afi

CONSUMER EMPOWERMENT AND MARKET CONDUCT (CEMC) WORKING GROUP

DIGITAL FINANCIAL SERVICES (DFS) WORKING GROUP

POLICY MODEL ON CONSUMER PROTECTION FOR DIGITAL FINANCIAL SERVICES

POLICY MODEL

CONTENTS

EXECUTIVE SUMMARY

In the last decade, digital financial services (DFS) has registered fast-paced growth that has contributed to the expansion of financial inclusion. This progress has not come without drawbacks – specifically Consumer Protection (CP) related risks. Though most regulators have instituted regulations on consumer protection for the wider financial market, the unique peculiarities of DFS necessitates relevant reforms/adaptations to existing regulations, to reflect on 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 AFI knowledge products developed over the decade, coupled with best practices within the AFI network, in a policy model on Consumer Protection for DFS (CP4DFS).

As part of the process, reference was also made to relevant policy guidance from other policy stakeholders.

Accordingly, this policy model (PM) has been developed around

FIVE GUIDANCE PILLARS, namely:

1 POLICY AND REGULATORY ENVIRONMENT

See page 4

2 PRODUCT DEVELOPMENT AND SERVICE DELIVERY

See page 5

3 CONSUMER AWARENESS, COMPLAINT AND REDRESS

See page 6

4 SUPERVISION AND ENFORCEMENT

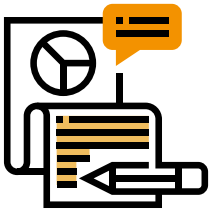
See page 7

5 CROSS CUTTING ISSUES

See page 8

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

GUIDANCE AREAS OF THE PM FRAMEWORK WITH THEIR MAIN GUIDING PRINCIPLES AND KEY RECOMMENDATIONS.



1. GUIDANCE ON POLICY AND REGULATORY ENVIRONMENT

1.1.

Clear DFS relevant legal and regulatory provisions in CP frameworks

HIGHLIGHT OF KEY RECOMMENDATIONS

- Undertake a diagnostic analysis on CP4DFS.
- Undertake DFS responsive CP policy design.
- Design DFS provisions that are driven by evidence-based and risk-based approaches.
- Incorporate DFS provisions into existing CP policies.
- Synthesize and harmonize key DFS-specific legal mandates and regulatory provisions into a compendium/regulatory framework on CP4DFS.

1.2.

Clear and harmonized governance framework

HIGHLIGHT OF KEY RECOMMENDATIONS

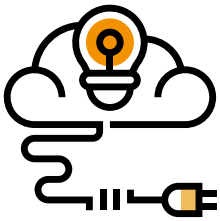
- Facilitate a dedicated inter agency CP unit for DFS.
- Facilitate inclusion of CP4DFS on the agenda of financial sector boards/national payment systems councils.
- Define and harmonize specialized regulatory, supervisory and dispute resolution oversight strategy on CP4DFS.
- Define inter-agency information sharing framework.

1.3.

Clear legal/regulatory framework for regulating market competitiveness

HIGHLIGHT OF KEY RECOMMENDATIONS

- 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

HIGHLIGHT OF KEY RECOMMENDATIONS

- 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

HIGHLIGHT OF KEY RECOMMENDATIONS

- Develop a cybersecurity framework with sector-specific provisions within the principle of proportionality.
- 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.
- Facilitate a framework for engagement with external regulators and supervisors on non-resident DFS providers.

2.3.

Fair treatment and responsible business conduct

HIGHLIGHT OF KEY RECOMMENDATIONS

- Encourage the development of an industry code of conduct.
- Ensure the code of conduct highlights ethical principles and practices.
- Set responsible lending practices for delivery of digital credit through:
  - Clear legal mandate and regulatory framework
  - Appropriate institutional capacity
  - Comprehensive and effective credit referencing systems to address over indebtedness
  - Interventions to address predatory lending by digital credit providers - interest caps/ceiling, innovative non-predatory interest regimes (e.g. cash-back incentive, future interest rate reduction, customization of interest, etc.).
- Transparency and disclosure 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).

2.4.

Product suitability: customer centricity, inclusiveness, relevance and usability

HIGHLIGHT OF KEY RECOMMENDATIONS

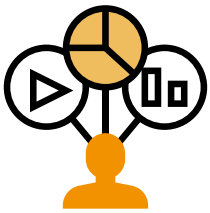
- Incorporate CP4DFS provisions in product development, adopting a customer-centric approach.
- Define measures to build an inclusive marketplace and ensure clients' access and mobility.
- Facilitate progressive customer due diligence - tiered KYC models.

2.5.

Adoption of risk management approach

HIGHLIGHT OF KEY RECOMMENDATIONS

- 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 REDRES

3.1.

Promotion of digital financial literacy and capability

HIGHLIGHT OF KEY RECOMMENDATIONS

- 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, prevention, mitigation, complaints and redress.
- DFL& C interventions should be evidence-based.
- Authority(ies) to communicate/disclose (e.g. via websites, or periodically via social and traditional media) approved and blacklisted DFS providers, permissible digital services/products, etc.

3.2.

Responsible marketing / advertisement and sales (disclosure and transparency)

HIGHLIGHT OF KEY RECOMMENDATIONS

- Facilitate suitability of digital communication through customer-centric features, appropriate language and relevant digital tools (e.g. digital calculators).
- Provide principle-based guidance on format and manner for responsible marketing/advertisement/ sales.
  - Effective transparency and disclosure
  - Use of appropriate language
  - proportionate and not restrictive to creativity in marketing/advertising and does not place undue cost in implementation.
- Consider/include provisions for a standardized price reporting to a central and public database to promote transparent comparison of DFS providers.

3.3.

