FINAL DRAFT - Policy Model on Consumer Protection for Digital Financial Services

Abbreviations and Acronyms

AFI	Alliance for Financial Inclusion
AI	Artificial Intelligence
AML	Anti-Money Laundering
APR	Annual Percentage Rate
BCEAO	Banque Centrale des Etats de l'Afrique de l'Ouest
BMGF	Bill and Melinda Gates Foundation
BTCA	Better Than Cash Alliance
CBA	Central Bank of Armenia
CEMCWG	Consumer Empowerment Market Conduct Working Group
CERT	Computer Emergency Response Team
CFI	Center for Financial Inclusion
CFPB	Consumer Financial Protection Bureau
CFT	Combating the Financing of Terrorism
CGAP	Consultative Group to Assist the Poor
CICO	Cash-in and Cash-out
CP	Consumer Protection
CP4DFS	Consumer Protection for Digital Financial Services
CSIRT	Computer Security Incident Response Team
CSOC	Cybersecurity Operations Centre
DFS	Digital Financial Services
DFSWG	Digital Financial Service Working Group
EIR	Effective Interest Rate
e-KYC	Electronic Know Your Customer
FSP	Financial Service Provider
G2P	Government to People
GDPR	General Data Protection Regulation
ITU	International Telecommunication Union
IVR	Interactive Voice Response
KYC	Know Your Customer
MIS	Management Information System
MSME	Micro, Small and Medium Enterprises
MNO	Mobile Network Operator
OECD	Organisation for Economic Co-operation and Development
PNG	Papua New Guinea
PM	Policy Model
USSD	Unstructured Supplementary Service Data
WB	World Bank

Executive summary

In the last decade, Digital Financial Services (DFS) has registered fast-paced growth contributing to the expansion of financial inclusion. This progress has not come without drawbacks – specifically Consumer **Protection (CP) related risks.** Though most regulators have regulations on consumer protection for the wider financial market, the unique peculiarities of DFS necessitate relevant reforms /adaptations to existing regulations to reflect the increasing role of DFS in the markets.

In line with this, the Digital Financial Services Working Group (DFSWG) and the Consumer Empowerment and Market Conduct Working Groups (CEMCWG) codified key policy guidance from relevant knowledge products developed over the decade, coupled with best practices within the AFI network in a policy model on Consumer Protection for DFS (CP4DFS).

Accordingly, this policy model (PM) has been developed around **five guidance pillars, namely** :

1. Policy and regulatory environment
2. Product development and service delivery
3. Consumer awareness, complaint and redress
4. Supervision and enforcement
5. Cross cutting issues

Each guidance pillar has corresponding **guiding principles and key policy recommendations,** as summarized in the table below. These are further enhanced with an introductory rationale and concluding best practices and industry insights within the AFI network (text boxes

Guiding principles	Key recommendations
1. Guidance on policy and regulatory environment	
1.1. Clear DFS relevant legal and regulatory provisions in CP frameworks	• Undertake a diagnostic analysis on CP4DFS • Undertake DFS responsive CP policy design • Design DFS provisions driven by evidence- based and risk-based approaches • Incorporate DFS provisions into existing CP policies • Create a specialized CP4DFS regulatory framework
1.2. Clear and harmonized governance framework	• Set up a dedicated CP unit or department for DFS • Facilitate inclusion of DFS on the agenda of financial sector boards/ national payment systems councils • Organize inter-agency CP4DFS framework • Define specialized regulatory oversight strategy • Define inter-agency information sharing framework
1.3. Clear legal / regulatory framework for regulating market competitiveness	• Facilitate a level playing ground for DFS providers to foster healthy competition • Define measures to prevent monopolistic and anti-competitive behaviors
2. Guidance on product development and service delivery	

2.1. Safeguarding privacy and protection of consumer data	• Integrate provisions on data privacy and protection into existing related policies • Mandate DFS providers to have internal policies on - data privacy and data protection - disclosure and consent • Extend regulation on data privacy and protection to third-parties
2.2. Strengthen cybersecurity	• Develop a cybersecurity framework with sector specific provisions • Foster cooperation between relevant stakeholders on cybersecurity • Facilitate awareness campaigns for customers • Mandate DFS providers to have internal policies and processes to protect consumers, secure delivery of services, manage internal risks and ensure security in the longer term • Mandate regular and incident reporting from DFS providers on cybersecurity
2.3. Fair treatment and responsible business conduct	• Encourage the development of an industry Code of Conduct for DFS providers • Encourage DFS providers to have internal policies compliant with regulation and attentive to the protection of the most vulnerable segments on - responsible practices and a Code of Ethics - responsible lending practices - fair price, terms and conditions - agent due diligence and supervision - prudent outsourcing
2.4. Product suitability: customer centricity, inclusiveness, relevance and usability	• Incorporate CP4DFS provisions in product development adopting a customer centric approach • Define measures to build an inclusive marketplace and ensure clients' access and mobility • Facilitate progressive customer due diligence – tiered KYC models
2.5. Adoption of risk management approach	• Mandate DFS providers to have an internal risk management framework • Define relevant regulatory provisions to mitigate risks from loss or misuse of client fund

3. Guidance on consumer awareness, complaint and redress	
3.1. Promotion of digital financial capability	• Define digital financial literacy and capability (DFL&C) strategies • Facilitate collaboration of relevant stakeholders • Incorporate DFL&C in product marketing/advertisement • DFL&C interventions should cover awareness, mitigation, complaints and redress. • DFL& C interventions should be evidence based. -
3.2. Responsible marketing / advertisement and sales (disclosure and transparency)	• Facilitate suitable digital communications / notifications between DFS providers and their clients • Provide guidance to DFS providers on - rules on format and manner - information to disclose and timing of said disclosure
3.3. Mechanism to ensure complaints and redress resolution	• Define DFS relevant provisions in regulatory directives on consumer complaints and redress Mandate DFS providers to have an Internal Dispute Resolution mechanism in place • • Institute reportingguidelines for both IDR and EDR. • Facilitate cooperation in complaints handling and redress.

4. Guidance on supervision and enforcement

4.1. Supervisory techniques and tools specific for DFS	• Undertake an assessment of supervisory tools and techniques for relevance to DFS • Adapt existing supervisory tools and techniques to the DFS sector • Integrate CP4DFS in the existing supervisory approaches • Create thematic benchmarks for supervising CP4DFS • Define techniques for agent network and non-bank e-money issuers • Explore incorporating supervisory benchmarks in regulatory sandbox and innovation hub frameworks.
4.2. Clear and harmonized supervisory governance framework	• Define an effective supervisory framework for CP4DFS • • Promote inter-agency cooperation between supervisory bodies • Define inter-agency information sharing framework • • Consider industry self-regulation initiatives for CP
4.3. Effective enforcement mechanism	• Adapt enforcement mandate and tools to DFS sector • Adopt principles-based mechanisms • Promote inter-agency coordination for enforcement
5. Guidance on cross cutting issues	
5.1. Promotion of CP principles for vulnerable segments	For relevant vulnerable groups in the country: • Leverage existing supervision tools to identify relevant CP4DFS risk issues and trends prevalent among identified vulnerable segments. • Facilitate multi stakeholder approach, to promotion of CP4DFS • Design relevant demand driven, and evidence based digital financial literacy and capability interventions • Define relevant vulnerable segment responsive provisions in prudential and market conduct regulations. • Encourage DFS providers to adopt relevant behavioural insights of relevant vulnerable segments in the design and delivery of products, services and / delivery channels;. • Encourage DFS providers to incorporate strategies relevant to vulnerable segments in their consumer awareness interventions -
5.2. DFS in disaster / emergency response	• Take prompt interventions towards coordination of response • Launch awareness campaign • Ensure emergency interventions are aligned with the CP principles • Mandate DFS providers to have a Business Continuity plan

Table 1. Guidance areas of the PM framework with their main guiding principles and key recommendations.

Background and context

Digital financial services (DFS) are expanding extensively with its characteristic dynamism in products, services, distribution channels, use case and players.

The multifaceted scope of DFS mirrors the **Consumer Protection (CP) related risks** associated with it across its value chain and players - demand, supply and regulatory sides as highlighted below.

Demand side	Supply side	Regulatory side
• Asymmetry of information • In adequate digital financial literacy and capability • Over indebtedness (for digital lending) • • Lack of trust in agent network / new technologies • Illiteracy (literacy and numeracy)	• Products not tailored to clients' needs and/ sutability • Misleading communication • Unfair / excessive pricing • Aggressive commercial practices • Fraud / theft • Data breach • Lack of /ineffective recourse mechanism • Inadequate safeguard of consumer rights • Inadequate mechanisms for clients' feedback •	• Regulatory framework not tailored to DFS sector or not covering all Consumer Protection principles • Inadequate capacity to identify existing and new CP4DFS risks • Inadequate supervisory capacity • Regulatory overlaps - uneven regulation, arbitrage, overregulation

Table 2. Summary of the main CP4DFS related risks from demand, supply and regulatory perspectives

Emerging trends across financial markets indicate that these risks have the potential adversely impact trust of consumers, destabilize financial markets, discourage uptake and usage of DFS, eroding the gains made in financial inclusion. Though regulators acknowledge the need for DFS relevant consumer protection regulation, most are yet to adapt existing consumer protection regulations and interventions to reflect the deepening role of DFS.

