_digital_payments_guidelines_and_background.pdf

Title of recommendation	Payments should generally be considered irrevocable with exceptions as specified
Working Group	Consumer Experience and Protection
Theme	Revocability
Audience for recommendation	Regulators

Regulators should ideally establish that digital payments are irrevocable unless the receiving party consents to the return of the money. However, regulators should recognize that different provisions may be needed depending on the market context (e.g. whether a validation protocol allows senders to confirm the recipient prior to sending a transfer), and may be needed for different use cases (e.g. rights and responsibilities may be different in P2P payments than in merchant payments).

The ability to reverse an erroneous transaction is an important consumer protection, but it also opens the door to potential fraud. For example, incorrect transactions are common, particularly among low-income DFS customers, and thus protections are needed so these customers do not lose money. At the same time, fraud is possible when, for example, a customer claims that a transfer to a merchant was sent to the incorrect number when in fact it was a legitimate purchase. The customer could thus fraudulently retain the purchased good and retrieve the payment.

Because of the potential for fraud, regulators should ideally require DFS payments to be irrevocable unless the receiving party consents to the return of the money. However, in markets where safeguards against incorrect transactions are insufficient, such as where a mechanism for senders to verify recipients before confirming a transaction is absent, alternatives may be necessary.

The GSMA Code of Conduct for Mobile Money Providers[18]states that mobile money providers shall develop specific policies for handling reversals.

Different regulations and rules may be needed for P2P transfers and merchant payments. For P2P transfers, the transfer by the sending consumer should be irrevocable without the consent of the recipient in cases where the payment system used supports a validation or verification protocol. If the payment system used does not support a validation protocol, transfers may be revocable by the sending party within a specified time limit. In this case, DFS providers may be allowed to charge the consumer a small fee for the revocation. In either case, a message or protocol to digitally request an error correction should be supported; this would enable a return of the sending customer's funds by consent of the receiving customer.

In general, consumer-to-merchant transactions should be irrevocable without consent of the receiving merchant. Fraud may be more likely in reversing payments to merchants, and the sums are often larger presenting larger possible gains from fraud. Allowing reversals of payments to merchants could also harm the development of a digital ecosystem as merchants may be hesitant to accept digital payments if they fear they could be reversed.

DFS providers should be encouraged to create mechanisms for consumers to dispute transactions with fraudulent merchants, and in some specific instances support revocation of funds. For example, PayPal[47] describes in detail the situations, time frames, and restrictions on reversing a transaction by a customer.

[47] PayPal User Agreement (2016) https://www.paypal.com/webapps/mpp/ua/useragreement-full?locale.x=en_GB

Title of recommendation	Consumers should be informed of deposit insurance scheme coverage for DFS
Working Group	Consumer Experience and Protection
Theme	Protection of Funds
Audience for recommendation	Regulators

Regulators should require DFS providers to inform consumers whether mobile money and other digital stored-value products are covered by the deposit insurance system or not and, if so, under what conditions (e.g. the maximum amount covered per account or per customer). Public awareness initiatives should be carried out to raise consumer understanding of the deposit insurance system and its role in protecting DFS customer funds.

Disclosure of key DFS terms and conditions is important to promote consumer confidence in DFS products and consumer trust in DFS providers. This is especially true when the DFS product allows customers to digital store-value in small amounts. If a deposit insurance system is already in place, consumers should be informed on whether such digital stored-value product is covered by the deposit insurance system or not, before they make a purchasing decision.

Whatever approach is adopted, public awareness programs is important to explain to consumers what digital stored-value products are, whether they are covered by deposit insurance and, if so, under what conditions they are covered (e.g. the maximum amount covered per account or per customer). These programs would complement requirements on disclosure of information on deposit insurance for digital stored-value products, preferably in standardized format and language. This information would be useful for consumers to access through all relevant channels at the pre-selling stage (e.g. advertising, marketing, and informational materials; consumer agreements; USSD menus). As the coverage level may be updated regularly, consumers would benefit from easy access to check the coverage level during the life of the DFS product. In the Philippines, e-money issuers disclose on their websites that these products are not covered by deposit insurance. In Colombia and Mexico, where the direct approach is applied, disclosure on deposit insurance coverage is required.

The International Association of Deposit Insurers (IADI) has public awareness as one of its Core Principles for Effective Deposit Insurance. IADI indicates that "…public awareness campaigns should adequately address what types of deposits and money transfer vehicles are covered by deposit insurance and what types are not, in order to minimize potential confusion among small-scale depositors and financial service providers alike." The Basel Committee on Banking Supervision[48] in its latest financial inclusion guidance also recommends that a list of financial institutions be publicly available, indicating for each institution: "(i) the permitted activities; (ii) the supervisory authority; and (iii) whether deposit insurance is available to the deposits placed with them – and, if so, from whom. Each such institution should be required to disclose its status prominently – both at branches and through agents or other third parties acting on its behalf."

[48] The Basel Committee on Banking Supervision, *Guidance on the Application of the Core Principles for Effective Banking Supervision to the Regulation and Supervision of Institutions Relevant to Financial Inclusion* (2016) http://www.bis.org/bcbs/publ/d383.pdf

Title of recommendation	Adopt clear approach to deposit insurance treatment of DFS stored-value
Working Group	Consumer Experience and Protection
Theme	Protection of Funds
Audience for recommendation	Regulators

Regulators should address legal and customer uncertainties on whether a DFS is or is not considered a deposit and, taking into account specific country legal and market conditions, adopt a clear approach to the deposit insurance treatment of digital stored-value products (e.g. exclusion, direct coverage, or pass-through coverage). If digital stored-value products are excluded from deposit insurance coverage, then alternative mechanisms to protect customer funds should be in place.