Mechanism to ensure complaints and redress resolution

HIGHLIGHT OF KEY RECOMMENDATIONS

- Define DFS relevant provisions in regulatory directives on consumer complaints and redress.
- Mandate DFS providers to have an Internal Dispute Resolution (IDR) mechanism in place.
- Institute reporting guidelines for both IDR and EDR.
- Facilitate cooperation in complaints handling and redress.
- Where feasible, as national jurisdiction permits and per the maturity of the DFS industry within the jurisdiction, consider a specialized DFS unit within national independent dispute resolution body or the EDR office for the financial sector/regulator.
- Regulators to consider adopting technology for complaints management -
  e.g. chat box, interactive videos etc.

4. GUIDANCE ON SUPERVISION AND ENFORCEMENT

4.1.

Supervisory techniques and tools specific for DFS

HIGHLIGHT OF KEY RECOMMENDATIONS

- Undertake an assessment of existing supervisory approaches, tools and techniques for relevance to supervisory needs of DFS industry.
- Adapt existing supervisory tools to reflect the DFS sector.
- Ensure supervisory approaches, tools and techniques reflect DFS relevant principles.
- Create supervisory benchmarks for key thematic areas relevant to the DFS industry (e.g. data protection, cyber security, agents, IT, outsourcing, etc.) in the jurisdiction.
- Authority(ies) to monitor unregulated DFS to inform review of regulatory perimeters and provisions.

4.2.

Clear and harmonized supervisory governance framework

HIGHLIGHT OF KEY RECOMMENDATIONS

- Promote inter-agency cooperation among relevant authorities with supervisory oversight on the DFS sector.
  - An inter-agency supervisory forum
  - Define an inter-agency information sharing framework
  - Establish a common platform for data reporting
  - Standardize the supervision of core DFS thematic issues, such as data privacy and protection, cyber security, KYC, fair treatment and business conduct, etc.

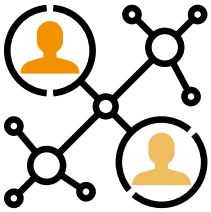
4.3.

Effective enforcement mechanism

HIGHLIGHT OF KEY RECOMMENDATIONS

- Adapt enforcement mandate and tools to DFS sector.
- Adopt principle-based mechanisms.
- Promote inter-agency coordination for enforcement.
- Consider public disclosure of enforcement actions (particularly sanctions) to encourage adequate conduct by DFS providers.

5. GUIDANCE ON CROSS CUTTING ISSUES



5.1.

Promotion of CP principles for vulnerable segments

HIGHLIGHT OF KEY RECOMMENDATIONS

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 promote 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

HIGHLIGHT OF KEY RECOMMENDATIONS

- Take prompt interventions towards coordinating response.
- Launch awareness campaign.
- Ensure emergency interventions are aligned with the CP principles.
- Ensure relaxation of regulations does not adversely affect requirements on adequate authentication.
- Mandate DFS providers to have a Business Continuity plan.

BACKGROUND AND CONTEXT

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 in Table 1 below.

Emerging trends across financial markets indicate that these risks have the potential to adversely impact the trust of consumers, destabilize financial markets, and 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.

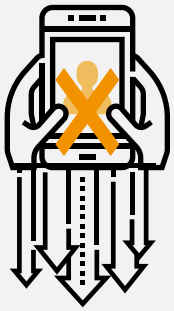
In line with this, the DFSWG and the CEMCWG committed to synthesize and harmonize learnings, best practices and policies from its relevant knowledge products, and across the network, into a recognized policy model.

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.

TABLE 1: SUMMARY OF THE MAIN CP4DFS RELATED RISKS FROM DEMAND, SUPPLY AND REGULATORY PERSPECTIVES

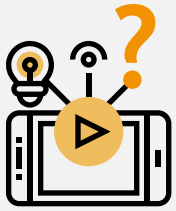
DEMAND SIDE

- Asymmetry of information
- Inadequate digital financial literacy and capability
- Over-indebtedness (for digital lending)
- Poor trust in DFS providers
- Poor trust in agent networks
- Illiteracy (literacy and numeracy).



SUPPLY SIDE

- Products not tailored to clients' needs and/suitability
- Misleading communication
- Lack of transparency
- Unfair/excessive pricing
- Aggressive commercial practices
- Fraud/theft and scams
- Data breach
- Lack of or ineffective recourse mechanism
- Inadequate safeguarding of consumer rights
- Inadequate mechanisms for clients' feedback.

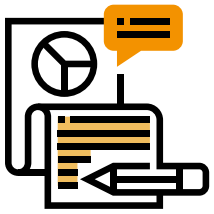


REGULATORY SIDE

- Regulatory framework not tailored to the DFS sector
- Weak consumer protection laws
- Poor redress system
- Inadequate capacity to identify existing and new CP4DFS risks
- Inadequate supervisory capacity
- Regulatory overlaps - uneven regulation, arbitrage, overregulation.

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 electronic money and transaction accounts to credit, savings, investment, insurance, cross border remittances, services that facilitate consumer's comparison, understanding, access, use, management of financial products, among others. 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, by entrenching DFS within consumer protection regulatory frameworks. It highlights the need to consciously identify, define and incorporate relevant DFS 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 relevant DFS industry 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(ies) 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.** To reform/amend existing policies or develop new consumer protection policies to be responsive to the DFS industry within the principle of technology neutrality. The main objective is to reflect the existing, as well as projected, DFS landscape with its associated risks, addressing demand, supply and regulatory perspectives.

> **Design DFS provisions driven by evidence-based and risk-based approaches.** The authority(ies) 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.

- provisions to follow a risk-based approach, responsive to existing and projected product portfolio delivery channels and innovation.
- Utilize both supply-side (e.g. analysis of procedures, etc.) and demand-side research (e.g. focus groups, surveys, mystery shopping) to better understand consumer and DFS provider insights.

> **Ensure DFS relevant principles-based approach to the development of CP4DFS policies.** This should include but not limited to the principle of "technological neutrality" (i.e. ensuring that regulatory responses are neutral in terms of the way that a product or service is distributed) and "proportionality" (i.e. ensuring that regulatory responses reflect the business model, size, systemic significance, as well as the complexity and cross-border activity of the regulated entities).