In line with this, the Digital Financial Services Working Group (DFSWG) and the Consumer Empowerment and Market Conduct Working Groups (CEMCWG) committed to synthesize and harmonize learnings, best practices and policies from its relevant knowledge products and across the network into a recognized policy model.

This will serve as a **compendium** of relevant approaches, frameworks and directives for policy guidance on **practical regulatory and policy approaches** on consumer protection regulation for DFS.

The Policy Model on Consumer Protection for Digital Financial Services (CP4DFS)

1. Guidance on Policy and Regulatory Environment

1.1 **Guiding Principle:** Clear DFS relevant legal and regulatory provisions in consumer protection frameworks

Rationale

Financial markets are witnessing a deepening of DFS, with the industry moving beyond the basic cash-in and cash-out (CICO) services to an extended bouquet of services ranging from credit, savings, investment, insurance, cross border remittances, etc. Furthermore, DFS providers are developing innovative business model such as leveraging the use of data in product design and delivery and bundling of products.

Given these developments, there is a need to improve the existing regulatory frameworks to reflect the deepening and complex nature of DFS and to minimize the incidence of scattered, ad hoc and "catch-up" approaches to addressing both existing and potentially new DFS related risks issues.

This guidance is anchored within the proposition that a clear legal and regulatory provision on DFS ensures the foundational integrity of wider subsequent interventions as entrenching DFS within consumer protection regulatory frameworks. It highlights the need to consciously identify, define and incorporate DFS relevant legal and regulatory provisions within existing consumer protection frameworks of the financial market (such as a national consumer protection policy, national data protection policy, etc.) as well as DFS industry relevant regulatory instruments (such as policies on mobile financial services, electronic money, branchless banking, etc.) among others.

Key recommendations

- **Undertake a diagnostic analysis on CP4DFS.** The authority to carry out a diagnostic analysis of the ecosystem to map the existing CP provisions related to DFS and identify main gaps to guide future policy interventions.
- **Undertake DFS responsive consumer protection policy design.** Undertake the design of new consumer protection policies, or the reform of existing ones, either for an agnostic industry landscape or specific to the DFS industry. The main objective is to reflect the existing, as well as projected, DFS landscape with its associated risks. This should cover all relevant players – policy makers, regulators, providers, consumers, etc.
- **Design DFS provisions driven by evidence-based and risk-based approaches.** The authority to design DFS provisions following an evidence-based approach, utilizing data on critical factors within the DFS industry such as: market maturity; product portfolio; regulatory capacity; risk patterns (existing and projected); pace of innovation within the market; digital financial literacy and capability capacity of consumers; vulnerable segments; and market interaction with outside jurisdictions among others. Furthermore, provisions to be technology/product agnostic, designed following a risk-based approach, responsive to existing and projected product portfolio delivery channels and innovation.
- **Incorporate DFS provisions into existing consumer protection policies.** There are varying models to consumer protection frameworks across the various jurisdictions. These include: a national level industry agnostic consumer protection policy; specialized consumer protection policy for the banking sector; consumer protection policies by allied financial sector regulators (capital market, insurance, pensions etc.); and technology / product specific regulatory directives for mobile money, e-money, branchless banking, fintech, payment systems, and Electronic Know Your Customer (e-KYC) among others.
    - Irrespective of the model being implemented in a jurisdiction, regulators should review consumer protection policies with a DFS lens. They should design and

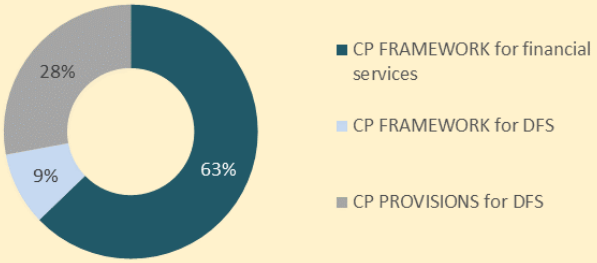
integrate/incorporate DFS specific provisions to address gaps across the various legal mandates and regulatory instruments.

- **Create a specialized CP4DFS regulatory framework.** Where feasible, jurisdictions should synthesize key DFS specific legal mandates and regulatory provisions into a compendium / regulatory framework on CP4DFS.
    - **Harmonization of existing provisions:** Regulators to identify and harmonize possible duplications and contradictory provisions across various legal mandates, policies, or regulatory provisions.
    - **Inclusive approach to development of CP4DFS framework:** Regulators to facilitate the participation of allied financial sector regulators, and relevant stakeholders in the synthetization and harmonization of existing DFS legal mandates and regulatory provisions across various instruments into a comprehensive CP4DFS
    - **Include a consumer centric approach in the development of the CP4DFS framework:** The authority to consider adopting a consumer centric approach which is sensitive to the needs, norms and financial behavior of various segments such as women, youth, rural poor, Micro, Small & Medium Enterprises (MSME), etc.
    - **Make DFS provisions consistent with relevant international industry and thematic regulatory standards and protocols:** Regulators to consider making CP4DFS provisions consistent with existing global industry standards/guidance and best use cases within the local context. These could include but are not limited to: globally recognized standards on data protection, cloud computing, and cybersecurity, credit referencing and e-money, deposit insurance, among others.

TEXT BOX n.1: CP4DFS policy measures in place across AFI members

Regulators are showing growing interest towards having a CP4DFS related framework, despite the gaps in targeted regulations in CP4DFS.

In a survey within the AFI, **few members reported targeted /specialized CP4DFS frameworks**



Countries with CP provisions for DFS covered the following thematic issues:

Graph 1. Results from the survey on the existing CP4DFS framework and specific provisions.

TEXT BOX n.2: Process to develop a CP framework – the case from Papua New Guinea

Papua New Guinea (PNG) has a significant percentage of the population excluded from the formal financial sector. However, in recent years, with the widespread use of mobile money , the Central Bank of PNG is developing a Consumer Protection framework which integrates DFS.

With the increasing attention towards financial inclusion, the National Government developed the Financial Sector Development Strategy 2018-2030 and the National Financial Inclusion Strategy 2016-2020. Consumer protection provisions were incorporated in both strategies In 2018, the report of the Treasury commissioned Consumer and Competition Framework Review team which was mandated to review the Independent Consumer and Competition Commission and examine the laws and institutions that protect consumers and promote competition in PNG recommended the development of a specialized Consumer Protection framework for the financial sector. Although financial inclusion in the country is mostly driven by traditional financial institutions, and competition between MNOs is still at an early stage , an **important collaborative process with regional/provincial industry stakeholders** has motivated the Central Bank of PNG to expand the scope of the framework to fintech and include CP4DFS considerations. Regulations, which were initially based on an institutional approach, were revised to a **product-based approach** to include all the miscellaneous and unregulated financial institutions present in the country which hitherto were not under the oversight of the Central Bank.

1.2 Guiding Principle: Clear and harmonized governance framework

Rationale

Increasingly, innovations in DFS such as digital deposit taking, credit, micro insurance, micro pensions, and investments involve multifaceted players. This positions DFS innovations within the regulatory oversight of different regulators from the wider financial sector, to the telecommunication and trade sectors.

Across some jurisdictions, the regulatory oversight mandate is further blurred by industry agnostic national authorities/ombudsmen such as national consumer protection, data protection, cybersecurity, and competition authorities. At the institutional level, consumer protection oversight is shared across different technical units/departments within the same regulator (e.g. prudential department, market conduct unit, consumer protection unit, payment systems unit, DFS unit, non-bank financial services unit, financial inclusion unit, etc.). This creates a blur in the scope of mandates, roles, responsibilities and oversight. The plethora of regulatory oversight mandates deepens the complexity of the governance framework and has the potential to drive regulatory arbitrage and over regulation of DFS.

A number of jurisdictions have established financial sector governance boards which seek to provide an integrated oversight to the governance of the wider financial sector. To a large extent these boards provide high level policy leadership with implementation and supervision delegated to micro level institutional units. The challenge lies in ensuring harmonized implementation and supervision of regulatory interventions for CP4DFS.