The emergence of a wide range of DFS (e.g. electronic wallets, prepaid debit or virtual cards, online transaction accounts) has made it harder for authorities, providers, and consumers to clearly identify what products are legally considered deposits. This issue impacts which products can be covered by deposit insurance and which providers need to be licensed or prudentially regulated, which in turn could affect access to central bank facilities, among other regulatory aspects. Regulators thus need to give certainty to all actors and explicitly indicate whether a new DFS is considered a deposit and, subsequently, the deposit insurance treatment it will receive.

CGAP[49] has observed that countries with deposit insurance have adopted one of three approaches to digital stored-value products: (i) the **exclusion approach**, whereby such products are explicitly excluded from deposit insurance coverage, although other measures to protect customers' stored value are adopted; (ii) the **direct approach**, whereby such products are directly insured by a deposit insurer and their providers must be or must become members of the deposit insurance system; and (iii) the **pass-through approach**, whereby deposit insurance coverage "passes through" a custodial account at an institution that is a deposit insurance member which holds customer funds from stored-value products, to the individual customer of the DFS provider (although this is not a deposit insurance member).

Countries applying the exclusion approach (e.g., Peru, the Philippines) typically consider digital stored-value products to be primarily instruments of temporary value storage to make payments or transfers – although here customer funds are still protectable from some risks associated with the failure of their provider, for example, by requiring that the digital float be held in a custodial account. Countries adopting the direct approach (e.g. Colombia, Mexico) emphasize the need to ensure that customers only have access to digital stored-value products offered in a safe and sound manner by supervised financial institutions. The pass-through approach is being adopted in countries where digital stored-value products may be offered by nonfinancial firms, such as MNOs and technology companies (e.g. Kenya, Nigeria). GSMA[50] and the Committee on Payments and Market Infrastructures[51] (CPMI) have highlighted the benefits of this approach. It is worth noting that in countries where the legal and regulatory framework has been adjusted to accommodate the pass-through

[49] Izaguirre, Juan Carlos, Lyman, Timothy, McGuire, Claire, Grace, Dave. CGAP, Deposit Insurance and Digital Financial Inclusion (2016) http://www.cgap.org/publications/deposit-insurance-and-digital-financial-inclusion

[50] Grossman, Jeremiah, GSMA, *Safeguarding Mobile Money: How providers and regulators can ensure that customer funds are protected* (2016) http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/01/2016_GSMA_Safeguarding-Mobile-Money_How-providers-and-regulators-can-ensure-that-customer-funds-are-protected.pdf

[51] World Bank Group, Committee on Payments and Market Infrastructures, Payment Aspects of Financial Inclusion (2016) http://www.bis.org/cpmi/publ/d144.pdf

approach, practical challenges are arising in its implementation. International Association of Deposit Insurers (IADI)[52] has signaled this approach as an important area for further research.

The feasibility and effectiveness of each approach, and how it may need to be tailored in a given country, will depend on the legal, regulatory and supervisory framework, the characteristics of the deposit insurance system, and the specific types of DFS providers, products, and associated risks. Regardless of the approach taken, it is important for regulators to make a conscious policy decision on the deposit insurance approach to digital stored-value products so as to address legal uncertainties and improve the protection of digital customer funds.

[52] International Association of Deposit Insurers, Financial Inclusion and Deposit Insurance (2013) http://www.iadi.org/en/assets/File/Papers/Approved%20Research%20-%20Discussion%20Papers/2013-06_Financial_Inclusion_and_Deposit_Insurance_publication-clean.pdf

Title of recommendation	Implementation of measures to safeguard funds
Working Group	Consumer Experience and Protection
Theme	Protection of Funds
Audience for recommendation	Regulators

Regulators should require DFS providers to implement measures to safeguard customer funds, such as full liquidity backing, fund isolation, and ring-fencing.

Regardless of the existence of deposit insurance protection for digital stored-value products, regulators should require DFS providers to implement specific measures to safeguard customer funds, so as to reduce the risk of consumers losing their funds in the event of insolvency of a provider of digital stored-value products. These mechanisms are especially important in countries that apply the exclusion approach or the pass-through approach, when some DFS providers are not members of the deposit insurance system.

The most common safeguarding mechanism is the requirement for DFS providers to hold funds equivalent to all digital stored-value in circulation in liquid and safe assets, including government securities or deposits at several prudentially regulated institutions, especially when digital stored-value exceeds a certain threshold (e.g. Colombia, Philippines). This requirement may still be insufficient to guarantee that customers will receive the total amount they kept in digital stored-value products, as customers may only have unsecured claims on the DFS providers' assets. For this reason, another important safeguarding mechanism is to require DFS providers to isolate or separate customer funds from other assets, so that they can only be used for the customer's benefit and not for business purposes. This is typically done by placing funds in a trust or a custodial account (e.g. Kenya, Nigeria), particularly in common-law countries where the legal concept of a trust exists. In civil-law countries, fiduciary contracts are used for similar fund isolation purposes. Regulators in civil-law countries may require additional ring-fencing provisions to ensure that customer funds are protected from creditor claims in the case of insolvency of the DFS provider, the trustee, or the custodian holding such funds (e.g. Paraguay and Peru).