> **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 e-KYC, among others.

- Irrespective of the model that is implemented in a jurisdiction, regulators should review consumer protection policies through a DFS lens. They should design and integrate/incorporate DFS-specific

provisions to address gaps across the various legal mandates and regulatory instruments.

> Where feasible and where existing regulatory frameworks do not adequately address DFS-specific issues or present a fragmented and ambiguous scope, jurisdictions could consider synthesizing and harmonizing key DFS-specific legal mandates and regulatory provisions into a compendium/regulatory framework on CP4DFS. This should be horizontal within the principle of technology neutrality.

> Should a regulator choose to either incorporate DFS-specific provisions into existing consumer protection polices or create a compendium of regulatory provisions on CP4DFS, the following should be ensured:

- **Harmonization of existing provisions:** Where feasible, regulators should identify and harmonize possible duplications and contradictory provisions across various DFS-relevant legal mandates, policies, or regulatory provisions. The objective is to avoid fragmentation of relevant regulatory provisions on CP4DFS, address unnecessary complexities, ambiguities, and conflicts in the interpretation and oversight of policies.
- **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 framework.
- **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/regional industry/thematic standards/ policy guidance (e.g. from standard setting bodies, industry associations, etc.) and best use cases within the local context. These could include but are not limited to, globally recognized standards/guidance on data protection, cloud computing, cybersecurity, credit referencing, e-money, and deposit insurance, among others.

BOX 1: 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 has been developing a Consumer Protection framework that integrates DFS.

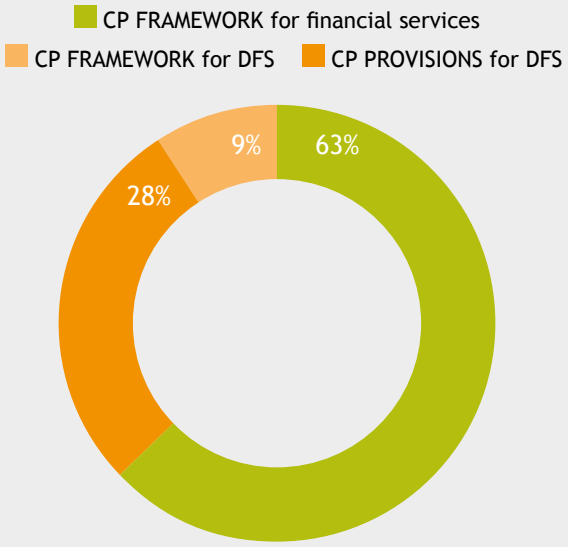
With the increasing attention on financial inclusion, the National Government developed the Financial Sector Development Strategy 2018-2030 and the National Financial Inclusion Strategy 2016-2020. Consumer protection provisions were incorporated in both strategies. In 2018, the report by the Treasury commissioned a 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, and 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.

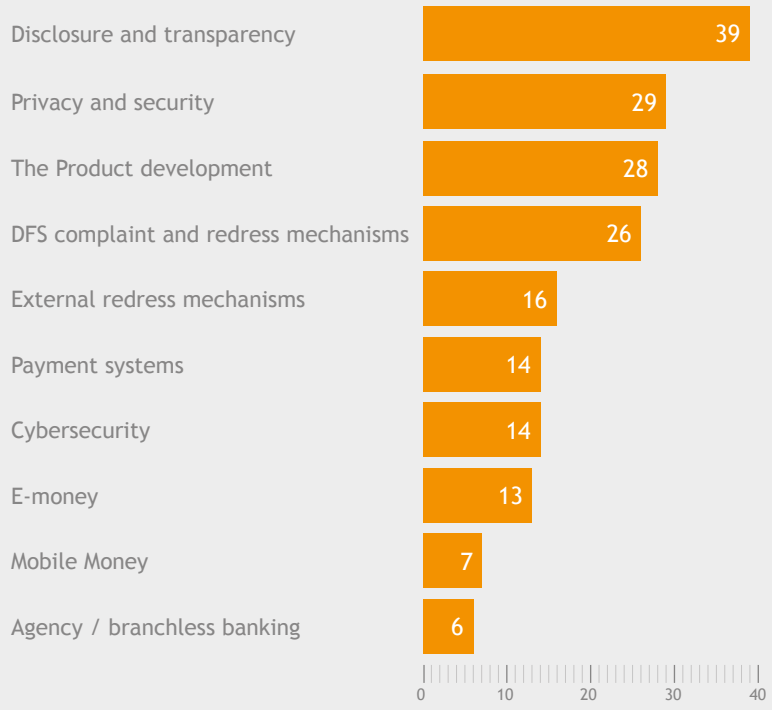
Regulations, which were initially based on an institutional approach, were revised to a product-based approach to include all the miscellaneous and unregulated financial institutions present in the country, which hitherto were not under the oversight of the Central Bank.

BOX 2: CP4DFS POLICY MEASURES IN PLACE ACROSS AFI MEMBERS

Regulators are showing a 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.

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, supervisory oversight and dispute resolution mandate are 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 regulation, supervision oversight and dispute resolution may be 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.

Though there are some known interventions in the coordination within the financial sector on market conduct and consumer protection, through financial sector committees/councils on safety, soundness and stability issues, it is not widely reported within the network. As DFS deepens to significant proportions within markets, it will be apt to encourage regulators to consider adapting such committees/councils in the coordination, harmonization, planning, implementation and supervision of CP4DFS to ensure consistency and efficiency in the use of resources and maximum impact. The objective of this guidance is to address the incidence of fragmentation in policy development and implementation across varying organizations/agencies, and their related policies.

KEY RECOMMENDATIONS

> **Facilitate a dedicated inter-agency Consumer Protection unit for DFS.** Where feasible and per the maturity of the DFS industry and depth of DFS-related risk issues within a jurisdiction, the authority(ies) to facilitate the development of an inter-agency unit on CP4DFS to drive a coordinated and specialized approach on CP4DFS. Among others it could also address any possibilities of regulatory overlaps. This unit should have a clear legal mandate to address CP4DFS, with the clear 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 unit is 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 established as:

- A dedicated unit/department for DFS under the financial service regulator.
- A unit within an independent consumer protection agency (with oversight of the financial sector).
- A unit within a dedicated market conduct authority for financial services.

