cenfri

Consumer Protection in Digital Finance

Policy Brief

22 August 2022

Federal Ministry
for the Environment, Nature Conservation,
Nuclear Safety and Consumer Protection

giz Deutsche Gesellschaft
für Internationale
Zusammenarbeit (GIZ) GmbH

Author(s)

Andrew Partridge

Christine Hougaard

Morongwa Marutha

Cenfri

Tel. +27 21 913 9510
Email: info@cenfri.org
The Vineyards Office Estate
Farm 1, Block A
99 Jip de Jager Drive
Bellville, 7530
South Africa

PO Box 5966
Tygervalley, 7535
South Africa

www.cenfri.org

The authors of this report would like to acknowledge the support of the International Dialogue on Consumer Protection in Context of the SDGs, coordinated by GIZ.

Table of contents

List of Figures

List of tables

List of boxes

Executive summary

Consumer protection in digital financial services is important for sustainable development. Consumer protection is a core consideration in the sustainable development agenda. The digitalisation of commerce and financial services has positively contributed to sustainable development by expanding the ability of individuals around the world to engage with the global economy. Rapid growth in the accessibility and use of digital financial services (DFS) has extended the reach and usability of financial services and fundamentally changed the way consumers interact with financial products and services. However, accessibility is only one step in achieving improved socio-economic outcomes. With digitalisation also come new and heightened risks, including in cybersecurity, to which consumers with low digital literacy are especially vulnerable. Without adequate and appropriate consumer protection the trends in digitalisation could reinforce the digital divide and result in negative collective outcomes such as discrimination, over-indebtedness and widening inequality.

Box 1: Main consumer protection risks in DFS

A 2022 publication by the Consultative Group to Assist the Poor (CGAP) identifies 66 risks that consumers face when using DFS, classified into four broad risk types and two cross-cutting risk types (Chalwe-Mulenga, et al., 2022), based on an in-depth literature review:

Fraud risks relate to deceptive malicious activities - such as cybercrime, identity fraud, social engineering, SIM swap fraud, hoaxes and scams - which result in financial loss for consumers. These risks put consumers' financial health at risk and deteriorate trust in the financial services sector. Most of the new risks emerging in recent years have been related to fraud.

Data misuse risks arise from the unauthorized use of customer data and information for purposes other than what it is intended for. This can manifest in a number of different ways including algorithmic bias, unfair sales and marketing practices, privacy intrusions and breaches of personal data, all leading to consumers being afraid to share information even in secure environments, which in turn can prevent the efficient and suitable provision of financial services.

Lack of transparency risks result when the terms, conditions, fees and features of a financial service or product are not communicated to and understood by the consumer. Examples of lack of transparency risk are hidden charges, misleading advertisements and complex or confusing interfaces or languages. Where transparency is lacking consumers do not make decisions in their best interest and undisclosed financial risk can be easily passed onto them, resulting in over-indebtedness and exploitation of vulnerable groups.

Inadequate redress risks arise where there aren't sufficient, accessible and effective channels for consumer complaints. This would mean that there is no feedback loop

from consumers to providers to better tailor the provision of services and products and that consumers are not able to hold providers accountable for their actions.

There are also two risk categories that manifest across all of the above categories: **agent-related risks** refer to issues stemming from the interaction between a consumer and the designated agent of a service provider such as manipulation or unfair treatment of customers, insufficient liquidity and prevailing gender norms that affect customer outcomes; and **network downtime risks** relating to technological failures which prevent consumers from being able to effectively use products and services, such as power outages, failed transactions, inadequate infrastructure and distributed denial of service attacks. These cross-cutting risks can exacerbate the other risk types and can undermine the delivery of DFS.