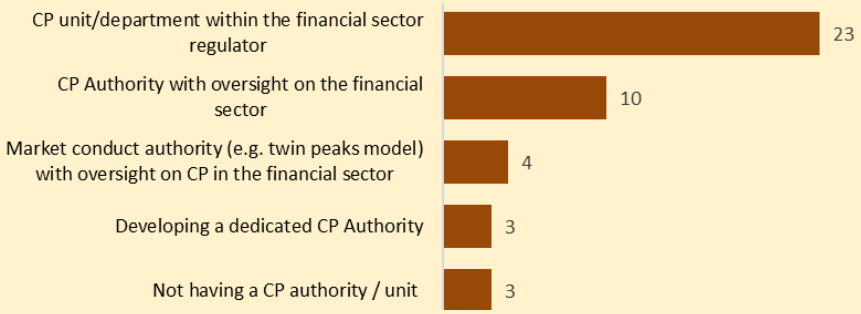
Key recommendations

- **Set up a dedicated Consumer Protection unit or department for DFS.** The authority to have a clear legal mandate to address CP4DFS, with the definition of roles and responsibilities, adequate range of powers and scope of oversight through which to operate (also extending oversight to non-regulated players - e.g. fintech, big tech etc.). The authority to be equipped with institutional capacity in terms of technical skills, resources, supervisory tools and systems. Based on the existing regulatory framework, the dedicated consumer protection unit can be set under:
    - A dedicated unit / department for DFS under the financial service regulator
    - A dedicated consumer protection agency (with oversight of the financial sector)
    - A dedicated market conduct authority for financial services.

- **Entrench DFS within framework of national financial sector boards.** Where feasible per the maturity/depth of the DFS industry within the financial sector of a jurisdiction, the authority to encourage the entrenchment of DFS within the representation and focus of financial sector boards / councils. This could include but not limited to representation of DFS relevant expert on the board, incorporating key DFS relevant indicators/issues within the oversight agenda of the board.
- **Organize inter-agency CP4DFS framework.** Authority(ies) to encourage initiating a representative board of consumer protection for DFS focal points across the various relevant regulatory bodies. The representative board to have a clear governance framework per level of responsibility within the consumer protection and DFS ecosystem.
- **Define specialized regulatory oversight strategy.** The inter-agency CP4DFS board is to review strengths of mandate, responsibility and capacity and assign the varied thematic focus of CP4DFS to relevant authorities as specialty oversight regulators. Identified specialized regulator(s) for thematic areas could be an individual institution or more. In the case where more than one institution is assigned regulatory oversight of a thematic issue, authorities need to ensure a clear and result oriented responsibility framework for that thematic team.
- **Define inter-agency information sharing framework.** Authority(ies) to establish mechanisms to facilitate easy sharing and swift access to information/ data on CP4DFS among members of the interagency regulatory board. These could include:
    - Establishing a common platform for data reporting either in real time or periodic reporting
    - Instituting periodic reporting protocols/ requirements for members.

TEXT BOX n.3: Consumer protection governance models within the AFI network

Survey within the AFI network, indicates varied models with oversight of **consumer protection**. There is neither a best practice model or a "one size fits all" approach to the governance of CP4DFS. , However it is critical for the governance framework to be well defined , with clear mandates, , defined range of powers, scope of oversight, defined scope cooperation among allied regulators and agencies for a harmonized and effective approach to CP4DFS. This will encourage the effective use of resources and minimize if not prevent the incidence of regulatory arbitrage and over regulation.



Graph 2. Results from the AFI survey on the different typologies of CP authority

1.3 Guiding Principle: Clear legal / regulatory framework for regulating market competitiveness

Rationale

Competition within the DFS market is important to ensure market stability and multiplicity of products and players. However, the digital transformation of the financial sector requires significant investments in resources (human and capital) for the development of innovative products and to drive the required changes in the infrastructure, that may position some providers in a competitive advantage within the market. With the characteristic feature of DFS as multifaceted, the industry creates/relies on interdependencies within providers, products, channels, data and customers. This

inherent interdependent ecosystem creates opportunities for industry players to obtain unfair/dominate market share. With time a dominant player could control the bulk of the industry data, influence delivery channels and enhance operational efficiency through mergers and acquisitions of relevant technology players and delivery channels. A monopoly within the market has the capacity to distort the market, create a supply centric market orientation, limit the portfolio of choice and power for consumers and adversely affect financial inclusion.

It is therefore critical for the regulator to foster a healthy competition with the DFS market.

Key recommendations

- **Facilitate a level playing field for DFS providers to foster healthy competition.** Authority(ies) to consciously facilitate a level playing field within the DFS industry to promote healthy competition. Where possible, authority(ies) to develop a DFS industry wide competition framework. This should outline critical risks, paths and players.
    - For jurisdictions with national competition authorities/ombudsman, the authority(ies) to incorporate the DFS competition framework within their wider regulatory framework.
- **Define measures to prevent monopolistic and anti-competitive behaviors.** The authority to adopt measures to prevent monopolistic and anti-competitive behaviors by dominant players. This should be implemented in collaboration with the competition authority in the jurisdiction to closely monitor anti-competitive measures and other instances of market abuse.

2. Guidance on Product Development and Service Delivery

2.1 Guiding Principle: Safeguarding privacy and protection of consumer data

Rationale

In the digital financial era, data is at the core of DFS. It runs through the entire operating value chain of the DFS industry, as an operating input (e.g. for product development or Application Program Interfaces), output (data generated by consumers in the use of DFS) and as a product (collection and sale of data). Also, digital data management is witnessing increasing sophistication in innovations for example, in algorithm-based creditworthiness assessments, the use of big data or Artificial Intelligence (AI) etc.

In this context, inappropriate use, management and storage of clients' data coupled with poor disclosure and transparency, has the potential to exclude vulnerable segments from financial services, drive a lack of trust in DFS and erode the gains in financial inclusion.

It is therefore critical for regulators to address two main risks, namely (i) how to secure data against unauthorized access (data protection) and (ii) how to ensure the appropriate use and management of consumer data (data privacy). Even though across countries the concept of privacy can have different nuances, the regulators should ensure that the promotion of this guiding principle will ensure the protection of the fundamental right of customers.

Key recommendations

- **Integrate provisions on data privacy and protection into existing related policies.** Through consultative processes with the DFS industry, the authority to consider undertaking a review of existing provisions on data privacy and protection to identify possible gaps and evaluate potential risks. Reforms should safeguard the protection and privacy of consumer data in the gathering, processing, use, distribution and storage of data. Where relevant, the authority to have provisions for big data, AI, IT outsourcing, cross border data flows and cloud-based storage (oversight of nonresident providers and cross-border data transfers).
- **Mandate DFS providers to have internal policies on data privacy and data protection.** The authority(ies) to mandate or encourage DFS providers to have an internal policy on consumer data protection and privacy which covers the holistic cycle in consumer data – from generation to deletion. It should also define a balanced and mutually beneficial relationship between the data subject (customer) and data controller (DFS provider). Among others, it could provide:
    - Typology of data that can be collected to be justified by the operational needs.
    - Define maximum timing of storage
    - An assessment plan to identify data privacy risks and mitigation measures
    - A penalty matrix for data privacy breaches
    - Safeguard provisions to prevent illicit or accidental alteration of data files (e.g. user restrictions or system violation logs)
    - Processes to ensure regulator access and usage of data for supervisory purposes, etc.
- **Mandate DFS providers to have internal policies on disclosure consent.** The authority(ies) to define a detailed guidance for consumer awareness on privacy, such as:
    - Obligation to adequately inform clients on how client data is secured, distributed and reported and ensure their understanding.
    - Mandate contracts with clients should contain a privacy clause, which should be communicated in an easy to understand format and language and where feasible read and explained to the clients.
    - Obligation to secure clients´ consent before data / information is used and shared with third-party entities (such as credit registry / bureaus, central banks, center data sellers,

etc.) and the possibility for clients to withdraw this permission at any time (if not mandatory for receiving the product / service).

- **Extend regulation on data privacy and protection to third parties:** authority(ies) to mandate providers to ensure responsibility for data privacy and protection in dealing with third party entities (such as in the case of operational and technology outsourcing). This should include provisions to inform and seek clients consent for the data sharing.

2.2 Guiding Principle: Strengthen cybersecurity

Rationale

DFS providers are revolutionizing the speed and reach of financial inclusion with providers reaching consumers at the bottom of the pyramid. For low income people, opening a digital account is likely to represent their first formal financial account. This progressive departure from cash to DFS implies a logical transition of financially motivated crimes from physical threats/attacks to cyber threats attacks. This has led to increasing incidences in system outages, data breaches and fraud.

The integrity and security of the operating and delivery systems as well as the devices used by consumers is critical to: (i) safeguard customer assets/funds; (ii) protect consumer data; (iii) and for the operational stability of providers and the general financial market.

Jurisdictions with generally less investments in cyber system development and security remain vulnerable to these growing threats/attacks, especially with consumers at the bottom of the pyramid who characteristically, have minimal to no digital financial literacy. This is creating a negative experience for consumers, damaging the reputation of DFS and eroding the gains in financial inclusion.