> **Facilitate inclusion of CP4DFS on the agenda of financial sector boards/national payment systems councils.** Where feasible and per the maturity/depth of the DFS industry within the financial sector of a jurisdiction, the authority to encourage the inclusion of CP4DFS within the agenda/focus of financial sector boards/national payment councils. This could include but not limited to incorporating key CP4DFS relevant indicators/issues within the oversight agenda of the board.

- In jurisdictions with Financial Sector Consumer Protection (FCP) boards, authorities to ensure that CP4DFS is entrenched. This could include but not limited to the creation of a working group on CP4DFS, which should include relevant non-financial sector regulators, such as telecommunications, data protection authorities, as well as relevant consumer associations.
- In jurisdictions without FCP boards, regulators to consider initiating an inter-agency committee/ working group of relevant financial sector and non-financial sector players on CP4DFS.

> **Define and harmonize regulatory, supervisory and dispute resolution strategy on CP4DFS.** The inter-agency CP4DFS working group should seek to ensure harmonization in the development and implementation of policies and interventions on CP4DFS across the DFS sector. This could include reviewing strengths of the mandate, responsibility and capacity, and assign the thematic leadership to reflect the capacities of its members. Identified leader of a thematic area/focus could be an individual institution or more. In the case where more than one institution is assigned leadership of

a thematic issue, authorities need to ensure a clear and result-oriented responsibility framework for all players within the 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 relevant agencies, including consumer associations where relevant 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.

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. This may position some providers in a competitive advantage within the market. With the multifaceted characteristic feature of DFS, 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 and/or dominate market share. In 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.

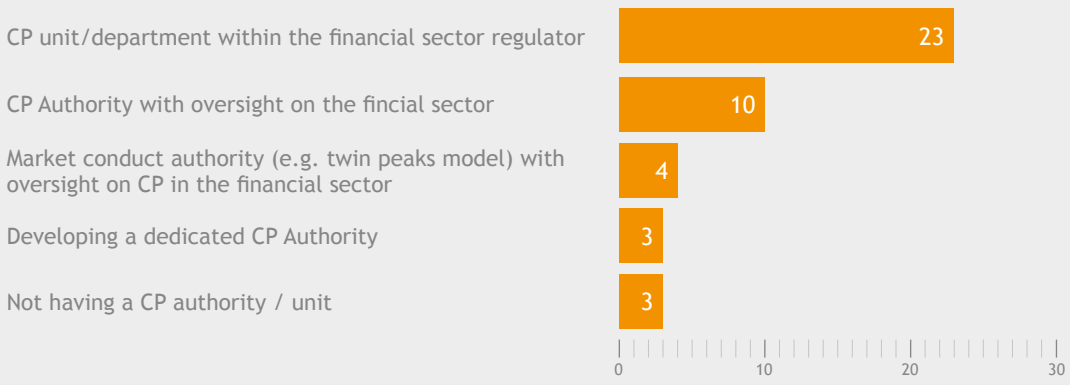
KEY RECOMMENDATIONS

> Facilitate a level playing field for DFS providers to foster healthy competition. Authority(ies) to consciously facilitate a level playing field within the

BOX 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.

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.
- Regulators to ensure fair access to payment settlement systems through fair pricing to enhance fair access for non-bank e-money providers.
- Regulators to work towards achieving interoperability without significant price difference by the growth stage of the DFS market.
- In accordance with the accommodation of domestic jurisprudence, regulators to discourage the practice of agent exclusivity/vertical restraints, especially in emerging DFS markets.

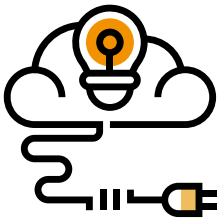
> Define measures to prevent monopolistic and anti-competitive behaviors. The authority to adopt measures to prevent monopolistic and anti-competitive behaviors by dominant players. This should be implemented in collaboration with the competition authority in the jurisdiction to closely monitor anti-competitive measures and other instances of market abuse.

- Authorities to ensure that regulation of monopoly reflects the maturity of the DFS market. Emphasis should be on addressing challenges to market entry (for others beyond the dominant provider) and abuse of dominant power. This is important to ensure that regulation of monopoly does not unduly discourage/stifle infrastructure and market expansion by DFS providers, which can have adverse effects on financial inclusion.

> Acknowledge the deepening role of data ownership in creating uneven playing fields/market monopoly and define regulatory provisions to address unfair data-led monopoly. This could include/address;

- Entry, access, management, and storage (localization and cross boarder flows of data) of data by Big Techs.
- Specific guidance on data sharing to regulate access, control and usage of consumer data, e.g. portability of data to enable consumer records to be sent from one provider to another, thus promoting competition.

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, e.g. in the 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 maintain the protection of the customers' fundamental rights.

KEY RECOMMENDATIONS

> **Integrate provisions on data privacy and protection into existing related policies**. Through consultative processes with the DFS industry, the authority(ies) 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 financial sector authority(ies) to have specific provisions for

big data, AI, IT outsourcing, open banking, biometric identification, cross-border data flows and cloud-based storage (oversight of non-resident providers and cross-border data transfers).

- Benchmark provisions to relevant regional and international data protection laws, e.g. GDPR and national best practices (e.g. such as that of Malaysia and Brazil).

> **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 and 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 and protection 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 and consent.** Among others, the authority(ies) to define a detailed guidance for consumer awareness, such as:

- Obligation to adequately inform clients on particulars of data being collected/stored by DFS providers, how the data is secured, distributed and reported, and ensured of their understanding.
- Consumers' right to access their data and dispute inaccuracies.
- 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.
  - Regulators could consider placing the burden to protect data on providers through provider usage restrictions. This could limit the use of data to the customer's interest (fiduciary duty).
- Obligation to secure clients´ consent before data/information is used and shared with third-party entities (such as, central banks, 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 client's consent for data sharing.