Need for a principles-based framework focused on consumer outcomes.
The fact that DFS trends and risks are dynamic and continually evolving, means that traditional rules-based frameworks quickly become out of touch with the realities faced by DFS consumers. In contrast, principle-based frameworks can accommodate new trends and technologies and remain relevant over time and across different contextual settings. Basing frameworks on consumer outcomes, as opposed to financial institution conduct, ensures that financial consumer protection efforts work towards the ultimate objectives they are intended for and align with the broader consumer protection agenda. From the financial consumer protection literature, ten core principles can be identified, aligning closely with the seminal *G20 High-Level Principles on Financial Consumer Protection* (OECD, 2011):

Element	Principle
1. Legal recognition	Financial consumer protection must be grounded in legislation and regulation in a manner that effectively addresses consumers' risks.
2. Oversight and monitoring	Oversight bodies should be created and empowered to enforce and monitor financial consumer protection, with explicit reference to the need for inter-governmental coordination.
3. Responsible market conduct	Responsible conduct by service providers and their agents should be integrated into financial service providers' internal proceedings and in their engagement with customers.
4. Access to information	Regulation should entrench the need for customers to be provided with all relevant information, in an appropriate format, to allow for appropriate customer choice and usage behaviour.
5. Financial education	Dedicated financial education programs and strategies should be set up to increase consumers' knowledge of and skills in navigating financial services.
6. Dispute resolution	Consumers should have access to and knowledge of adequate complaints-handling mechanisms both within businesses as well as through independent or alternative dispute resolution structures

Element	Principle
7. Prudential protection	Regulation should entrench the need for consumers' assets to be protected and for FSPs to remain financially sound. Such regulation should be enforced through risk-based prudential supervision.
8. Data protection and privacy	Consumers' financial and personal information should be adequately protected through appropriate control and protection mechanisms.
9. Cybersecurity	Financial service providers should have the relevant controls in place to evaluate, monitor, test and respond to cyber-security risks. Regulatory authorities should ensure that they have the scope and relationships with other authorities and jurisdictions to adequately manage and address cyber-risks.
10. Competitive financial sector	A competition regulatory framework should be in place to ensure a competitive and inclusive financial sector.

Table 1. Elements of financial consumer protection in the context of DFS
Source: adapted from OECD (2011), AFI (2010; 2021), CFI (2019), CGAP (2010; 2020), FMT (2016), Gibson (2011), UNCTAD (2016), World Bank (2017).

These ten elements come together and culminate in the overarching principle of **fair consumer outcomes,** namely that consumers should be treated equitably, honestly and fairly at all stages of their relationship with FSPs, *to lead to fair outcomes from the consumer's perspective* (CGAP, 2020).

Future-proofing against the key risks. The consistent, principles-based application of the financial consumer protection elements, gauged against positive consumer outcomes as ultimate measure of success, provides a sound way for mitigating the main DFS consumer risks – and ensuring that emerging future risks are accounted for. For instance:

- The increases in ***fraud risks*** such as cybercrime, identity fraud, social engineering, SIM swap fraud, hoaxes and scams heighten the need for sound ***prudential regulation*** and ***cybersecurity***.
- Increasing pressure to share data needs to be balanced with effective ***privacy and data protection*** to manage ***data misuse risks*** such as algorithmic bias; unfair sales and marketing practices; privacy intrusions; and breaches of personal data.
- ***Inadequate redress risks*** such as unclear, expensive, or time-consuming complaint procedures and unsatisfactory dispute resolutions are addressed by giving consumers a more direct voice through various ***dispute and redress*** channels.
- ***Lack of transparency risks*** such as misleading advertisements, hidden charges and complex or confusing interfaces or languages can be combatted through the ***disclosure of information*** and through ***financial education***.
- ***Responsible conduct*** extends from the service provider to also cover the provider's agents and the associated ***agency risks*** such as the manipulation or unfair treatment of customers, insufficient liquidity and gender norms.

Coordination and exchange are key for effective principles-based financial consumer protection implementation. As technology cuts across boundaries, implementing a holistic and principles-based framework requires a cross-cutting approach spanning several financial sectors and broader government fields. Within a specific jurisdiction, this highlights the need for coordination and exchange between different financial regulatory authorities, coordinated by the financial sector policymaker, as well as between the financial sector policymaker and its counterparts in the competition and broader economy-wide consumer protection spheres. It also calls for dialogue involving different stakeholder groups – policymakers, regulators, providers and, importantly, consumers themselves – at the national and global levels. There has already been positive work in establishing knowledge-sharing platforms to engage on issues relating to FCP. These can now form the springboard to even more policy-level engagement and collaboration across countries and stakeholder groups.