The CPMI/World Bank's report Payment Aspects of Financial Inclusion highlights the aforementioned safeguarding mechanisms among the key aspects of the payment services' legal and regulatory framework that are critical enablers of financial inclusion. The GSMA Code of Conduct for Mobile Money Providers[18] requires mobile money providers to safeguard customer funds against risk of loss (Principle 1). The BTCA Responsible Digital Payments Guidelines[53] also indicates the need to safeguard the float for client funds held in digital payment accounts (Guideline 2).

[53] Better Than Cash Alliance, Responsible Digital Payments Guidelines (2016) https://www.betterthancash.org/tools-research/case-studies/responsible-digital-payments-guidelines

Title of recommendation	Interest payments for e-money balances
Working Group	Consumer Experience and Protection
Theme	Payment and use of interest on customer funds
Audience for recommendation	Regulators and policymakers

Policymakers should consider allowing the payment of interest or returns on e-money balances to consumers, especially when they are required to be placed in an interest-earning trust or custodial account at a financial institution. Policymakers should assess the pros and cons of this decision, taking into account specific legal, market, and operational aspects, and monitor the impact on the market following the authorization of payment of returns.

The payment of interest or returns on e-money balances to consumers may create further incentives for customers to: open, use, and store value in such products; make it more appealing to unserved or underserved customers[54]; create additional competition among DFS providers; and allow for distribution of interest accrued on a trust or custodial account to the ultimate beneficiaries of the funds being held for the customers. On the other hand, payment of interest may create further confusion for consumers where e-money is not considered a deposit, as consumers may not understand the difference between interest-bearing e-money accounts and deposits (and why the former are but the latter are *not* covered by deposit insurance); also DFS providers may engage in aggressive price competition or deceptive advertising regarding higher returns, and the transmission of interest to beneficiaries may be operationally challenging.

The importance of the arguments in favor or against the payment of interest or returns will differ among countries depending on their specific legal and regulatory framework (e.g., whether e-money is considered a deposit or not), market structures (e.g., competition and financial inclusion levels), operational aspects (e.g., existence of trust or custodial accounts or fiduciary arrangements). In the past two years, Tanzania and Ghana[55] have allowed the payment of returns (or rather the sharing of profits in Tanzania), whereas Peru and the Philippines have clearly stated that no such payment is allowed. Policymakers and regulators should carefully assess the advantages and disadvantages of this decision, make an informed decision, and monitor the market to see either the effects of a positive decision or the challenges or opportunities of a negative decision.

[54] World Economic Forum, The Mobile Financial Services Development Report (2011) http://www3.weforum.org/docs/WEF_MFSD_Report_2011.pdf

[55] McKay, C. CGAP, Interest Payments on Mobile Wallets: Bank of Tanzania's Approach (2016) http://www.cgap.org/blog/interest-payments-mobile-wallets-bank-tanzania%E2%80%99s-approach

Title of recommendation	Identifying data privacy and protection issues
Working Group/Work Stream	Consumer Experience and Protection
Theme	Data protection
Audience for recommendation	Regulators

Regulators should seek to understand data privacy and protection issues of consumer data and personal information associated with DFS products and services in their markets, through regular consultations with providers, consumer groups, and other stakeholders. Regulators should identify provisions in their existing legal and regulatory frameworks relevant to data privacy and protection for DFS, identify gaps, and develop an action plan to progressively strengthen data privacy and protection and minimize adverse consequences for consumers.

With the rapid growth of DFS, DFS providers are collecting an unprecedented quantity of personal information from and about consumers, including transaction details and amounts, payers/payees, and the parties' locations. Providers are beginning to utilize this data to offer products and services, such as by using algorithms to determine a customer's credit worthiness.

The growing collection and use of data in DFS makes it critical for regulators to better understand the related data privacy and protection issues in their market. To do this, they should consult with DFS providers under their supervision as well as with representatives of industry, consumers, and other DFS stakeholders. They should seek to understand the ways data is being used, current provider policies and practices with regards to data, and the potential risk and harm that could come from poor data practices.

Regulators should also seek to understand the attitudes and preferences of consumers in their jurisdictions. For example, research shows consumers generally view[56] their financial information as being sensitive and have concerns about how their personal information will be used and shared, fearing it could expose them to identity theft, embarrassment, and tax or criminal liability. In addition, consumer attitudes differ by country. ITU research showed, for example, that Ghanaians and Filipinos are much less willing then Tanzanians are to share their data to access a loan.

As a first step towards regulating and enforcing good data privacy and protection practices, regulators should survey relevant provisions or authorities in their existing laws and regulations. Many countries that - do not have a central data authority or comprehensive data protection law - do have data-relevant provisions dispersed throughout other laws or regulations, such as in bank secrecy and credit reporting laws. For instance, Tanzania's Banking Act[57] prohibits unauthorized disclosure of transaction information and Kenya's Central Bank credit reference bureau regulations[58] require that credit bureaus protect the confidentiality of customer data. Regulators can use this review to identify which regulatory tools are available and where there are gaps in their authority.