Authority(ies) to facilitate a framework for engagement with external regulators and supervisors on the extension/coordination of supervision for non-resident DFS providers.

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-incomed 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 DFS sector-specific provisions.** The authority(ies) to harmonize legal and regulatory provisions into a framework for DFS providers. It should follow principle-based approaches (including technology neutrality),

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

referencing international standard frameworks, and be adapted to the local environment and trends.

- Ensure the framework is proportionate and risk-based to avoid expensive and expansive requirements that negatively affect low-margin DFS businesses and evolving ecosystems.

> The authority to have a defined 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 the 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.
- Institute periodic engagement between DFS providers and regulators to deliberate on emerging issues, increase awareness and develop coordinated response strategies.
- Establish an industry-wide Cybersecurity Operations Centre (CSOC) and Computer Emergency Response Team (CERT).
- Facilitate cooperation between the established national CSOC/CERT and regional/international CSOC/CERT.

> **Mandate DFS providers to have internal cyber security policies, processes, and incident response plan:** 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.
- Set minimum regulatory requirements/directives to safeguard the integrity of operating systems and technologies. This could include but not limited to:
  - Robust authentication protocols, e.g. single-factor authentication for lower value transactions or simple account viewing, but multiple factors (including biometrics) considered for account changes and initiating larger transactions, etc.
  - Data Privacy and Protection – minimum standards on encryption, effective authorization by staff of provider, selections of cryptographic algorithms, key lengths, key management tools, etc.
  - Active, automated transaction monitoring and alert functions for the detection and prevention of fraud.
  - Vulnerability assessment and penetration testing.
  - Appointment of focal points to supervise internal strategies – e.g. a Fraud Officer for smaller businesses and a Chief Information Security Officer (CISO) for larger organizations with a market share of above 10 percent.

> **Mandate regular and incident reporting.** The authority(ies) to mandate DFS providers to deliver regular and incidents reporting on cyberattacks, disruption of services and data breaches, with redress actions undertaken and timeframes involved. Ensure reporting requirements be guided by the principle of proportionality to prevent undue burden on small DFS businesses.

BOX 4: CYBERSECURITY MEASURES: THE CASE OF GHANA

In 2018, Bank of Ghana[2] released the cybersecurity framework "Cyber and Information Security Directive", which defined 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 For more details, please refer to AFI knowledge product "Cybersecurity for financial inclusion: Framework & Risk Guide" (2019)

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, with many signing up for a DFS to represent 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, resulting in a 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(ies) to encourage the incorporation of DFS-specific provisions in existing financial sector industry code of conduct or the development and adoption of an industry Code of Conduct, by new industry players such as FinTechs, etc. It should reflect broadly-recognized principles (e.g. integrity, transparency, fairness, confidentiality, etc.) for developing a safe and responsible CP4DFS environment. This would ensure DFS service providers to take ownership of the process; being actively involved in the identification of risks and definition of mitigation practices; and being 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.

- The Code of Conduct should be public and should be periodically evaluated by the regulator and the relevant industry association, and evaluations should be public, as well and open to comments.
- Codes should include provisions and penalties for non-compliance, monitored by the industry (autoregulation).
- The Code of Conduct should cover fair pricing, terms and conditions - agent due diligence, and prudent outsourcing, among others.
- Regulator should require DFS providers to ensure that the COC is known and applied by their agents, and other third parties.
- Where feasible, encourage DFS providers (specifically, those with footprints across multiple jurisdictions within a region) to pursue an industry-wide Code of Conduct at the regional/sub regional levels, to facilitate the streamlining of CP4DFS standards across the region/sub region.

B) Ensure the Code of Conduct highlights ethical principles and practices.

Authorities to require/encourage DFS providers to include ethical principles in its internal Code of Conduct Ethics towards the fair and respectful treatment of clients. It should 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 avoiding discrimination, with attention towards vulnerable segments, such as women or people with disabilities, avoiding conflict of interest, privileged information, and 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).
- Avoiding 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 the 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 the delivery of small loans through digital means, regulators should consider

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)

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.

- Mandate that digital credit providers use the credit reference systems, to reduce the risk of over indebtedness. Also, due consideration should be given to the costs associated with credit reporting and referencing, as well as the adverse consequences of negative listing of small ticket loans.

> **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).

> Address predatory lending by digital credit providers through specific interventions such as:

- Set interest caps/ceiling – low income/ economically vulnerable segments should be taken into consideration when setting these caps/ceiling.
- Through industry collaboration, include moral suasion to encourage/facilitate the use of innovative non-predatory interest regimes by DFS providers. This could include but not limited to:
  - incentive-driven interest structures such as 'cash back incentive' and future interest rate reduction.
  - Customization of interest, especially for vulnerable segments.

BOX 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 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 the innovation of DFS per scope of products, services, delivery channels, use cases, etc., continually extends 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

> **Facilitate a customer-centric approach to development of DFS.** The authority(ies)to consider any of the following approaches per relevance to their jurisdictions in the development of products and delivery channels:

- Pro-actively mobilize data on suitability throughout the customer journey through both supply and demand side research and tools.

- Product approval approach: the regulator to intervene in reviewing/approving DFS product features (terms and conditions), including subsequent changes, defining a list of prohibited products/services and features (e.g. bundling products).
  - encourage minimum product features to ensure innovations can support financial inclusion and is responsive to the market.
- Principle-based approach: the regulator to require providers to adhere to identified principles (e.g. data protection and privacy, disclosure/ transparency, affordability, etc.) 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).
  - To encourage affordability, the regulator to facilitate/guide scope of pricing with ceilings/ caps to DFS products and services through industry collaboration and other interventions, including moral suasion.
- Testing approach: the regulator to incorporate product suitability indicators in regulatory sandbox, innovation hub interventions, etc. for the testing of new products.