1. Introduction

Consumer Protection is a core element of the Sustainable Development Goals. Following the release of the *2030 Agenda for Sustainable Development* (United Nations, 2015), and the accompanying Sustainable Development Goals (SGDs) in 2015, the United Nations published a report on *Achieving the Sustainable Development Goals through Consumer Protection* (UNCTAD, 2017). The report highlights the importance of consumer protection for sustainable development. Indeed, the adoption of the United Nations Guidelines for Consumer Protection (UNCTAD, 2016) can support countries in working towards all 17 of the SDGs. This is particularly relevant for marginalised communities and populations, such as women and rural communities[1].

Digitalisation of commerce and financial services is bringing new considerations for consumer protection policy. Consumer protection policies are particularly relevant in the era of digital commerce (UNCTAD, 2021). The OECD revised recommendations for *Consumer Protection in E-Commerce* acknowledge that e-commerce brings new consumer protection considerations, such as the need to provide redress for non-monetary transactions, the complexity of digital content which consumers need to understand, the increase in consumer-to-consumer transactions, mobile technology innovations and increased need for data and product safety protection (OECD, 2016). The need for safe digital payments is equally important. The rise of e-commerce goes hand in hand with the rise of digital financial services (DFS). Apart from forming the foundation for e-commerce, DFS also has broad-ranging relevance in the economy and forms the basis for much of the financial inclusion gains that the world has seen in recent years. DFS bring distinct advantages for consumers and businesses alike. They can substantially lower the costs of financial services whilst also making them faster, safer and more transparent to be more fit-for-purpose for all potential users (Pazarbasioglu, et al., 2020). However, DFS also introduce new consumer risks.

A "balancing act". Financial consumer protection (FCP) encompasses the legal, regulatory and other institutional arrangements that safeguard consumers as they adopt and use financial products and services (World Bank, 2022). Effective FCP requires balancing two important and often conflicting agendas (Figure 1). On the one side is the need to ensure that financial consumers receive adequate protection. However, on the other side overly stringent, unnecessary, or unequal protection measures can act as a barrier to market provision and can prevent consumers from realising the full benefits of DFS. Finding the balance between these two objectives is

1 The difficulties faced by women and the need for policies to protect and empower women is at the heart of sustainable development with an entire SDG devoted to efforts to "achieve gender equality and empower all women and girls" (United Nations, 2015, p. 20). The World Social Report 2021 (UN DESA, 2021) also highlights the importance of rural development for achieving the SDGs and the need for renewed efforts at uplifting rural communities in light of lagging progress and persistent poverty.

crucial, especially for vulnerable groups such as women, rural communities and those with low financial literacy, that are also traditionally the most financially excluded[2].

Figure 1: The balancing act between financial inclusion and consumer protection
Source: Authors' own

A brief to build understanding and provide the basis for ongoing dialogue.
This document considers the topic of DFS within the broader consumer protection agenda. It is intended as input into the ongoing policy dialogue on consumer protection. The next section highlights some of the key trends emerging in DFS, followed by a section outlining the main risks this presents. Section 4 introduces a framework for assessing the full scope of financial consumer protection and provides a high-level application of the framework to the risks presented by DFS. Section 5 concludes with observations on the implications for the consumer protection policy agenda as input for dialogue moving forward.

2 The recent World Bank *Findex* Survey shows that the uptake of DFS amongst women and in rural areas has also been disproportionately low, highlighting the need to take advantage of the accessibility opportunities introduced through digital technological innovations to improve inclusion amongst these groups (Demirguc-Kunt, et al., 2022). As efforts are ramped up to improve financial inclusion for women and rural communities, it is important that consumer protection measures are tailored to ensure these groups are adequately protected in order that inequalities are reduced and not further exasperated.