Because DFS touch on many regulatory areas including telecommunications, financial services, competition, consumer protection, and data protection, country regulators should also consult with each other to develop a coordinated regulatory approach. As an example, in Tanzania, both the banking laws (as noted above) and the telecommunications regulations restrict the disclosure of customer information. Because DFS may occur over

[56] Costa, A., Deb, A., Kubzansky, M., *Big Data, Small Credit, The Digital Revolution and Its Impact on Emerging Market Consumers* (2015) https://www.omidyar.com/sites/default/files/file_archive/insights/Big%20Data,%20Small%20Credit%20Report%202015/BDSC_Digital%20Final_RV.pdf

[57] Act Supplement, The Bank of Tanzania Act, 2006, http://www.bot.go.tz/AboutBOT/BOTAct2006.pdf

[58] Special Issue, Kenya Gazette Supplement No. 3 (2014) http://www.ciskenya.co.ke/sites/default/files/The%20Credit%20Reference%20Bureau%20Regulations%202013.pdf

mobile devices that connect to financial institutions, the responsibility for providers' handling of customer information could implicate both authorities, making it all the more important that agencies coordinate their efforts.

Finally, based on these efforts, regulators and policymakers (to the extent legislative action is needed) can move progressively to develop a plan to ensure that DFS consumers have reasonable data protection. This can be accomplished in several ways, including calls for new legislation, issuance of new regulations, interpretations of law and regulatory guidance, and through encouraging voluntary industry efforts. Some jurisdictions are adopting comprehensive data protection laws and establishing commissions to implement them, such as Ghana; others, such as Uganda, are considering similar moves. These efforts could be undertaken in conjunction with industry self-regulatory initiatives and consumer education, so there is a balanced approach that benefits all DFS participants.

Title of recommendation	Informed consent on data collection and use
Working Group	Consumer Experience and Protection
Theme	Data protection
Audience for recommendation	Regulators

Regulators should require DFS providers to provide clear, conspicuous, and understandable informed consent with all DFS, so that customers appreciate what data is being collected; how it may be used; whether it will be disclosed to third parties and, if so, which parties and for which purposes; how long it will be retained; whether it will be disclosed for legal or public interest reasons (such as to the government for criminal or tax related investigations), and what options customers have if they believe their data has been improperly accessed or used. Regulators should also require DFS providers to obtain specific consent for each type of data use or sharing including when such information is being sold or shared with a third party for a purpose unrelated to the original transaction.

There is a growing international recognition of the importance of data protection as a component of DFS and mobile transactions. For instance, GSMA has developed a set of mobile privacy principles[59] that promote consumer privacy in the mobile ecosystem. On the governmental level, the European Union has recently adopted a General Data Protection Regulation that emphasizes key components of data protection, making them generally applicable across industry sectors. One of the BTCA's Responsible Digital Payments Guidelines[46] calls for the protection of clients' digital data. The Payment Aspects of Financial Inclusion (PAFI) states that a "lack of clarity regarding what can be disclosed, and to whom, may deter the use of a payment service by some potential customers." The United Nations Guidelines for Consumer Protection[60] calls for the "protection of consumer privacy and the global free flow of information."

In addition, new research commissioned by the ITU shows that half of DFS customers in Ghana, Tanzania, and the Philippines think DFS providers or agents could use their personal information to harm them. In the same study, more than half in each country expressed concern about advertisers using their data.

In keeping with emerging data protection principles, there are several steps regulators should take to protect DFS consumers. First, consumers should be given clear, conspicuous, and understandable disclosures so they understand what data is being collected from them, how that data will be used, what choices they have regarding such uses, how long their information will be retained, and whether their information will be disclosed to third parties. This information could help empower those consumers to make informed choices about the handling of their personal information. Given the display limitations on devices often used to access DFS, and low literacy levels of some users, this may be challenging, but research has shown[61] that simple explanations and informational brochures can help customers understand data use. Regulators and providers can use consumer research to test different disclosure options can help identify the most effective mechanisms.

In addition, it is important for consumers to be informed about certain provider policies and practices, including the policies for selling data to third parties. One way to reduce risk and empower customers is to require that providers obtain separate consent for each instance of data sharing or selling, allowing the customer to decide when the benefits of sharing personal data will outweigh the risks. Consumers should also be informed of provider policies for sharing data with government entities, such as law enforcement and tax authorities. And,

[59] GSMA Privacy Principles, *Promoting Consumer Privacy in the Mobile Ecosystem* (2016) http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/GSMA2016_Guidelines_Mobile_Privacy_Principles.pdf
[60] United Nations Guidelines for Consumer Protection (2016) http://unctad.org/en/PublicationsLibrary/ditccplpmisc2016d1_en.pdf
[61] Mazer, R., Carta, J., Kaffenberger, M., Informed Consent: How do we Make it Work for Mobile Credit Scoring? (2014) http://www.cgap.org/sites/default/files/Working-Paper-Informed-Consent-in-Mobile-Credit-Scoring-Aug-2014.pdf

regulators should require that providers inform customers of their ability to access, dispute, and have corrections made to their personal information, as well as redress options available, including administrative or judicial remedies if a customer has suffered harm or providers fail to comply with legal requirements. Finally, regulators should review contracts and terms and conditions to evaluate whether the data protection provisions are clear, balanced, and in compliance with regulation.

Title of recommendation	Further data protection provisions for consideration
Working Group	Consumer Experience and Protection
Theme	Data protection
Audience for recommendation	Regulators

Regulators may also consider the following provisions to protect consumer data privacy: Require that customers have the right and the ability to access, verify, and correct their data; require DFS providers have adequate security provisions in place and promptly notify customers in the event of breaches or other security issues affecting customers; establish clear DFS provider liabilities in cases of data mishandling, data misuse, or failure to adopt reasonable security measures for data the provider holds; consider mandating retention limitations, whereby data may only be retained for a specified time period after its collection or use, after which it will be properly destroyed; and take steps to ensure customers have the right and ability to port their data from one provider to another and that data is interoperable across providers and platforms to make this practical.