> **Define measures to build an inclusive marketplace and ensure clients' access and mobility.** The authority(ies) to adopt measures to build an inclusive marketplace and ensure clients' access and mobility through:

- Facilitating the interoperability of the payment system infrastructure.
- Reducing 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(ies) 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/simplified customer due diligence – tiered Know Your-Customer (KYC) models:** The authority(ies) 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 development 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

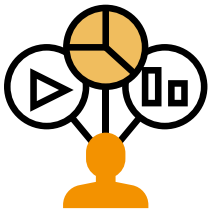
> **Mandate DFS providers to have an internal risk management framework.** The authority to require DFS providers to develop a risk management framework which could include:

- A risk measurement framework to identify, assess and prioritize risks related to CP4DFS.
- A reporting and management information system that allows for identification and measurement of consumer protection/conduct risks and outcomes.
- An appropriate management structure satisfying the 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 (within the principle of proportionality) 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).
- Provide guidance on the management of dormant DFS accounts.

3. GUIDANCE ON CONSUMER AWARENESS, COMPLAINT AND REDRESS



3.1 GUIDING PRINCIPLE: PROMOTION OF DIGITAL FINANCIAL LITERACY AND 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 specific demographics or segments with vulnerabilities, in relation to financial inclusion; these will need specialized interventions to build their literacy and 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. This 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 Literacy and Capability strategies:** Establish strategies and interventions to promote the knowledge of DFS, awareness of the risks and its prevention, consumer rights, responsible complaint and redress procedures (digital financial literacy), as well as the confident and informed application of this knowledge into sustainable attitudes and skills, for

the effective and secured use of DFS (digital financial capability). This should also cover vulnerable groups such as women, youth, the elderly, migrants, and 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, and the media, among others.

- Authority(ies) to consider adopting a 360-degree approach to digital financial literacy and capability. This will create awareness for end users, service providers and regulators.

> **Encourage DFS providers to incorporate digital financial literacy and capability in product advertisements** and campaigns and contribute to industry-wide digital financial literacy and capability programs.

- DFS providers can also be encouraged to promote unbiased content on DFL&C, including through industry-wide consumer awareness interventions.
- The authority(ies) to monitor and ensure that digital financial literacy messages included in advertisements are accurate and appropriate.
- Support programs by DFS providers that provide high-touch, in-person or one-on-one strategies to enhance digital financial capability at the point of use to increase usage. These strategies, such as click and mortar, using traditional relationships, such as in-branch or agent connections such as touch points, should also provide education on usage.

> **Conduct periodic demand-side surveys** to assess the digital financial capabilities of consumers and devise appropriate interventions in national financial education strategies.

> **Authority(ies) to communicate/disclose** (e.g. via websites, or periodically via social and traditional media) approved and blacklisted DFS providers, permissible digital services/products, etc.

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 the 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

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.).

BOX 6: DIGITAL FINANCIAL CAPABILITY

Consumer awareness is the biggest concern among AFI's members. However, digital financial literacy capability is yet to gain a primary role within the national financial education initiatives. Almost two-thirds of AFI member countries are promoting initiatives on financial education/awareness campaigns but only in a few cases are specific DFS topics/issues covered.[4] Nonetheless, some members have instituted specialized interventions towards digital financial literacy and capability of consumers.

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 scams. 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 the Bank of Russia both have developed financial literacy websites that address many topics, including some DFS-related issues (such as online deposits, cashless payments, internet banking and crowdfunding).

disclosure in product marketing. For example, with regards to 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.

- Incorporate customer-centric features such as 'minimum scroll downtime and length for reading pre-contractual information.
- DFS providers to create and use common iconography around digital security to socialize consumers around common and visual language on to how to use DFS safely.
- Acknowledgment or sign-off key product statements through digital modes, such as interactive SMS, etc.
- Incorporation of digital calculators for relevant products.
- Require apps to provide key information without the consumer having to first disclose personal financial information. Key information includes product features, uses, demos, terms and conditions, and info on redress mechanisms. This information should be made available on the home page or with just one-click.
- Require pre-read or pause function before any purchase decision via DFS to provide brief time to review transaction and key ToCs before making final decision.

> **Provide guidance on format and manner for responsible marketing/advertisement/sales.** The authority(ies) 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, and the DFS marketing and sales information (e.g. to disclose information publicly on websites, marketing material, agents' point of sales, adoption of live calculators on applications or websites, etc.);
- Customers to be informed on all revisions (fees, features, terms and conditions, etc.) related to the DFS with the right to reject the product without monetary loss.
- 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 the use of multiple mediums such as written and oral communications, as deemed feasible.

> **Authority(ies) to ensure that requirements are proportionate and not restrictive to creativity** in marketing/advertising, innovation and does not place undue cost to implement. Where feasible, authority(ies) to consider/include provisions for a standardized price reporting to a central database (possibly managed by authority) that is open to the public, to promote transparent comparison among DFS providers.

BOX 7: BEST PRACTICES ON TRANSPARENCY AND DISCLOSURE – THE CODE OF CONDUCT OF ARMENIA

In Armenia, digital financial inclusion is growing fast (from 12 percent in 2011 to 42 percent in 2017) and becoming of great interest to 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 that was taken is on the 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 signed.

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, since to many, 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 of 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 (IDR) mechanisms of DFS providers and a secondary appeal focus on External Dispute Resolution (EDR) 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 that 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 that are operated by/involving non-resident or cross border providers.

> **Mandate DFS providers to have an effective IDR mechanism in place.** Ensure IDR is "fit for purpose" and reflects the unique scope of the DFS provider's product/service, channel, consumers, relevant risks, and volumes of complaints that 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.
  - When encouraging use of digital channels and innovative technology in IDR, provide guidance on storage of complaints received/responded to by those channels, as well as related guidance on data protection.

> **Institute a reporting framework and guidelines on DFS for both IDR and EDR:**

> The framework should be standardized in the format (e.g. indicators, reporting template, scope of data, scope of reporting etc.) and timeline (periodic).