Key recommendations[1]

- **Develop a cybersecurity framework with sector-specific provisions**. The authority(ies) to harmonize legal and regulatory provisions into a framework for DFS providers. It should follow principle-based approaches that reference international standard frameworks, adapted to the local environment and trends.
- The authority to have a defined supervisory / oversight role to supervise and monitor cybersecurity within the DFS ecosystem. The authority to define specific provisions, such as:
    - Mechanism to ensure appropriate cybersecurity risk mitigation measures are established by all players in the DFS value chain
    - Define clear responsibility for end-user cybersecurity awareness for all DFS players in the value chain
    - Provide Service Level Agreements for resolution of DFS end-user cybersecurity challenges to all players.
- **Foster cooperation between relevant stakeholders**. The authority to foster information sharing and collaboration between relevant local and international stakeholders (DFS providers, regulators, universities, etc.) to explore/consider the :
    - Creation of a national cyber-awareness and warning body; in case of insufficient capacity it should consider identifying regional or international partners to support.
    - Establishment of an industry-wide Cybersecurity Operations Centre (CSOC) and Computer Emergency Response Team (CERT).
    - Facilitation of cooperation between the national CSOC/CERT and regional/international CSOC/CERT that is in place.

[1] For more details, please refer to the AFI knowledge product "Cybersecurity for financial inclusion: Framework & Risk Guide" (2019)

- **Mandate DFS providers to have internal cyber security policies and processes:** Authority to ensure that DFS providers define internal policies **with provisions** to
    - protect customers,
    - secure delivery of services,
    - manage internal risks
    - Understand and manage potential risks with partners/third parties
    - Ensure a long-term proactive approach to risk mitigation and management.
- **Mandate regular and incident reporting**. The authority to mandate DFS providers to provide regular as well as incidents reporting on cyberattacks, disruption of services and data breaches with redress actions undertaken and timeframes.

TEXT BOX n.4: Cybersecurity measures: the case of Ghana

In 2018, Bank of Ghana[2] released the cybersecurity framework "Cyber and Information Security Directive", which defines protocols and procedures, referencing international regulations and standards (as the ISO7001 for information security or guidelines ISO27032).
Main topics addressed by the framework are:

- routine and emergency scenarios
- main team and responsibilities
- communication and cooperation intra-company and with regulator
- regular and ad-hoc reporting
- security measures
- assurance of data and network security.

2.3 Guiding Principle: Fair treatment and responsible business conduct

Rationale

The DFS industry is characterized as a very competitive landscape with providers vying for customer acquisition. This has been effective in driving financial inclusion, especially to the last mile - to many signing up for a DFS represents their maiden access to a formal financial service. However, the competitive landscape has the potential to drive some DFS providers to adopt abusive and harmful practices towards consumers with a consequent reputational risk for the entire sector.

In relation to financial inclusion, these unfair and irresponsible business practices can take advantage of the vulnerabilities (example illiteracy, low digital financial literacy etc.) of consumers, especially those at the bottom of the pyramid On the other hand, it could further deepen their vulnerabilities such as, limiting their access to financial services due to digital profiling or over indebtedness from over lending and predatory interest rates. The objective of this guidance is to promote high ethical standards and build a trusted and reliable ecosystem based on respect, fair conduct, and adequate safeguards to detect and correct irresponsible and unfair practices by providers.

Key recommendations

A) Encourage the development of an industry Code of Conduct.

- The authority to encourage the development and adoption of an industry Code of Conduct with broadly recognized principles (e.g. integrity, transparency, fairness, confidentiality, etc.) for developing a safe and responsible CP4DFS environment. This would ensure DFS service providers take ownership of the process, being actively involved in the identification of risks, definition of mitigation practices and responsible for their implementation. Authorities should ensure all financial services providers, including non-bank providers, ascribe to the industry code of conduct for the provision of financial services.

[2] For more details, please refer to AFI knowledge product "Cybersecurity for financial inclusion: Framework & Risk Guide" (2019)

B) Encourage DFS providers to establish code of ethics and internal procedures on responsible practices.

- Besides the industry Code of Conduct, authorities to require / encourage DFS providers to develop and communicate to consumers its internal Code of Ethics towards the fair and respectful treatment of clients. The Code of Ethics should be a live document, to be regularly updated, based on the core values of the providers that governs internal and external relations and norms of conduct (such as having standards of professional conduct, respecting the clientele and avoidance of discrimination with attention towards vulnerable segments such as women or people with disabilities, avoidance of conflict of interest, privileged information, corruption). It should also address how the DFS provider will internally report / manage breaches and define a set of sanctions (complaint mechanisms / suggestions boxes / ad hoc reporting system, etc.). Main guidance can be:
    - The adoption of high ethical standards of professional conduct that are expected to be followed by all staff (including third parties)
    - Avoidance of institutionalized (e.g. data profiling) and individual discrimination (by a staff or agent) of consumers. Based on systems, algorithms, ethnicity, gender, age, disability, etc.).
    - Guidance on types of internal control mechanisms that can be developed (e.g. performance evaluation systems with rewards and/or sanctions, complaint mechanisms, among others.).

C) Set responsible lending practices[3]: Within the context of delivery of small loans through digital means, regulators should consider the following principles to enhance their regulatory interventions towards a responsible digital credit industry.

- **Clear legal mandate and regulatory framework:** Authorities to define a clear legal mandate for licensing, regulating and supervising market conduct for the provision of digital credit.

- **Appropriate institutional capacity:** Authorities should invest in adequate capacity in terms of technical skills, resources, supervisory tools and systems for the effective regulation and supervision of the digital credit industry.
- **Comprehensive and effective credit referencing systems:** Authorities should implement comprehensive and effective credit referencing systems that incorporate a wide range of sourcing information, including from non-bank financial services providers.
- **Transparency and disclosure**: Authorities should mandate provisions to ensure digital credit is offered with appropriate disclosure of terms and conditions (e.g. loan tenure, effective interest rates, fees and charges, recovery process, sharing of consumer data, penalties and other information).

TEXT BOX n.5: Scope of regulation on Fair treatment and responsible business conduct across surveyed AFI members

Survey among AFI members, indicates that in general regulators have instituted regulatory provisions to reflect the key principle-based policy recommendations discussed above. Nonetheless most regulators are yet to develop specialized regulation on digital credit/ responsible lending. Only Thailand, reported a specialized

[3] For more details, please refer to the AFI knowledge product: "Digitally Delivered Credit: Consumer Protection Issues and Policy Responses to New Models of Digital Lending" (2017) and "Policy Framework for Responsible Digital Credit" (2020)

regulation on digital credit, with only 10 countries reporting regulatory oversight of non-bank digital credit providers, especially for fintechs.

2.4 Guiding Principle: Product suitability: customer centricity, inclusiveness, relevance and usability

Rationale

The rate of sophistication in innovation of DFS per scope of products, services, delivery channels, use cases, etc., keeps extending at a fast rate. In the pursuit of operational efficiency, product development and delivery could tend to be more biased towards the provider than the consumers. In markets where DFS have become a critical catalyst for financial inclusion, a mismatch between product development, delivery, usability and consumers capability to use and afford the product has a direct implication to bridging the financial gap in such jurisdictions.

Hence, it has become critical for regulators to facilitate the development of a market which is consumer centric, promotes inclusiveness of all consumer segments (including specific needs based on consumer group profiles such as women, youth and disabled persons) and is affordable, especially to the bottom of the pyramid. This is fundamental in ensuring the progressive growth in access, usage and quality of DFS - which will subsequently lead to improved and sustainable financial inclusion rates.

Key recommendations

- **Mandate a customer centric approach to development of DFS.** the authority to consider any of the following approaches per relevance to their jurisdictions in the development of products and delivery channels:
    - *Product approval approach*: the regulator to intervene in reviewing / approving DFS product features (price, terms and conditions) including subsequent changes, defining list of prohibited products / services and features (e.g. bundling products), and also
    - *Principle based approach*: the regulator to require providers to adhere to identified principles that ensure product suitability through the incorporation of minimum standards during the design phase, pilots and/or rollouts (e.g. adopting clients' behavioral insights with attention to vulnerable segments, data protection and privacy, disclosure, etc.)
- *Testing approach*: the regulator to incorporate product suitability indicators in regulatory sandbox for the testing of new products. **Define measures to build an inclusive marketplace and ensure clients' access and mobility.** The authority to adopt measures to build an inclusive marketplace and ensure clients' access and mobility through:
    - Facilitating the interoperability of the payment system infrastructure.
    - limiting barriers for entry into and exit out of the market (for DFS providers) and to encourage switching products/services for consumers (e.g. provisions on cooling off period, closing an account, prepaying a loan, charges for change in product/service and switching to another provider);
    - The authority to encourage and facilitate proportionate reach of payment infrastructure (e.g. agent's points of sales, ATM and PoS, etc.) across the jurisdiction, especially last mile access, to promote financial inclusion.
- **Facilitate progressive customer due diligence - tiered Know Your-Customer (KYC) models:** The authority to define provisions to facilitate progressive customer due diligence – tiered KYC models(such as the use of SIM registration data)to encourage access to financial services for all, especially the bottom of the pyramid segment .