A key area of consumer concern is data security. Two recent episodes highlight the problem. In India, between three and six million ATM cards have been hacked[62], exposing financial institutions to millions of dollars in potential losses and undermining consumer confidence in the payment system. It has also been revealed that half a billion Yahoo! email users worldwide were affected by a serious data breach[63]. While many of them reasonably expected that their email service provider would have sufficient data security measures in place to prevent this from happening, or would have at least let them know once the breach had been discovered so they could take steps to limit the damage, neither was the case. In 2015, a study was conducted by University of Florida[64] that found serious security shortcomings with a number of mobile money apps, leading the authors to recommend "that dramatic improvements to the security of branchless banking applications are imperative to protect the mission of these systems." Accordingly, in order to reinforce confidence in DFS, it would be appropriate for regulators to mandate DFS providers have adequate security provisions in place and, when a breach is discovered, promptly notify affected customers who could then take steps to protect themselves. Imposing clear DFS provider liabilities in cases of data mishandling and misuse, or failure to adopt reasonable security measures would create important compliance incentives.

Another important protection that can benefit providers and consumers is limiting how long customer information can be retained, requiring data be properly destroyed after a specified time period following collection or use. If data is not on hand, it cannot be compromised, thus protecting consumers from the consequences of a security breach and providers as well, since breaches can result in reputational harm as well as liability and associated legal expenses.

Regulators can take other data protection measures as well, such as Kenya's[64], credit-reporting laws which give consumers the right to access their information, dispute it if incorrect or incomplete, and have it corrected. Providing access and correction rights to DFS consumers benefits everyone. Inaccurate negative information in DFS provider files can result in denials of credit to creditworthy consumers. Letting those consumers see their information and have a chance to correct it can result in more credit approvals and increased file accuracy.

[62] Scroll.in, ATM security breach: Economic affairs secretary asks people to not panic, promises swift action, Updated Jan. 3, 2017 http://scroll.in/latest/819702/atm-security-breach-economic-affairs-scretary-asks-people-to-not-panic-promises-swift-action
[63] Lord, B.. Yahoo! An Important Message About Yahoo User Security (2016) https://yahoo.tumblr.com/post/150781911849/an-important-message-about-yahoo-user-security
[64] Reaves, B., Scaife, N., Bates, A., Traynor, P, Butler, K. R.B. University of Florida, Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World (2015) http://www.cise.ufl.edu/~butler/pubs/sec15a.pdf

Finally, customers could be given the right and ability to port their data from one provider to another. Customer data would need to be maintained in a form that is interoperable across providers and platforms in order to make this practical. Portability is an important tool for promoting competition among providers and easing the barriers to entry for new providers, because providers will know that consumers can take their business to other firms easily and at any time. Vigorous DFS competition can result in lower prices, expanded geographical coverage, and better and more services.

Title of recommendation	Harmonize market conduct rules for credit products
Working Group	Consumer Experience and Protection
Theme	Digital credit
Audience for recommendation	Regulators

Regulators should take steps to identify gaps and establish adequate market conduct and consumer protection rules for digital credit products with the goal of harmonizing market conduct rules for all comparable credit offerings, regardless of the type or location of the provider, or the channel/method by which the product is sold.

Digital channels have the potential to fill a range of unmet credit needs of consumers and very small businesses. These small-value, short-term (typically one-to-three month), and often unsecured loans are "instant, automated, and remote" as described by CGAP[65]. Product and delivery innovations target a wide range of customers by linking to mobile money accounts and bank accounts, and utilize a range of communication channels such as social media, SMS, and the internet. Loans may be offered directly by a lender or indirectly through a merchant acquirer/distributor or other value chain actor, and are serviced entirely via mobile or online channels rather than through branches or physical premises.

Many digital credit customers are new to formal finance and lack conventional credit histories. Digital lenders commonly assess potential borrowers and manage risks using scores based on alternative data such as call detail records, mobile payments transactions, and social network profiles, instead of or in addition to data available through more conventional means such as credit bureaus. Credit scoring allows for instant decision-making with limited or no in person interactions which can allow digital credit to reach scale relatively quickly compared to traditional lending programs.

Digital credit models involve multiple participants subject to varying degrees of oversight, including banks, nonbank credit providers, MNOs, EMIs, payment services providers, and peer-to-peer platforms. Inconsistent oversight elevates risks to customers and can lead to an un-level playing field. Typically, disclosure, underwriting, data handling, and reporting requirements, for example, are more rigorous for regulated lenders. In addition, consumer protection rules may not adequately address issues raised by digital channels. For example, disclosure may be challenged by the use of a small screen, menu-driven process, as well as lack of consumer digital and financial literacy. Scoring algorithms may not accurately predict ability to repay, unfairly profile or discriminate, or lack adequate informed consent by the consumer for data collection and usage.