> Authority(ies) to develop a general grievance-handling mechanism framework and blueprint, to be customized by DFS providers, according to the nature of product/service and the types of complaint.

> 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 periodically publish on complaints and redress, encouraging the use of digital channels for the publication.

> Define reasonable timelines for resolution of customer complaints.

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

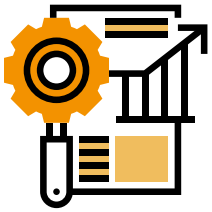
> **Facilitate and encourage consumer awareness campaigns on IDR and EDR/ADR systems,** including the use of local languages and social media.

> **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 the sharing of information, for the effective and coordinated handing and redress of consumer complaints.

> Where feasible, as national jurisdiction permits and as per the maturity of the DFS industry within the jurisdiction, *consider a specialized DFS unit within independent dispute resolution body* (e.g. Consumer Protection Ombudsman) or the EDR office for the financial sector or regulator. Alternatively, authority(ies) to enhance the framework and capacity of existing independent dispute resolution body to effectively address the DFS industry.

> **Regulators to consider adopting technology for complaints management** - e.g. chat box, interactive videos etc.

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, and process risks beyond the scope of the traditional/cash-oriented financial sector, including the digitization of procedures, contracting and interactions, including where there are no funds moving. These have introduced new dependencies (such as third-party contractors) within the supply side, 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, which includes the use of supervision technology (SupTech). Yet, the 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 efficient and effective.

KEY RECOMMENDATIONS

> **Undertake an assessment of existing supervisory approaches, tools and techniques for relevance to supervisory needs of DFS industry,** which should cover:

- The effectiveness of their supervisory approaches to the DFS sector. This covers the relevance of indicators, techniques, tools, etc.
- The scope and capacity in data collection, aggregation, analysis and reporting.
- The quality of data collected and reported, including the level of granularity (such as demographic segregation etc.).

> **Adapt existing supervisory tools** (institution-based offsite and onsite examinations, market-based monitoring/surveillance, enforcement), and techniques (such as thematic reviews, interviews,

transaction simulation, review of documents, mystery shopping, among others) to reflect the DFS sector. Consider interventions such as:

- Adoption of innovative technology solutions, such as artificial intelligence (AI), machine learning (ML), Application Program Interfaces (API), big data analysis, among others, in SupTech and RegTech to enhance efficiency and quality in data collection and analysis, as well as proactive/pre-emptive approach to supervision.
- Investment in DFS-relevant technical expertise (e.g. 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.
- Ensure reporting requirements are reflective of the DFS industry in the jurisdiction.
- Extend supervision to relevant third parties, such as IT/technology contractors, agents, etc. in the supply-side supervision.
- Develop a robust surveillance system to serve as an early warning platform, as the reliance on off-site supervision increases.
- 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. data protection, cybersecurity, fair treatment and business conduct, etc.) and blacklisting.
- Include technology-based techniques such as forensic auditing, auditing a digital customer interaction, auditing customer voice recordings through AI, scanning documents with AI, reviewing algorithms, etc.

> **Ensure supervisory approaches, tools and techniques reflect DFS-relevant principles**, such as

- Risk-based: reflect the risk profile (known and potential) of both DFS providers and consumers to ensure supervision is targeted and 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 the DFS providers and do not impose undue compliance burden on them, 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.
- Standardization of approaches, tools and techniques. This includes but not limited to, templates, operational/technical definitions, indicators, data collection and process, etc.

> Create supervisory benchmarks for key thematic areas relevant to the DFS industry (e.g. data protection, cyber security, agents, IT outsourcing, etc.) in the jurisdiction to guide thematic reviews of the industry.

- Explore the idea of incorporating supervisory insights in regulatory Sandbox and frameworks for innovation hubs.

> Authority(ies) to monitor the unregulated market with the objective of identifying emerging consumer protection risk issues, to inform the review of regulatory perimeters and provisions.

4.2 GUIDING PRINCIPLE: STANDARDIZED SUPERVISORY GOVERNANCE FRAMEWORK

RATIONALE

Similar to the regulatory environment, multiplicity of regulators in the supervision of DFS sector, create overlapping responsibilities and compliance burden on DFS providers, among others.

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

KEY RECOMMENDATIONS

> **Promote inter-agency cooperation** among relevant authorities with 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.

> Standardization of the supervision of core DFS thematic issues, such as data privacy and protection, cyber security, KYC, fair treatment and business conduct, etc. The objective should be to minimize compliance burden on DFS providers, which might be transferred to consumers through transaction fees.

BOX 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 more than half of AFI members, the regulator supervises the implementation and compliance of established policies and frameworks by DFS providers, and 42 percent 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 percent of the members) or for very few countries, the regulators supervise pilots or rollout during the development. In only 23 percent 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, where websites, radio and tv advertisement are monitored), and it carries out activities to monitor DFS providers' practices vis-à-vis consumers 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 and encourage the gradual and increasing adoption of good business practices among providers over time. This guideline advocates robust legal mandate, proportionate powers and adequate enforcement tools and a 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.

- Explore CP-specific tools, such as the withdrawal of products/advertisements from the market, and change requirements to consumer agreements or other documents, which hold much relevance to the DFS sector.
- Explore extending enforcement beyond non-compliance, with a specific regulatory provision to practices deemed as contravening key CP principles.

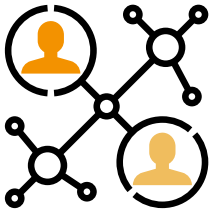
> **Adopt principles-based approach to enforcement of the DFS sector** to ensure measures do not stifle innovation and growth in the sector but rather support the development of a sound DFS sector, such as:

- The credibility of the 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 the 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.

> **Consider public disclosure of enforcement actions** (particularly sanctions) to encourage adequate conduct by DFS providers.