2.5 Guiding Principle: Adoption of a risk management approach

Rationale

Significant consumer protection risk issues arise between product delivery and service delivery pathways. Inefficient or weak safeguards at the supply end of DFS, such as security and integrity of operating systems has immense potential to expose consumers to vulnerabilities hence adversely affecting access, usage and quality of financial services.

Also, the fluid, fast paced, wide reach characteristic of DFS is reflective of its related risks - similarly ramifications of its risks could be swift and far reaching with grave consequences on market stability and financial inclusion. Hence it has become critical, yet strategic, for regulators and providers alike to be proactive and preemptive in their approach to addressing consumer protection risks within the DFS market. This will ensure that an ad hoc or catch up approach to addressing risks after it penetrates the market is minimized. The objective is not only to avoid the risks but primarily to ensure there is an adequate framework to anticipate and manage them (i.e. to identify, classify, measure, prevent, transfer or mitigate).

Key recommendations

- **Mandate DFS providers to have an internal risk management framework.** The authority to require DFS providers to develop a risk management framework which could include:
    - A risk measurement framework to identify, assess and prioritize risks related to CP4DFS.
    - An appropriate management structure satisfying regulator directed 'fit and proper' requirements (e.g. appointment of Chief Information Security Officer (CISO)) in the management of DFS relevant functions (such as cybersecurity, data protection, etc.)
    - Business continuity mechanisms and risk response interventions for relevant CP4DFS risks and emergency situations.
- **Define relevant regulatory provisions to mitigate risks from loss or misuse of client funds.** This could include:
    - *Minimum capital requirements*: to require e-money issuers, regardless of their licensing model, to have an initial and ongoing minimum capital amount to mitigate risks associated with unexpected losses (insolvency risk) and operations (operational risk). Capital requirements could be based on the characteristics of the market, economic and regulatory reality.
    - *Safeguarding Client Funds:* authorities to establish minimally burdensome and cost-effective guidance for safeguarding client funds by e-money issuers. Examples include.
        - Liquidity Risk: Require e-money issuer to set aside funds equal to 100% of outstanding e-money liabilities.
        - Issuer Insolvency Risk: Require e-money issuer to hold funds set aside to repay clients in trust (or similar fiduciary instrument). Ring-fence client funds from issuer funds.
        - Bank Insolvency Risk: Provisions for client funds to be covered by direct or pass-through deposit insurance.
    - *Client compensation requirements*: to require e-money providers, regardless of licensing model, to develop guidelines for compensations to clients in case of loss or misuse of their funds (such as, system malfunctions / network downtime, fraud by agents, employees and third parties, and agent misconduct).

3 Guidance on Consumer Awareness, Complaint and Redress

3.1 Guiding Principle: Promotion of digital financial capability

Rationale

Innovations in fintech are driving the development of sophisticated financial products. Hence, it has become important for consumers to constantly increase their knowledge and skills to effectively use these products and services in a secure manner. However, a significant proportion of the population across jurisdictions remains illiterate, challenging usage beyond adoption while deepening their susceptibility to risk. Similarly, some jurisdictions have significant proportions of some demographics or segments with particular vulnerabilities in relation to financial inclusion; these will need specialized interventions to build their capability for sustainable financial inclusion.

Yet, digital financial education has traditionally not been a core objective of regulators. Nonetheless, the aftermath of the global financial crises, coupled with growing incidences in DFS related consumer protection issues such as fraud, data protection, over indebtedness, inadequate transparency / information, unbalanced marketing/selling of products/services etc., which adversely impacts trust of consumers, destabilizes financial markets, discourages uptake and usage of DFS and erodes the gains made towards financial inclusion has compelled the interest of regulators in digital financial education.

It has, therefore, become important for regulators to understand how to facilitate the development of a financially knowledgeable digital market.

Key recommendations

- **Digital Financial Capability strategies:** Establish strategies and interventions to promote awareness of DFS and enhance digital financial literacy and capability, especially among vulnerable groups like women, youth, the elderly, migrants, refugees/ IDPs.
- **Facilitate collaboration of relevant stakeholders** in the design, implementation, and evaluation of digital financial capability strategies/interventions. Stakeholders could include allied financial sector regulators, education sector, DFS providers, development partners, the media among others.
- Encourage DFS providers to **incorporate digital financial literacy in product advertisements** and campaigns and contribute to industry-wide digital financial literacy programs.
- Authorities to ensure scope of digital financial literacy and capability interventions include awareness raising, risk mitigation and the consumer complaint and redress process.
- Conduct periodic demand-side surveys to assess the financial capabilities of consumers and devise appropriate national financial education strategies.

TEXT BOX n.7: Digital Financial Capability

Consumer awareness is the biggest concern among AFI's members. **However, digital financial capability has not gained a primary role** within the national financial education initiatives. Almost two third of AFI member countries are promoting initiatives on financial education / awareness campaigns but only in a few cases are DFS topics covered[4].

The Central Bank of Nigeria has developed an E-Learning Portal to help deploy Financial Literacy Trainers and it is leveraging social media to drive financial education awareness. It is also addressing DFS, teaching people how to use digital services such as ATMs or digital money transfers and to be aware of possible frauds and scam. Many countries cover topics such as: how to open, use and manage a digital account; how to protect from theft/fraud; PIN protection; etc. The **National Bank of Belarus and Bank of Russia** have a financial

[4] Many countries have declared of carrying out digital financial education just because they rely on digital tools (such as applications, tablet, social media, etc.).

education portal that addresses many topics including some DFS related issues (such as online deposits, cashless payments, internet banking and crowdfunding).

3.2 Guiding Principle: Responsible marketing / advertisement and sales (disclosure and transparency)

Rationale

As with any other financial product, disclosure and transparency principles are fundamental to reduce asymmetry of information and ensure that clients especially those vulnerable and with limited (digital financial) literacy, take informed decisions. However, in an attempt to gain significant market share, providers could resort to irresponsible advertisement and marketing strategies. These include but are not limited to aggressive marketing; push marketing; bundling of products; deceptive information; and poor transparency in the disclosure of costs and features, terms, and conditions during advertisement.

Critical to the success of any policy model is the enabling environment to support its application and adherence. Poor regulatory guidance has the potential to discourage providers to incorporate effective disclosure in product marketing. For example, regarding the disclosure of pricing for credit products, it is a good practice to provide clients with APR or EIR. However, in countries with no such regulation or weak enforcement, providers who disclose their APR or EIR could be at a disadvantage as consumer are likely to perceive them as expensive.

For these reasons, regulators should facilitate well defined disclosure and transparency principles to ensure clients can trust the DFS.

Key recommendations

- **Facilitate suitability of digital communication:** Establish provisions to ensure that terms and conditions for DFS are disclosed digitally in simple terms and in a language that most target consumers understand.
- **Provide guidance on format and manner for responsible marketing / advertisement / sales.** The authority to suggest/mandate rules on format and manner within the following principles:
    - Effective transparency and disclosure of costs/fees(charges at digital providers' premises and their agent outlets), features, risks, terms and conditions in the advertisement, marketing and sales information of DFS (e.g. to disclose information publicly on websites, marketing material, agents' point of sales, adoption of live calculators on applications or websites, etc.;
    - Use of appropriate language to ensure consumers effectively understand the product information. This could include the use of local languages, avoidance of technical jargons, incomplete, unprecise, and misleading information and use of multiple mediums such as written and oral communications as deemed feasible

TEXT BOX n.6: Best practices on transparency and disclosure – the Code of Conduct of Armenia

In Armenia, digital financial inclusion is growing fast (from 12% in 2011 to 42% in 2017) and becoming of great interest for the regulator, the Central Bank of Armenia (CBA). Among others CBA with the Financial Stability Department and its subgroup "Center of Consumer Rights protection and Financial education center" has oversight of consumer protection practices.