Regulators should harmonize market conduct rules and oversight for all comparable credit offerings, regardless of the provider and channel. This is in line with the G20 High-Level Principles[13] on Financial Consumer Protection emphasizing the need for cooperation by regulators of different segments of the financial and non-financial (e.g., telecommunications) sectors. This will help to avoid regulatory gaps and inferior treatment for borrowers taking loans via digital versus non-digital means. The Competition Authority of Kenya, for example, has established common transparency and price disclosure requirements for all DFS providers[66] including digital lenders not subject to regulation by financial authorities. AFI[67] describes the case in Zambia, where non-bank DFS providers are not allowed to extend credit but can partner with an institution licensed to provide

[65] CGAP, *An Introduction to Digital Credit: Resources to Plan a Deployment* (2016) http://www.slideshare.net/CGAP/an-introduction-to-digital-credit-resources-to-plan-a-deployment

[66] Mazer, R., CGAP, *Kenya Ends Hidden Costs for Digital Financial Services* (2016) http://www.cgap.org/blog/kenya-ends-hidden-costs-digital-financial-services

[67] Digitally Delivered Credit Policy Guidance Note and Results from Regulators Survey, Consumer Empowerment and Market Conduct (CEMC) Working Group (2015) http://www.afi-global.org/sites/default/files/publications/guidelinenote-17_cemc_digitally_delivered.pdf

credit. In such cases, the licensed institution will be responsible for the management and extension of credit while the DFS provider provides the delivery channel.

AFI[67] recommends that potential gaps in recourse mechanisms also be reviewed to ensure ease of access to customers through both digital and non-digital channels, regardless of whether the provider is subject to financial sector regulation. CGAP[68] reports that partnerships in digital credit and other sophisticated non-payment products may require new approaches to complaints handling. Kenya's M-Shwari has a dedicated complaints team within MNO Safaricom's call center to respond to inquiries, resolve issues, encourage timely repayment, and support delinquent borrowers.

[68] Mazer, R., Fiorillo, A., Digital Credit: Consumer Protection for M-Shwari and M-Pawa Users (2015) http://www.cgap.org/blog/digital-credit-consumer-protection-m-shwari-and-m-pawa-users

Title of recommendation	Transparent disclosure of digital credit costs using standardized definitions
Working Group	Consumer Experience and Protection
Theme	Digital credit
Audience for recommendation	Regulators

Regulators should establish standard definitions for the cost of digital credit including all bundled services (and including all interest, credit-related fees, and fees for bundled products), and require clear, conspicuous, and understandable disclosure of the cost, as well as financial and other consequences of early, partial, late, or non-repayment of the loan.

Terms and conditions for DFS, especially more complex services such as credit, are often poorly disclosed according to CGAP[69] research. Lack of transparency standards may result in disclosures and agreements that are difficult to comprehend, provided piecemeal, or received at the wrong time to be useful. Conversely, establishing and enforcing a consistent regime for disclosing the cost of products could help to improve the quality of customer decisions[70] and may promote comparison shopping. Competition may in turn lead to overall reductions in costs[71].

The World Bank's Good Practices for Financial Consumer Protection[39] specify basic transparency standards for all types of products, such as being as concise as possible, using plain language and easily understandable terms, and giving prominence to key features so customers are more likely to notice and seek clarification with the staff or agent if needed. The Good Practices also state that regulations should allow providers to use digital means of providing terms and conditions, and establish the timing of disclosures, especially during the sales and the pre-signing periods. Going a step further, it is important to specify that all digital products provide the full cost of the loan, including interest, fees, and bundled services, prior to the execution of the transaction on the digital delivery channel, as was recently mandated by the Competition Authority of Kenya[66].

Digital credit creates unique transparency challenges. Information is provided mainly on a small screen with limited room for text. There are few opportunities for customers to ask questions in person, and some information may only be posted online even if the customer is using a mobile handset to access the product. For example, M-Shwari in Kenya, which offers instant access to credit without a previous banking history, provides terms and conditions through a web link, even though many users lack access to the internet. In practice[68], many M-Shwari applicants skip this pre-purchase step to avoid the hassle, and may not know the cost or repayment conditions of the loan. With a 7.5 per cent facilitation fee for a 30-day loan, this can be an expensive mistake.

Standard definitions should be used to communicate the cost of digital credit. Regulators should design the calculation and disclosure using a consistent metric that reflects the total cost, so that digital borrowers do not pay more than the amount advertised and understand the full cost of the product. The standardized method for determining total cost should include all interest and credit-related fees. Disclosing fees and requirements for tied and bundled products, such as insurance or deposit accounts, may be especially problematic due to the limited space available and increased complexity of the offer.

[69] CGAP *The Proliferation of Digital Credit Deployments* (2016) https://www.cgap.org/sites/default/files/Brief-Proliferation-of-Digital-Credit-Deployments-Mar-2016_1.pdf

[70] Mazer, R., *USSD Access: A Gateway and Barrier to Effective Competition* (2015) http://www.cgap.org/blog/ussd-access-gateway-and-barrier-effective-competition

[71] Mazer, R., Rowan, P., Competition in Mobile Financial Services: Lessons from Kenya & Tanzania (2016) http://www.cgap.org/publications/competition-mobile-financial-services-lessons-kenya-tanzania

AFI[67] cites a need for comprehensive disclosure of costs to allow for comparison between digital and non-digital credit options, which may be difficult as many digital products are priced in terms of a periodic (e.g., weekly, monthly) "facilitation fee" or other term rather than interest. Even when an interest rate is disclosed, the very short tenor may obscure the long-term cost if the loan is renewed repeatedly. This makes it important for markets to have standardized methods for calculation of cost of credit, such as the APR or effective interest rate (EIR) methods employed in many jurisdictions for conventional credit. However, policymakers should also consider whether APR or EIR is the most salient way to communicate costs of short-term credit to consumers, and, if not, be open to additional methods for disclosing costs, such as the nominal value of all charges.

Another common feature is for a digital loan to be rolled over if not fully repaid at maturity, with assessment of an additional fee on the outstanding balance. Disclosures should communicate rights and responsibilities related to early, partial, late, or non-payment of a loan. Regulators may want to discuss standards or limits on the number of roll overs to avoid turning a short-term loan into a long-term debt that becomes larger with every renewal.