2. Global Trends in Digital Financial Services

Defining digital financial services. Digital financial services (DFS) are defined as financial products and services that are delivered via digital or electronic technology. This includes payments, transfers, savings, credit, insurance, securities, financial planning, and the provision of account statements. The technology for delivering DFS includes e-money (initiated either online or on a mobile phone), payment cards as well as a regular bank account (Pazarbasioglu, et al., 2020).

Growth in the adoption of digital financial services sees the developing world 'catching up'. One of the core requirements to be able to interact with DFS is to have a digital transaction account. Globally, there has been strong growth in the share of the population with account access, from 51% in 2011 to 76% in 2021. As expected, this has been coupled with an increase in the use of digital financial services. In 2014 the share of the population reporting to have made a digital payment was only 36%; by 2021 this had risen to 59%. The increase in developing countries has been disproportionate to the developed world, seeing a sharp increase in both the percentage of adults with a financial account and the percentage of adults who make digital payments over the past decade (World Bank, 2021). Whilst there are still disparities in the availability and accessibility of DFS, they are increasingly becoming more universally available and accessible.

Initially driven by mobile money, DFS now span much broader. The rise of mobile money in the developing world is a key driver of this trend[3]. It, in turn, is enabled by a rapid increase in the uptake of mobile phones in the developing world, coupled with technological advances in mobile services[4]. But consumers in developing countries are not using DFS just as a basis for payments and transfers. They are also increasingly making use of more sophisticated financial services such as digital lending, investments and mobile or online insurance (Pazarbasioglu, et al., 2020).

DFSs are fundamentally changing how individuals access and use financial services. Advances in communications technology have essentially eliminated physical distances between providers and customers. This is drastically improving the accessibility of customer services and improving the quality, accessibility and affordability of financial services around the world (Pazarbasioglu, et al., 2020). In addition to providing new access channels to extend reach to the previously underserved, digitalisation is changing the way that individuals and businesses from all countries and walks of life engage with the various components of the financial system – from how products are designed to suit their needs, to how client acceptance or funds allocation decisions are made, to how customers interact

3 In low-income countries the share of the population with mobile money accounts has increased from 7% in 2014 to 27% in 2021 (World Bank, 2021).

4 Mobile phone access has also connected people to the internet, with more than 200 million people connecting to mobile internet for the first time in 2021, bringing the total of connected individuals to 4.19 billion people (53% of the global population). This is expected to continue to increase as mobile adoption continues to rise around the world (Awanis, et al., 2022).

with/transact on their financial services, how they receive client services and, finally, how they access recourse.

A shifting landscape of provision. DFSs are also changing the playing field for financial service provision, particularly via the rise of fintech firms. Fintech is defined as the meeting point between financial services and technology. Although not a new phenomenon, recent years have seen a growing prominence of fintech firms causing significant disruptions to the provision of financial services around the world. FinTech firms can provide new service offerings and provide certain services at lower costs and through channels which are more suitable for low-income consumers. The rise of fintech has introduced substantial uncertainty over who should be regulating FinTech activity and how to deal with unfamiliar avenues for data breaches, fraud and price discrimination (Bates, 2017).

Enabled by underlying technological advances. The adoption of several new-age technologies is underpinning these trends. The "internet of things" is changing the way service providers can incorporate, store and use customer data (Chio, et al., 2021). Robotic Process Automation is allowing computer software to complete straightforward repetitive tasks such as loan processing, client onboarding, fraud detection and financial risk management (BDO, 2020). The application of artificial intelligence and machine learning is enabling more efficient, timely and speedy analysis of data in respect of credit decisions, identification of threats and addressing financing gaps, allowing service providers to extend their reach to a wider and more inclusive range of customers (Biallas & O'Neill, 2020). Finally, rapid growth in crypto assets (private digital assets mainly based on cryptography and distributed ledger technology) has created new channels to transact and interact with the financial sector (BIS, 2021)[5].

With the benefits come risks. Despite these benefits, DFS also introduce new risks to consumers and the system, plus fundamentally change the traditional risks that consumers face when using financial products and services. The next section explores the nature and implications of these risks.