An important measure taken is on transparency and disclosure of DFS. Through a **collaborative approach** between the entire financial sector (banks, insurance companies, MNOs, etc.) and a few CBA internal departments (market conduct, prudential regulation and legal departments), CBA adapted existing provisions to the idiosyncrasies of DFS. Most importantly CBA has created a **Code of Conduct** that all DFS providers are requested to sign with **guidance on how to communicate with clients and disclose information**. More specifically it covers:

(i) oral communication before signing contracts / agreements
(ii) the use of multiple channels
(iii) detailed information on main contents to share with the clients (terms, conditions, price, clause in case of any changes in conditions) at the time of contracts / agreements signature

3.3 Guiding Principle: Mechanism to ensure complaints and redress resolution

Rationale

Regulators Consumer complaint and redress mechanisms are critical to CP4DFS - as it is a key approach to entrenching the principle of customer centricity within the DFS value chain. An accessible, timely and efficient complaints and redress mechanism is central in entrenching consumer trust in the use of DFS. This is critical in the context of financial inclusion where DFS have become a core catalyst in extending formal financial services to the unbanked especially at the bottom of the pyramid. An efficient complaints and redress system does not only enhance their trust in DFS, but it also safeguards their rather meagre income, livelihoods and resilience to financial risks as to many of such, DFS represents their first and only formal account and a breach to it, is a breach to their survival.

Both regulators and DFS providers have taken note and are responding with varying approaches to complaints and redress mechanisms. However much remains to be done in ensuring the effective use of such mechanisms by consumers and efficient result-oriented process by providers and regulators alike.

Hence it is important that regulators and DFS providers move beyond the provision of complaint and redress mechanisms to ensure extensive consumers awareness, ease with accessibility, relevance, timeliness and result oriented effectiveness of these mechanisms.

Key recommendations[5]

- **Define DFS relevant provisions in regulatory directives on consumer complaints and redress** to ensure mechanisms are appropriate, accessible, timely and efficient for DFS consumers. Among others it should;
    - Facilitate a structured approach to complaints handling and redress - with primary level focus on Internal Dispute Resolution mechanisms of DFS providers and a secondary appeal focus on External Dispute Resolution by the regulator or independent ombudsman.
    - Encourage the use of digital channels such as social media platforms, website, e-mail, live-chat, text etc. for both IDR and EDR/ADR mechanisms.
    - Mandate provisions in IDR and EDR mechanisms reflect known and potential DFS risks, prioritizing for scope, gravity, and sensitivity of such risks to the consumer and the general financial system.
    - Ensure provisions in both IDR and EDR mechanisms are responsive to vulnerable segments (e.g. Women, illiterate, Persons Living With Disabilities, etc.) in their use of DFS in design, awareness, implementation and reporting.
    - Ensure provisions of guidelines on complaints handling and redress mechanisms involving DFS operated by/involving non-resident / cross border providers
        - **Mandate DFS providers to have an effective Internal Dispute Resolution mechanism in place**. Ensure IDR is "fit for purpose" – reflects the unique scope of the DFS provider's

[5] For more details, please refer to the AFI knowledge product: "Complaint handling in central bank framework" (2020)

product/service, channel, consumers, relevant risks, and volumes of complaints it is likely to receive.
    - Use of algorithms / AI in complaints handling and redress should be subject to robust and standardized frameworks/indicators with provisions for human oversight in sensitive complaints.
- **Institute a reporting framework and guidelines on DFS for both IDR and EDR:**
    - The framework should be standardized in format (e.g. indicators, reporting template, scope of data, scope of reporting etc.) and timeline (periodic).
    - Guideline should encourage to DFS providers to incorporate reported /analyzed data in product/service improvements.
    - Guidelines should facilitate the use of the reports for DFS sector policy guidance
    - Mandate DFS providers and relevant EDR/ADR agencies to publish periodic on complaints and redress, encouraging the use of digital channels for the publication.

- **Facilitate cooperation in complaint handling and redress mechanisms:** In view of the multifaceted nature of some DFS products and services across providers, regulators and cross border jurisdictions the authority(ies) should facilitate a framework for information sharing for effective and coordinated handing and redress of consumer complaints.

4 Guidance on Supervisory and Enforcement Framework

4.1 Guiding Principle: Supervisory techniques and tools specific for DFS

Rationale

DFS has introduced relatively new players, products, services, risks beyond the scope of the traditional/ cash oriented financial sector. These have introduced new dependencies, need for specialized expertise, policy guidance and technology (cybersecurity, AI, etc.) to effectively supervise the growing DFS sector.

Regulators are responding to the changing terrain in DFS supervision with varying approaches, notably the use of technology –supervision technology(suptech). Yet supervision of the fast paced DFS sector remains a learning curve for many regulators, who are yet to reform supervisory frameworks to respond to the expanding scope of DFS within the financial sector. The following outlines some key recommendations to enable regulators reform their supervisory frameworks to be DFS responsive.

Key recommendations

- **Undertake an assessment of existing supervisory tools and techniques for relevance to supervisory needs of DFS industry:** it should cover the
    - The scope and capacity in data collection, aggregation, analysis and reporting.
    - The quality of data collected and reported.
- **Adapt existing supervisory tools to the DFS sector.** Consider interventions such as:
    - innovative technology solutions (suptech and MIS) in artificial intelligence (AI) and machine learning (ML) to enhance efficiency and quality in data collection and analysis as well as proactive supervision. -
    - Investment in DFS relevant technical expertise (e.g.AI/ML, cyber security, data protection etc.) through in-house development or outsourcing.
      Define DFS relevant supervision indicators and guidance on DFS reporting including data dictionaries and taxonomy, to ensure quality and standardization of data.
    - reporting requirement reflective of the DFS industry in the jurisdiction.

- **Adapt existing supervisory techniques to the DFS sector.**
- The authority(ies) to ensure supply side techniques (e.g. market monitoring, onsite and offsite examinations) are:
    - *Risk based: reflect the* risk profile (known and potential) of both DFS providers and consumers to ensure supervision is targeted, efficient. It identifies, assesses and prioritizes risks to be addressed accordingly within a proactive orientation.
    - *Proportionate: techniques are proportionate to the scope and capacity of* DFS provider's and do not impose undue compliance burden on DFS providers, discouraging innovation and expansion to underserved segments.
    - Evidence based supervision: interventions and policies are informed by data from the industry such as demand side surveys, analysis of consumer complaints etc.

- Create thematic benchmarks relevant to the DFS industry in the jurisdiction to guide thematic reviews of the industry Employ periodic demand side surveys, focus group discussions and mystery shopping
- Define relevant techniques for agent network and non-bank e-money issuers reflecting the local environment. This could include but not limited to thematic focus (e.g. anti-money laundering/combating the financing of terrorism (AML/CFT), consumer protection, cybersecurity) *and* blacklisting.

- Explore incorporating of supervisory benchmarks in Regulatory Sandbox and framework for innovation hubs.

4.2 Guiding Principle: Clear and harmonized supervisory governance framework

Rationale

Similar to the regulatory environment, multiplicity of actors in the oversight of DFS sector creates lack of clarity in scope of oversight, overlapping responsibilities, compliance burden on DFS providers among others.

It is therefore important to encourage a well-defined supervisory framework for CP4DFS, through the promotion of interagency cooperation, between relevant agencies.

Key recommendations

- **Promote inter-agency cooperation** among relevant authorities with some level of supervisory oversight on the DFS sector. This could include among others;
    - **An interagency supervisory forum** to facilitate a platform for engagement, knowledge sharing and capacity building (e.g. working groups, workshops etc.) **Define an inter-agency information sharing framework** to facilitate swift, ease of sharing and access to information/ data on CP4DFS among members of the interagency supervisory board. These could include:
        - Establishing a common platform for data reporting either in real time or periodic reporting.
        - Instituting periodic reporting protocols/ requirements for members.
- **Define an effective supervisory framework for CP4DFS** which could cover:
    - Clearly defining the mandate, scope and responsibilities of relevant authorities in the supervision of DFS sector -addressing overlaps, and building synergies for effective supervision.
    - Defining a coordinated framework (tools, techniques, standards, templates etc.) for the joint supervision of the DFS sector to ensure consistency / efficiency in strategy and operations.
- **Consider Industry self-regulation initiatives.** Per relevance to the local supervisory environment, authorities could explore facilitating the DFS industry to commit to voluntary guidelines, practices, standards, peer review and initiatives towards safeguard CP4DFS.

TEXT BOX n.8: Examples of supervision approaches among AFI members

In general, authorities rely on a mix of tools and techniques in the supervision of the financial market. However, the **use of innovative technology solutions to carry out supervision activities for the DFS sector is still quite uncommon**. For instance, among AFI members, only 33% uses the regulatory sandbox tool to develop new products and incorporate consumer protection standards.

For more than half of AFI's members, the regulator supervises the implementation and compliance of established **policies and frameworks** by DFS providers, and 42% has fit and proper **guidelines** for relevant staff within FSP / DFSPs. For instance, during the development phase of products, services or delivery channels, the regulators **review and approve features of DFS/products** (for 65% of the members) or for very few countries, the regulators **supervise pilots or rollout** during the development. In only 23% of countries, there is a regulatory oversight for non-bank digital credit providers, especially fintechs.

In Armenia, for example, the Central Bank uses the **prudential tools of supervision** (manual, matrix on how to assess, define risk profile and rating for DFS providers) and some specific tools from the market conduct supervision. It supervises the market through **regular monitoring on information disclosure** (on a monthly basis, websites, radio and tv advertisement are monitored), and it carries out activities to monitor DFS/clients' behaviors with **mystery shopping or focus groups with clients**.