The disclosure regimen should be complemented by financial education and awareness efforts. Research by TechnoServe[72] on the experiences of farmers using the M-Pawa digital savings and credit product in Tanzania shows that customers who are inexperienced users of financial services find M-Pawa features, such as the interest rate and loan limits, difficult to understand despite various methods to communicate product terms, such as radio, billboards, SMS messages, and training sessions. At the same time, TechnoServe, in partnership with Vodacom, CGAP, and Arifu, developed an SMS-based educational program[73] for these same farmers to help increase understanding. This case highlights how providers can use consumer testing and innovation in digital communication channels to help consumers better understand, engage with, and use digital credit products.

[72] Zhou, A.. CGAP, *M-Pawa 1 Year on: Mobile Banking Perceptions, Use in Tanzania* (2015) http://www.cgap.org/blog/m-pawa-1-year-mobile-banking-perceptions-use-tanzania

[73] Mazer, R., CGAP*, Interactive SMS Drives Digital Savings and Borrowing in Tanzani*a (2016) http://www.cgap.org/blog/interactive-sms-drives-digital-savings-and-borrowing-tanzania

Title of recommendation	Further digital credit provisions for consideration
Working Group	Consumer Experience and Protection
Theme	Digital credit
Audience for recommendation	Regulators

Regulators may also consider additional rules that strengthen consumer protections and promote responsible development of the digital credit market such as: Requiring that auto-deduct be opt-in (and does not entitle the provider to set-offs) and that borrowers should be notified each time the provider deducts from, or attempts to deduct from the account; or restricting the use of customer data that is provided to access a loan for purposes of marketing or unsolicited loan offers; without obtaining explicit consent from the customer.

As providers and regulators gain experience in benefits and risks of digital credit, new issues will continue to emerge. The following are examples of trending consumer protection concerns regulators may also want to consider, if relevant to their country context.

For digital credit that is tied to a deposit or mobile money account, there are varying approaches by providers for the use of auto-deductions from a customer's related account to make payments on a loan. AFI[67] reports that both Timiza and M-Pawa in Tanzania have the ability to deduct the amount of a late payment from a mobile money or savings account charge, in addition to charging late fees. In Kenya, however, CGAP[74] reports that in the case of non-payment of an M-Shwari loan, none of the airtime or M-PESA balance is transferred to the loan without the customer's consent. To strengthen consumer protection and promote responsible development of digital credit markets, regulators could consider enhancing rules to require customers to opt-in to automatic deduction programs and governing whether providers are entitled to set-offs for delinquent payments.

Customer data is routinely obtained in digital credit for uses such as credit scoring. Clear and conspicuous informed consent should exist related to data privacy for all DFS, including digital credit. Thus, another consumer protection issue to consider is how this data is used for other purposes, such as in subsequent marketing and unsolicited loan offers.

A related emerging risk that regulators may want to consider is push marketing tactics through unsolicited SMS messages[75]. In digital, as well as non-digital lending, aggressive sales tactics, whether in person or via digital marketing, may lead customers to overborrow. Subsequent defaults can damage a customer's credit history. In Kenya, for example, borrowers of digital credit products administered by banks will have their non-repayment entered with the local credit bureaus, even for failing to repay a loan of only a few dollars[76], including more than 400,000 with outstanding loans of less than $2. This raises concerns regarding proportionality of punishment, especially since in Kenya most lenders do a simple "yes/no" check of credit history rather than using credit scores that weight the total amount of outstanding debt.

[74] Cook, T., McKay, C., CGAP, *Top 10 Things to Know About M-Shwari* (2015) http://www.cgap.org/blog/top-10-things-know-about-m-shwari
[75] Kaffenberger, M., Chege, P. CGAP, *Digital Credit in Kenya: Time for Celebration or Concern?* (2016) http://www.cgap.org/blog/digital-credit-kenya-time-celebration-or-concern
[76] *Pain of Kenyans blacklisted for amounts as small as Sh100 in mobile loans, bank fees* (2016) http://www.businessdailyafrica.com/Pain-of-Kenyans-blacklisted-for-amounts-as-small-as-Sh100/539552-3374802-103kvlwz/

Title of recommendation	Regular market consultations to understand new products and consumer experience and risks
Working Group/Work Stream	Consumer Experience and Protection
Theme	Digital credit
Audience for recommendation	Regulators

Regulators should engage in regular consultations with digital credit providers, consumer organizations, and other stakeholders to stay apprised of market developments, including new digital credit products and services being offered, the types of providers offering them, and consumer experiences and risks associated with them.

Monitoring the growth, business conduct, and lending practices of an increasingly diverse set of digital credit providers is challenging for regulators. Some models are scaling very rapidly and serving many lower-income consumers who are new to DFS or to formal credit. The arguments for balancing protection and market development considerations are strong: While the product fills a potentially important gap for consumers and can help drive eco-system development, there is potential for consumer detriment and even bubbles and the models are relatively untested.

Borrowers may be particularly vulnerable to the risks associated with high-cost consumer credit due to their lower, variable incomes and lack of familiarity with these products and their risks. In addition, the speed of delivery, confidential nature of the offer, and payment digitally rather than in cash, may affect consumer behaviour[68] by making the borrowing decision less intentional and reducing attention to the loan's full cost, affordability, and the consequences of late or partial repayment. Indeed, according to AFI[67] and CGAP[68], consumers may behave differently when presented with "instant" loans compared to a conventional lending process. Some will test out the system without actually needing the loan, racking up fees and negatively affecting their credit history if they have trouble with repayment. The instantaneous and impersonal nature of the transaction also precludes a cooling off period where customers can make sure that increasing their debt is a wise choice.