5 However, this has also created significant market volatility and the need to tailor regulations to specifically account for this new form of currency.

3. Digital Finance Risks

Six consumer risk categories in relation to DFS. Between 2020 and 2022 the Consultative Group to Assist the Poor (CGAP) undertook research to understand the evolution of the nature and scale of risks associated with DFS (Chalwe-Mulenga, et al., 2022)[6]. The research identifies 66 risks which are grouped into four broad and two cross-cutting risk types as displayed below in Figure 2 (see the Appendix of this report for a full listing of the 66 risks). Five of the risks are classified as newcomer risks which have only come into existence due to recent technological developments, however, CGAP also explain how pre-existing risks have become more complex and consumer vulnerability has increased due to the rise of DFS (Chalwe-Mulenga, et al., 2022). If not managed correctly, these risks can undermine the consumer gains from the financial services sector, resulting in over-indebtedness and deepening poverty, widening inequalities, and a loss of trust.

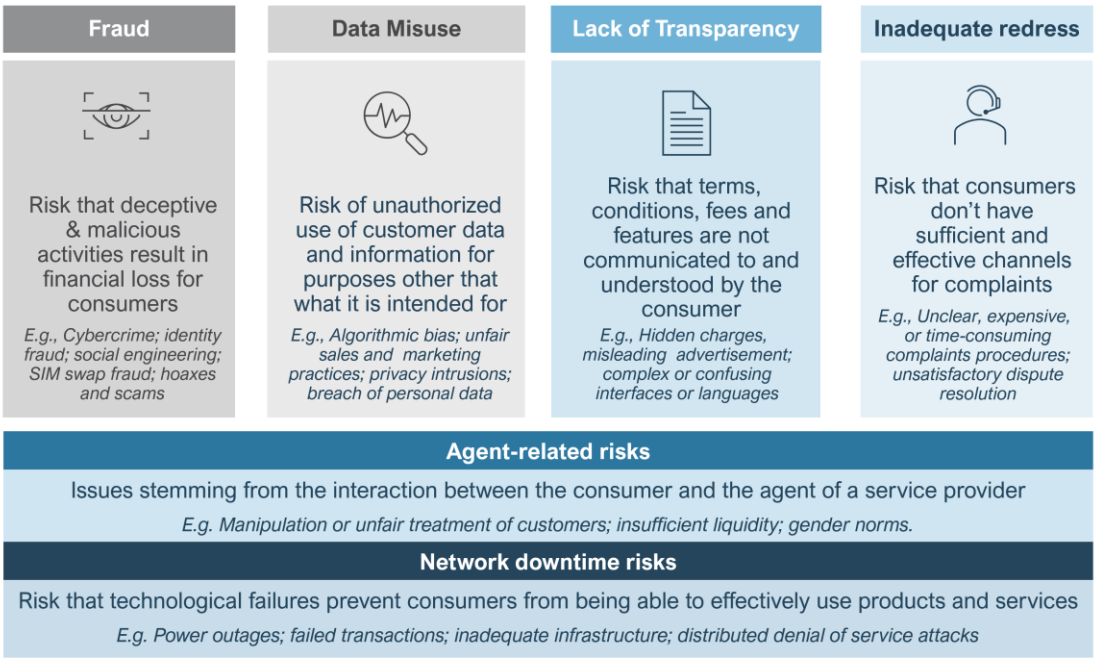

Figure 2: CGAP categorisation of DFS consumer risks

Source: (Chalwe-Mulenga, et al., 2022)

Most of the "newcomer" DFS risks identified relate to fraud. Fraud risk refers to a risk where an individual or entity intentionally engages in different deceptive activities that will cause a DFS consumer financial loss. Of the five newcomer risks introduced by CGAP, four relate to fraud: Mobile app fraud/phone espionage; biometric identity fraud; authorized push payment (APP) scams; and synthetic identity fraud (Chalwe-Mulenga, et al., 2022). If not effectively managed, fraud puts consumers and providers at risk of financial loss and will result in severe deterioration of trust in the DFS system.