4.3 Guiding Principle: Effective enforcement mechanism

Rationale

A well-established regulatory and supervisory framework without a credible enforcement mechanism, may weaken the effectiveness of the framework itself.

Hence an effective enforcement system is essential to ensuring adherence to regulations or guidelines on CP4DFS. This guideline advocates robust legal mandate, proportionate powers and adequate enforcement tools and harmonized implementation of enforcement measures for maximum outcome.

Key recommendations

- **Adapt enforcement mandate and tools to the DFS sector**. The authority to incorporate clear legal provisions, operational procedures, relevant institutional structures including capacity (technical and human resource), relevant to the DFS sector.
- **Adopt principles-based approach to enforcement of the DFS sector** to ensure measures do not stifle innovation and growth in the sector but rather support the development of a sound DFS sector. These could include;
    - There is credibility of threat of enforcement.
    - Timeliness of enforcement interventions
    - Proportionality of enforcement interventions, in relation to the gravity of breaches, size of DFS provider and impact of the wider DFS sector.
    - Ensure consistency and non-discrimination in application of enforcement measures across players in the industry in spite of size, scope, products etc.:
- **Promote inter-agency coordination** in the application of enforcement measures within the DFS sector to avoid duplication, and inconsistency in interventions

5 Guidance on Cross Cutting Issues

5.1 Guiding Principle: Promotion of CP principles for vulnerable segments

Rationale

DFS has been successful in connecting vulnerable, underserved / unbanked segments to formal financial services. This has been very instrumental in closing the financial inclusion gap across various jurisdictions.

Nonetheless, the inherent vulnerabilities associated with some segments exposes/ deepens the vulnerabilities to DFS related consumer protection risks. Vulnerable segments include populations exposed to low/poor socio- economic opportunities, per virtue of some inherent characteristics/factors such as gender, income, age, identification, citizenship, ethnicity, among others. Some key vulnerable segments in financial inclusion include but not limited to women, youth, refugees/internally displaced people/undocumented migrants, people living with disabilities for whom the following recommendations have been made. However, each country can identify other typologies of vulnerable groups, such as people living in rural areas, some religious segments (such as Muslims following the Islamic finance principles) among others.

DFS related consumer protection risks have the potential to adversely affect their experience in the use of DFS and their trust in it – deterring their access and usage of DFS thereby derailing the gains in financial inclusion.

Regulators are well placed to safeguard the protection of these segments in the use of DFS by facilitating appropriate CP4DFS interventions with providers and other relevant stakeholders.

Key recommendations

The following agnostic recommendations are made for the consideration of relevant authorities in promoting CP4DFS among general vulnerable segments. It is followed by some specific interventions for identified vulnerable segments.

- Leverage on existing tools (e.g. demand side surveys, complaints, and redress data etc.) to identify relevant CP4DFS risk issues and trends prevalent among identified vulnerable segments.
- Facilitate multi stakeholder approach, including stakeholders beyond the financial sector in the promotion of CP4DFS among vulnerable segments.
- Design relevant, demand driven, and evidence based digital financial literacy and capability interventions for the identified segments with an objective to enhance their knowledge to make informed and secured DFS decisions.
- Define relevant vulnerable segment responsive provisions in prudential and market conduct regulations. Example tiered KYC, guidelines on data profiling, charges/fees etc.
- Encourage DFS providers to adopt relevant behavioral insights of relevant vulnerable segments in the design and delivery products, services and channels.
- Encourage DFS providers to incorporate strategies relevant to vulnerable segments in their consumer awareness, disclosure, marketing, advertisement complaint and redress mechanisms.

Women and girl :

- Utilize Gender Impact Assessments when developing CP4DFS policy and regulation
- Encourage/incentivize the usage of female agents as feasible in a jurisdiction
- Require DFS providers to report data with gender disaggregation

- Support DFS providers to undertake gender sensitive capacity building of their workforce so as to better understand the women's market segments and ensure appropriate products and services are developed for them.

Youth:

- Consider reforming regulatory provisions that define legal age to access DFS (mostly for managing savings accounts, payment transactions, opening an e-wallet) and guidelines on custodial accounts (e.g. define when parents / guardians are needed to transact) to facilitate secure youth financial inclusion.
- Leverage on propensity of youth in the use of technology to drive digital financial literacy and capability interventions through social media, games among others.

Refugees / displaced people:

- Define provisions/ guidelines responsive to the challenges with identification and documentation relevant to refugees/IDPs.
- Define simplified KYC and CDD requirements using a Risk-Based Approach informed by a sound National Risk Assessment, to ensure that lower-risk FDPs are not unnecessarily excluded from lower-risk digital financial inclusion products due to a lack of documentation, proof of address, or wage slips;
- Enhance infrastructure for remittances and ensure robust supervisory framework.

People living with disabilities:

- Encourage DFS providers to make products and services disability friendly.
- Consider incorporating relevant indicators on accessibility and usage by PLWDs in demand side surveys to inform policy and practice.

5.2 Guiding Principle: DFS in disaster / emergency response

Rationale

Global crisis, such as the Covid-19 pandemic or natural disasters conflicts, on the one hand severely stresses economic and financial markets and on the other, pushes DFS to play a very important role, facilitating transactions beyond cash.

Especially in times of crisis the conversion of cash-based Government to People (G2P) welfare transfers or aid agencies' transactions to digital money becomes more imperative. DFS assists the population's access to funds when movements and use of traditional infrastructure are limited. DFS solutions have been central in the financial sector's response to the Ebola epidemics and COVID-19 pandemic.

In these emergency situations, the relaxation of strict prudential market conduct regulations may expose consumers and the financial sector to possible vulnerabilities. Therefore, the regulators have a critical role to play in making sure that the recourse to DFS does not expose consumers to further risks and secondly, that the payment infrastructure is able to cope with the increase in DFS usage (e.g. high traffic / use may lead to breakdowns/efficiency issues, inability of providers to effectively reach physical infrastructures to monitor or repair or increase attacks on ATMs, etc.).

Key recommendations

- **Take prompt interventions towards coordination of response**. The authority to facilitate an interagency coordination with relevant to launch coordinated activities and leverage (where existent) the risk framework on CP4DFS in emergency situations. In jurisdictions without a risk framework to promptly identify, assess and prioritize risks related to CP4DFS;

- **Launch awareness campaign.** The authority to launch/heighten consumer awareness interventions in collaboration with DFS providers to increase public awareness on relevant risk issues and mitigation measures.
- **Ensure emergency interventions are aligned with the consumer protection principles**. The authority when taking emergency interventions to ensure that the basic consumer protection principles are respected despite the relaxation of some regulations. This can include:
  Disclosure and transparency principle:
  - When, for instance, the fees for transactions are reduced or waived (under a certain amount or for any amount) and/or remove/increase limits on mobile transactions, the authority to mandate DFS providers to clearly inform clients about any measures taken: amendments of terms and conditions, length of the measures, any potential risk / consequence, etc.

  Prevention of over indebtedness:
  - When allowing for more relaxed loan disbursement criteria, the authority to mandate DFS providers to still prevent over indebtedness, ensuring that creditworthiness assessment is always carried out (even though in a simplified way).

  Fair treatment:
  - The authority to mandate DFS providers to avoid / ease hardship (e.g. suspending payments of loan installments, plan for rescheduling/restructuring, etc.)
  - When allowing for use of digital signatures and loan disbursements remotely, and relaxing KYC requirements, the authority to mandate DFS providers to avoid any discriminatory practices.

  Product suitability:
  - The authority to implement emergency regulatory measures to enable additional providers (e.g. mobile network operators, social network or e-commerce platforms) to disburse into e-wallets and allow for having more capillary operators.
  - The authority to mandate DFS provider to expand consumer choice and enable provider switching.

  Cybersecurity
  - The authority to mandate DFS providers to strengthen cybersecurity measures to ensure stable and safe connections / systems (above all in a situation where work from remote at home might increase risks of breaches);
  - The authority to ensure security and integrity of the payment infrastructure with regular monitoring activities.
- **Mandate DFS providers to have a Business Continuity plan**. The authority to mandate DFS providers to develop a business continuity plan for liquidity management and provision of services available during emergencies.
- Authority to ensure DFS providers **offer clients an appropriate and easy channel/mechanism for complaint and redress.**
- After/at the end of disasters or emergency, authorities to ensure **effective consumer awareness on changes /reversion of policies** to prevent fraud and ensure consumers make informed decisions post the period.

Annex 1. Main global initiatives that define CP4DFS

AFI Knowledge products on CP4DFS

Within the past decade, AFI's DFSWG (Digital Financial Service Working Group) and CEMCWG (Consumer Empowerment Market Conduct Working Group) have committed to the development of relevant knowledge products on DFS[6].