Therefore, it is important for providers to test their products and digital communications to minimize the risks of suboptimal behaviour by digital borrowers. There is emerging evidence how methods such as lab testing[77], interactive SMS[73], user testing of messaging scripts[78], qualitative research combined with data analysis can help digital lenders understand and address these behavioural challenges. These types of research and behavioural insights are currently being used by digital lenders to improve approaches to disclosure, consumer education, repayment, and understanding of digital data trails.

Regulators and providers need to maintain an open dialogue to enhance their understanding of the specific consumer protection issues that stem from digital credit features, such as how products are underwritten, marketed, disclosed, priced, and collected. Regulators could establish working groups, conferences, and newsletters to share information with each other on emerging digital credit risks and encourage providers to do the same. CGAP[10] reports that Bangladesh, Pakistan, and Tanzania have formal DFS industry discussion and coordination processes, and Kenya holds forums for stakeholders to share and discuss market trends and

[77] Mazer, R., Vancel, J., Keyman, A. CGAP, *Finding "Win-Win" in Digitally-Delivered Consumer Credit* (2016) http://www.cgap.org/blog/finding-%E2%80%9Cwin-win%E2%80%9D-digitally-delivered-consumer-credit
[78] Kaffenberger, M., Mazer, R. CGAP, *Simple Messages Help Consumers Understand Big Data* (2014) http://www.cgap.org/blog/simple-messages-help-consumers-understand-big-data

issues. These forums could be an opportunity to monitor trends and identify concerns in digital credit markets as they rapidly expand.

Market monitoring tools are important for reviewing debt trends on a continuous basis, using both demand-side data and review of digital credit portfolios. One useful step is to establish standardized reporting requirements for market monitoring. Reporting data can be complemented by information from other sources, such as complaint data, consumer research, consumer advocates, credit information bureau, and other potential indicators of debt stress and an overheated market.

Regulators' engagement with providers on product design can help to mitigate potential consumer protection weaknesses in a product and its value chain, identify cost-effective practices that improve transparency and repayment performance (that might serve as the basis for rules), and assess market trends as they arise. For example, the State Bank of Pakistan (SBP), recently created a digital credit "sandbox" by inviting prospective lenders to apply for approval; a first applicant has been approved for a six-month pilot, with a stocktaking midway and final approval decision at the end.

Analyzing available research and data on the customer experience, such as mystery shopping, surveys, and focus group discussions, will help to identify emerging risks and prioritize regulatory responses. In addition, regulators should encourage providers to improve consumer awareness and understanding over time.

Title of recommendation	Establishing QoS standards for DFS networks, platforms and other technical elements
Working Group	Consumer Experience and Protection
Theme	Quality of service (QoS)
Audience for recommendation	Telecom Regulators

Telecom regulators should establish QoS standards for DFS networks, platforms, and other technical elements, in consultation and coordination with the financial regulators and with input from stakeholders including DFS providers and telco operators. To oversee and enforce standards, the regulator should establish quarterly electronic reporting requirements on standardized metrics and should mandate corrective actions by noncompliant providers. Standards should be used as a criterion for licensing of DFS providers where reliable metrics can be established.

Quality of service (QoS) is defined[79] as the collective effect of performance that determines the degree of satisfaction of a user of the service. QoS generally is measured using objective criteria, versus a more subjective "quality of experience," and the term is generally used in the telecommunications sector. The above recommendation and related QoS topics have been taken up and are being considered by ITU-T Study Group 12 which deals with quality of service issues.

Issues (real or perceived), such as an inability to initiate or complete a transaction due to network downtime, excessive multi-step processes, and complex or confusing interfaces are deterrents to successful usage as well as trust and acceptance of DFS by potential customers. In fact, the failure to complete a transaction due to network downtime is frequently a top customer concern[10].

Telco regulators must ensure that the relevant networks, platforms, and other technical elements that serve DFS are in place and functioning properly. They should also consult and coordinate with financial regulators and DFS providers to establish QoS standards that are appropriate to the nature of digital delivery of financial services. QoS standards for DFS should evolve over time, taking into account new services, technologies, risks, and other relevant developments.

Because digital provision of financial services adds unique operational risks, such as new sources of potential fraud or technology failures, licensing decisions should consider the proposed DFS provider's ability to manage and mitigate these risks, including those related to agent involvement in transaction processing. Where standard QoS metrics have been established, these could be incorporated into licensing decisions as well.

Over time, standardized QoS metrics and methods for monitoring performance should be established so that the regulator does not solely rely on DFS providers' self-reported data. Regulators should require periodic electronic reports from providers disclosing their performance against these metrics and mandate corrective actions by providers who are not in compliance. In addition, DFS providers' performance results compared to the mandated service standards should be publicly available to promote transparency, oversight, and accountability.

Regulators should also consider establishing DFS provider liability for legitimate losses suffered by consumers (such as from fraud or agent misconduct) resulting from QoS issues (e.g. network downtime). Contractual agreements between DFS providers and other parties involved in the transaction could then establish the extent

[79] Recommendation E.800 (2008) http://www.itu.int/rec/T-REC-E.800-200809-I

to which DFS providers can assert claims on others. However, the regulatory-established liability should ideally rest with the DFS provider.