6 The work builds on a 2015 focus note motivating for stronger mitigation of consumer risks in digital finance (McKee, et al., 2015), taking note of DFS developments occurring in the interim.

Box 2: Business Email Compromise

Whilst business email compromise is not the most prevalent type of malicious email in terms of incidence, it has had the largest financial implications. Business email compromise occurs when an attacker pretends to be a legitimate business account by using either a compromised email address, a lookalike domain they have registered, or a free email service such as Hotmail or Gmail to send emails designed to trick recipients into taking some financial action, handing over sensitive information, or providing assets to the attacker. The most common occurrence of business email compromise has been in the form of gift card scams; however, wire transfer fraud has been noted as causing the most financial damage (Microsoft, 2021).

Data misuse risk needs to be managed in the face of increasing pressure to share data. Data misuse risk refers to the risk whereby an entity or person uses a DFS customer's data or information for other purposes it is not intended for. This is a particularly sensitive area as there is increasing pressure to share data to improve important decision-making processes and to increase the efficiency of the links between different components of the DFS ecosystem. The right balance must be found to realize the benefits of DFS in terms of the availability of usage data, whilst still ensuring that individuals' personal information remains protected from misuse. The only newcomer risk not covered under fraud was artificial Intelligence (AI) related risk which falls under data misuse risk (Chalwe-Mulenga, et al., 2022). An example of the manifestation of AI-related risk in the context of credit scoring is provided in Box 3.

Box 3: The risk of algorithmic credit scoring in exacerbating discrimination and inequalities in lending

Machine learning in the form of algorithmic credit scoring provides opportunities to improve the accuracy of service provision, however, it has also been noted to have exasperated discrimination and inequalities.

Vulnerable groups tend to have less data in their credit histories which perpetuates inequality in lending markets. Current data protection regulations grant limited control over the information these algorithms produce as outcomes. In addition, it is not currently mandatory for lenders to be transparent in how their AI models determine credit applications. As borrowers have access to more data about consumers to improve the design and marketing of credit products, they can exploit consumer biases and preferences to engage in less desirable forms of price discrimination and targeted marketing based on consumers' misperceptions (Remolina, 2022).

Regulators have an important role to play in ensuring that the financial sector can benefit from algorithm credit scoring whilst not entrenching discrimination and inequality.

Consumers see lack of transparency risks as the most significant. Lack of transparency risks refers to the risks that terms, conditions, fees, and other DFS features are not communicated to and understood by a customer (Chalwe-Mulenga, et al., 2022). A recent study on low- and middle-income countries revealed that the top-four most significant challenges DFS consumers faced in 2020 were related to lack of transparency, specifically contract terms not being clearly explained, hidden or inflated fees, unfair terms and conditions, and undisclosed levels of risk being passed onto the consumer (Consumers International, 2021). Where there is no transparency, undisclosed levels of financial risk can be easily passed on to the consumer, resulting in sub-optimal consumer outcomes (Chalwe-Mulenga, et al., 2022). In addition to hiding information, companies have also been noted to trick customers in the way information is disclosed, an issue referred to as "dark patterns", or "deceptive design" (see Box 4).

Box 4: "Dark patterns"

Dark patterns occur when websites and apps use misleading language or positioning of information to trick consumers into doing something they wouldn't otherwise do, such as buying a product or signing up for a particular service (Mathur, et al., 2021). A stock-take of complaints of dark patterns shows that there is a high incidence of this consumer risk, including on widely-used platforms such as Google, Facebook, Amazon and LinkedIn (Brignull, 2010).

Inadequate redress mechanisms can occur through lack of provision and/or through lack of communication. Inadequate redress mechanisms relate to a DFS user having no channel for complaints or when complaints are not appropriately addressed. This can occur through different means, in some cases it will be the result of a lack of effective recourse channels, in some as a result of the channels being inaccessible or unknown, in some cases it will be a combination of these factors (Chalwe-Mulenga, et al., 2022).