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 expose/deepen the vulnerabilities to DFS-related consumer protection risks. Vulnerable segments include populations exposed to low/poor socio-economic opportunities, as per the 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, the elderly, refugees/internally displaced people/undocumented migrants, and 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, certain religious segments (such as Muslims who adhere to 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, which derails 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 general recommendations are made for the consideration of relevant authorities in promoting CP4DFS among vulnerable segments. It is followed by some specific interventions for identified vulnerable segments.

> Leverage on existing tools and techniques (e.g. demand-side surveys, complaints, and redress data, market-based monitoring, 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 and implement relevant, demand-driven, and evidence-based digital financial literacy and capability interventions for the identified segments, with an objective of enhancing their knowledge to make informed and secured DFS decisions.

> Define the responsive provisions for relevant vulnerable segments in market conduct regulations – e.g. tiered KYC, guidelines on data profiling, charges/fees, etc.

> Encourage DFS providers to adopt 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 girls:

> 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 low-risk 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 the 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 that are responsive to the challenges with identification and documentation relevant to refugees/IDPs.

> Define simplified KYC and CDD requirements using a Risk-Based Approach that are 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(ies) to facilitate an interagency coordination 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(ies) 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(ies), 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:
  For instance, when the fees for transactions are reduced or waived (under a certain amount or for any amount) and/or removed/increased limits on mobile transactions, the authority(ies) 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 a more relaxed loan disbursement criteria, the authority(ies) 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(ies) to mandate DFS providers to avoid/ease hardship (e.g. suspending payments of loan installments, plan for rescheduling/restructuring, etc.).

  When allowing for the use of digital signatures and loan disbursements remotely, and relaxing KYC requirements, the authority(ies) to mandate DFS providers to avoid any discriminatory practices.
- Product suitability:
  The authority(ies) 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(ies) to mandate DFS provider to expand consumer choice and enable provider switching.

- Cybersecurity

  The authority(ies) to mandate DFS providers to strengthen cybersecurity measures to ensure stable and safe connections/systems (above all, in a situation where work from home or remotely might increase risks of breaches).

  The authority(ies) to ensure the security and integrity of the payment infrastructure with regular monitoring activities.

> The authority(ies) to ensure that relaxation of regulations does not adversely affect requirements on adequate authentication of client identity and consent by DFS providers to avoid fraud.

> **Mandate DFS providers to have a Business Continuity plan.** The authority(ies) to mandate DFS providers to develop a business continuity plan for liquidity management and provision of services available during emergencies.

> The authority(ies) to ensure DFS providers *offer clients an appropriate and easy channel/mechanism for complaint and redress.*

> After/at the end of disasters or emergency, the authority(ies) to ensure *effective consumer awareness on changes /reversion of policies* to prevent fraud, and to ensure consumers make informed decisions post the period.

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

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 table 5 opposite present a codification of the main AFI knowledge products over key categories of consumer protection (in orange):

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 of designing 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)

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

- 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 have a market perspective (actions to be taken by DFS providers to protect the consumers), it is worth mentioning the following (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)

TABLE 2: CODIFICATION OF SOME AFI KNOWLEDGE PRODUCTS IN TERMS OF CP PRINCIPLES AND REGULATORY, SUPERVISORY FRAMEWORK

	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)	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			x	x		x	
PRIVACY AND SECURITY			x	x	x	x	x		
PRODUCT SUITABILITY			x			x	x		
FAIR TREATMENT			x		x	x	x		
INTERNAL CONTROL			x			x	x		x
DIGITAL FINANCIAL EDUCATION			x				x		
DISCLOSURE AND TRANSPARENCY		x	x		x	x	x		
COMPLAINTS AND REDRESS	x		x		x	x	x	x	
SUPERVISION AND ENFORCEMENT		x	x		x	x			
VULNERABLE SEGMENTS			x						

ANNEX 2.
KEY CONCEPTS AND DEFINITIONS[7]

DIGITAL FINANCIAL SERVICE	The broad range of financial services accessed and delivered through digital channels, including payments, credit, savings, remittances and insurance. The DFS concept includes mobile financial services (MFS).[8]
DIGITAL FINANCIAL SERVICE PROVIDERS	Financial institutions that that deliver financial services accessed and delivered through digital channels, including payments, credit, savings,remittances and insurance. The DFS[9] concept includes MFS.
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).[10]
DIGITAL FINANCIAL LITERACY AND DIGITAL FINANCIAL CAPABILITY	Digital Financial Literacy is a multi-dimensional concept that covers knowledge of digital financial products and services, awareness of digital financial risks, knowledge of digital financial risk control, and knowledge of consumer rights and redress procedures.[11] Digital financial capability is the knowledge and application of attitude, knowledge, skills, and self-efficacy to undertake effective and secured decisions in the use of DFS that are relevant to one's needs.[12]
INTERNAL DISPUTE RESOLUTION	This refers to internal processes by a Financial Service Provider for the reporting and redress of complaints.
EXTERNAL DISPUTE RESOLUTION	Systems for complaints and redress outside the related financial service provider, such as the regulator.
ALTERNATIVE DISPUTE RESOLUTION	An alternative to formal court-based dispute resolution, providing affordable, yet timely and accessible resolution of complaints from consumers.

7 Based on definition from "Guideline Note Mobile Financial Services: Basic Terminology", AFI (2012) and consultants' re-elaborations.
8 Based on definition from "Guideline Note 19 - DFS Basic Terminology"
9 Re - elaboration based on definition of DFS from "Guideline Note 19 - DFS Basic Terminology"
10 Based on definition from "Guideline Note 19 - DFS Basic Terminology"
11 Based on definition from "Policy Brief Under T20 Japan Task Force 7: The Future of Work and Education for the Digital Age"
12 Re elaboration based on definition of financial capability by the Center for Financial Inclusion

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)
- **McKinsey:** 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

Alliance for Financial Inclusion
AFI, Sasana Kijang, 2, Jalan Dato' Onn, 50480 Kuala Lumpur, Malaysia
t +60 3 2776 9000 **e** info@afi-global.org www.afi-global.org
Alliance for Financial Inclusion AFI.History @NewsAFI @afinetwork