Within these knowledge products, many **consumer protection principles and regulatory implications were also addressed.** In a few cases (see table below), these cover many consumer protection principles with a good level of detail and provide practical guidelines for the regulators. Other studies have a stronger focus on a single topic, such as, the one on disclosure and transparency or those related to complaint and redress mechanisms. Others cover a transversal regulatory area, such as, market conduct, without considering prudential regulation. With the increasing convergence between DFS and CP, AFI members acknowledge the need to synthesize the relevant key principles across these knowledge products into a specialized policy guidance for their financial markets which are progressively transitioning to DFS.

The two tables below present a codification of the main AFI knowledge products over key categories of consumer protection (in blue):

	Complaint handling in central bank framework (2020)	Disclosure and transparency (2020)	Policy Model for e-money (2019)	Cybersecurity for financial inclusion (2019)	Digitally Delivered Credit (2017)
Policy and regulatory environment	x	X			x
Privacy and security			x	x	x
Product suitability			x		
Fair treatment			x		x
Internal control			x		
Digital financial education			x		
Disclosure and transparency		X	x		x
Complaints and redress	x		x		x
Supervision and enforcement		X	x		x
Vulnerable segments			x		

	Market conduct supervision of financial service provides (2016)	Consumer Protection in Mobile Financial Services (2014)	Help and redress for financial consumers (2013)	Trust law protections for e-money customers (2013)
Policy and regulatory environment	x		x	
Privacy and security	x	x		
Product suitability	x	x		
Fair treatment	x	x		
Internal control	x	x		x
Digital financial education		x		
Disclosure and transparency	x	x		
Complaints and redress	x	x	x	
Supervision and enforcement	x			
Vulnerable segments				

Table 3. Codification of some AFI knowledge products in terms of CP principles and regulatory, supervisory framework

[6] A comprehensive list of AFI knowledge products reviewed is available in Annex 3.

International standards for CP4DFS

In building this policy model and its related guidance areas, a wide literature on CP4DFS has been taken into consideration with the objective to design a comprehensive framework specific for regulation on CP4DFS.

Among the **most notable initiatives on CP4DFS** with a regulatory perspective launched by internationally recognized stakeholders, the following are worth mentioning (*from the most recent*):

- Consultative Group to Assist the Poor (CGAP): Consumer Protection Regulation in Low-Access Environments (2020)
- Bill and Melinda Gates Foundation (BMGF): Inclusive Digital Financial Services – A Reference Guide for Regulators (2019)
- Center for Financial Inclusion (CFI): Handbook on Consumer Protection for Inclusive Finance (2019)
- International Telecommunication Union (ITU): Regulation in the Digital Financial Services Ecosystem (2017)
- World Bank (WB): Good Practices for Financial Consumer Protection (2017)
- UNSW: The Regulatory Handbook: The Enabling Regulation for DFS (2015)
- Organisation for Economic Co-operation and Development (OECD): Consumer Policy Guidance on Mobile and Online Payments (2012)
- G20: High level Principles on Financial Consumer Protection (2011)

Among the initiatives that rather have a market perspective (actions to be taken by DFS providers to protect the consumers), it is worth mentioning (*in alphabetic order*):

- Better Than Cash Alliance (BTCA): Responsible Digital Payments Guidelines (2016)
- Consumer Financial Protection Bureau (CFPB): Consumer Protection Principles (2017)
- GSMA: Code of Conduct for Mobile Money Providers (2017)
- Smart Campaign: Client Protection Principles - updated with digital finance standards (2017)

Annex 2. Key Concepts and Definitions[7]

Digital Financial Service	Financial services that relies on use of technology (mobile phones or other devices). This includes both transactional and non-transactional services, such as viewing financial information on a user's mobile phone. Examples: **First generation DFS**: deposit, withdrawal, money transfer, loan repayment/disbursement, utilities payment (electricity, water bill), airtime top-up, merchant payment, labor (pension, salary payments), social payment (health, social transfer, tax payments), interconnection between a mobile money solution and an FSP (bank to wallet transfer or wallet to bank), remittances, e-commerce. **Second generation DFS**: Instant and automated short term/30-day loan, savings product, insurance.
Digital Financial Service Providers	Financial institution that uses technology / mobile phones to access financial services and execute financial transactions.
KYC and e-KYC	A set of due diligence measures undertaken by a financial institution, including policies and procedures, to identify a customer and the motivations behind his or her financial activities. e-KYC refers to online procedures (remote and paperless process)
Financial capability and digital financial capability	**Financial capability** is the combination of attitude, knowledge, skills, and self-efficacy needed to make and exercise money management decisions that best fit the circumstances of one's life, within an enabling environment that includes, but is not limited to, access to appropriate financial services.[8] It goes beyond the idea of financial literacy or financial education (increasing knowledge on specific terms and concepts), and it refers to the capacity of taking informed decisions (importance of planning and saving for instance). **Digital financial capability** refers to the capacity of costumers to use information and technologies to make financial transactions, being aware of risks, potential fraud, etc.
Privacy policy	It refers to confidentiality and privacy policy and procedures on gather, process, usage, distribution and storage of clients' data
Third party provider	Agents and others acting on behalf of a mobile financial services provider, whether pursuant to a services agreement, joint venture agreement, or other contractual arrangement.
Traditional cash-based financial market	Microfinance and banking systems (including all kind of financial service providers regardless licensing, microfinance institutions, deposit taking, cooperatives and credit unions, etc.) that provide products and services through delivery channels primarily cash-based with face-to-face meeting.

[7] Based on definition from "Guideline Note Mobile Financial Services: Basic Terminology", AFI (2012) and consultants' re-elaborations.
[8] Center for Financial Inclusion – ACCION definition.

Annex 3. Reference publications

AFI knowledge products:

- Consumer Protection in Mobile Financial Services (2014)
- Complaint handling in central bank framework (2020)
- Cybersecurity for financial inclusion: Framework & Risk Guide (2019)
- Digitally Delivered Credit: Consumer Protection Issues and Policy Responses to New Models of Digital Lending (2017)
- Driving Change in Financial Inclusion through Innovation in Africa (2017)
- Experiences in the Implementation of the Principle of Disclosure and Transparency in AFI Member Countries - Series 1: Credit Products (2020)
- Mobile Financial Services: Basic Terminology
- Help and redress for financial consumers (2013)
- Market conduct supervision of financial service provides – A Risk-Based Supervision Framework (2016)
- Policy Model for e-money (2019)
- Policy Framework for Responsible Digital Credit (2020)
- Trust law protections for e-money customers (2013)

Other publications

- Bill and Melinda Gates Foundation (BMGF): Inclusive Digital Financial Services – A Reference Guide for Regulators (2019)
- Better Than Cash Alliance (BTCA): Responsible Digital Payments Guidelines (2016)
- Center for Financial Inclusion (CFI): Handbook on Consumer Protection for Inclusive Finance (2019)
- CFI: What Is "Financial Capability?"
- Consultative Group to Assist the Poor (CGAP): Consumer Protection Regulation in Low-Access Environments (2020)
- CGAP: COVID-19: How Does Microfinance Weather the Coming Storm? Greta Bull, Timothy Ogden (2020)
- Consumer Financial Protection Bureau (CFPB): Consumer Protection Principles (2017)
- Digital Financial Services Go a Long Way: Transaction Costs and Financial Inclusion (2018) - Pierre Bachas, Paul Gertler, Sean Higgins, Enrique Seira
- G20: High level Principles on Financial Consumer Protection (2011)
- G20/OECD: Financial Consumer Protection Approaches in the Digital Age (2018)
- GSMA: Code of Conduct for Mobile Money Providers (2017)
- International Telecommunication Union (ITU), Focus Group DFS Main Recommendations (2017)
- ITU: Regulation in the Digital Financial Services Ecosystem (2017)
- McKynsey: Digital Finance for All: Powering Inclusive Growth in Emerging Economies (2016)
- Organisation for Economic Co-operation and Development (OECD): Consumer Policy Guidance on Mobile and Online Payments (2012)
- OECD: Effective Approaches for Financial Consumer Protection in the Digital Age: FCP Principles 1, 2, 3, 4, 6 and 9 (2019)
- OECD: Digitalisation and Financial Literacy (2018)
- Social Performance Task Force (SPTF): Serving Refugee Populations: The Next Financial Inclusion Frontier (2016)
- Smart Campaign: Client Protection Principles - updated with digital finance standards (2017)
- UNSW: The Regulatory Handbook: The Enabling Regulation for DFS (2015)
- World Bank (WB): Good Practices for Financial Consumer Protection (2017)
- WB, CGAP, International Policy, GiZ, Australian Aid: G2P Payments in COVID 19 context: Key areas of action and experiences from country emergency actions (2020)
- WB Global Findex data