Agent risks threaten financial service delivery and if not properly managed can lead to a lack of accountability on behalf of the DFS provider. Agent risks are those risks emanating from a DFS user's interactions with the designated agent of a DFS provider. Agents have become a valuable tool in advancing financial inclusion, particularly in developing countries. It provides an alternative to extend the reach of financial services in contexts where it is not financially or physically possible to extend the network of physical provider branches or automated teller machines (ATMs). As such, they are also a core component of mobile money schemes where mobile money operators are less able to develop branch or ATM networks (Demirguc-Kunt, et al., 2022). Agent risks cover a broad range of issues, agent misconduct can lead to the mistreatment of customers, a lack of training of agents can lead to poor service delivery and insufficient agent liquidity can result in a breakdown of transactions which leads to a lack of trust in the financial system (Chalwe-Mulenga, et al., 2022). These issues are difficult to manage and can lead to a lack of accountability on behalf of the service provider.

Network downtimes undermine DFS value to consumers. Despite developments in mobile technology making significant strides in expanding connectivity and access to DFS in developing countries, there remain large parts of the world where access and quality lag behind (GSMA, 2022). The quality of internet access is particularly low in Africa where there is also the highest concentration of "least-developed countries" (ITU, 2021). Network downtimes and broken connections because of poor network quality undermines DFS reliability and heightens the risk of uncertainty as to whether transactions have been processed. Consumers surveyed across seven African countries in a recent study on instant and inclusive payments revealed that network downtimes are one of the major deterrents for consumers to adopt and use digital payments (AfricaNenda, forthcoming). To fully allow consumers in LDCs to draw value from DFS developments, it is critical that network infrastructure is improved.

DFS risks threaten social consumer protection by disproportionately affecting vulnerable groups such as females and rural dwellers. There is a lack of disaggregated data on the exposure to DFS risks, however, anecdotal evidence suggests that females and rural dwellers in low-income countries are more vulnerable to DFS risks than the rest of the population. Lower levels of financial literacy and digital skills observed amongst females and rural dwellers create additional risk of lack of transparency as users are less likely to be able to access and understand contract terms and pricing information. Women have been shown to be more likely to encounter fraudulent activities such as Ponzi schemes. There are fewer agents and other access points in rural areas, particularly for women who prefer engaging with female agents who are far less common. This creates an additional access barrier and increases the probability of agent misconduct and liquidity challenges. There are also fewer recourse channels available in rural areas, particularly for women who tend to avoid complaints through male agents due to cultural concerns. As women and rural dwellers face higher levels of financial inclusion data is skewed towards males and urban dwellers meaning that women and rural dwellers are more likely to be negatively affected by algorithm bias (Chalwe-Mulenga, et al., 2022).

4. Principles of Financial Consumer Protection

Addressing the range of consumer protection risks as outlined above within the dynamic nature of DFS requires a holistic framework for financial consumer protection. This section introduces a high-level framework of consumer protection principles to address DFS risks and ensure that the provision of financial services supports sustainable development goals.

The dynamic and evolving nature of DFS risks calls for a principles-based approach. The fact that DFS trends and risks are dynamic and continually evolving, means that traditional rules-based frameworks quickly become out of touch with the realities faced by DFS consumers. In contrast, principle-based frameworks are "future proof" and adaptive allowing them to accommodate new trends and technologies and remain relevant over time and across different contextual settings. Basing frameworks on consumer outcomes, as opposed to financial institution conduct, ensures that financial consumer protection efforts work towards the ultimate objectives they are intended for and align with the broader consumer protection agenda.

A principles-based and consumer-centric framework for financial consumer protection. The financial consumer protection (FCP) framework laid out in Figure 3 outlines the various elements of a holistic FCP framework as covered in the global FCP literature[7].

7 The framework was adapted by drawing on other key frameworks in the FCP literature, notably the G20 High-Level Principles for Financial Consumer protection (OECD, 2011), as well as those published by the Alliance for Financial Inclusion (AFI, 2010; 2021), the Centre for Financial Inclusion (CFI, 2019), Consultative Group to Assist the Poor (CGAP, 2010), FinMark Trust (FMT, 2016), Katherine Gibson (Gibson, 2011), United Nations Conference on Trade and Development (UNCTAD, 2016) and the World Bank (World Bank, 2017). Cybersecurity was added in recognition of the important role it plays in the DFS space.

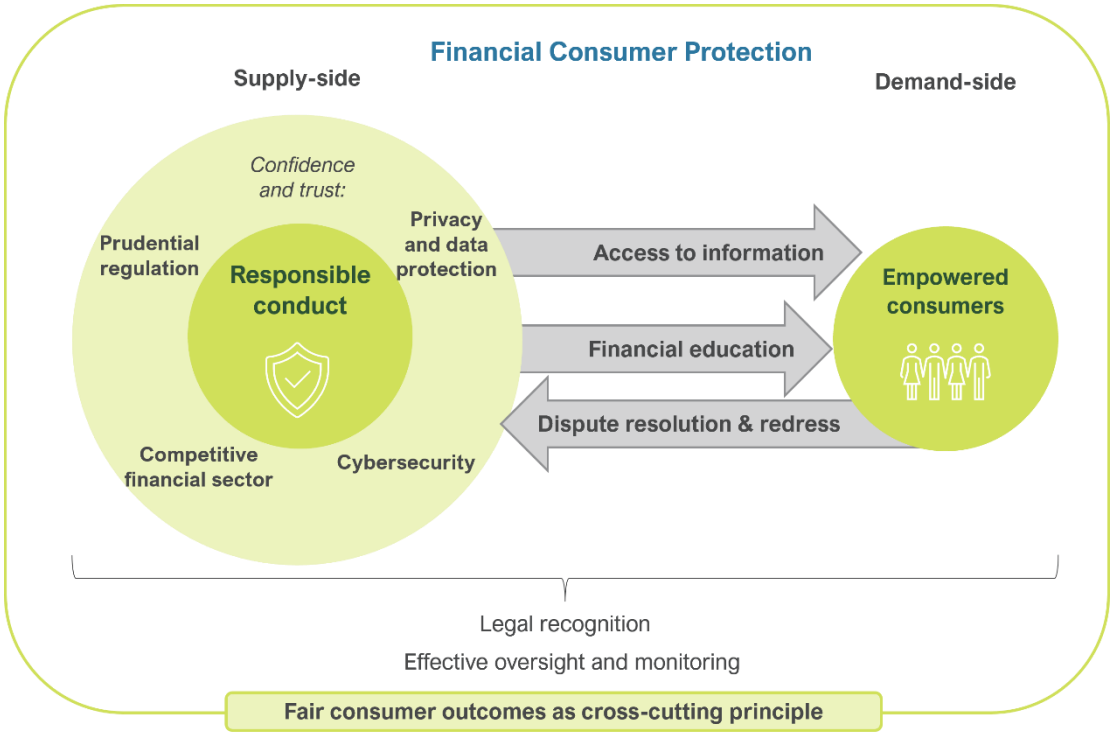

Figure 3: Consumer Financial Protection Framework

Source: Developed based on synthesis across OECD (2011), AFI (2010; 2021), CFI (2019), CGAP (2010; 2020), FMT (2016), Gibson (2011), UNCTAD (2016), World Bank (2017).

Supply-side and demand-side components of the FCP framework overarched by the regulation and oversight of the financial system. As the diagram indicates, the FCP framework classifies consumer protection into a "supply-side" component (different elements of responsible conduct by financial services providers) and a "demand-side" component (how such actions translate into empowered consumers), overarched by effective regulation and oversight:

- At the core of the supply side is the assurance that FSPs act responsibly and in their customers' best interests ("**responsible conduct**"). Consumers need to have confidence and trust in the financial system which requires consumer assets to be adequately protected from theft, fraud and mismanagement ("**prudential regulation**"), personal and financial data to be adequately protected from unauthorised use ("**privacy and data protection**"), consumers be adequately protected from cyber-attacks ("**cybersecurity**") and the promotion of competition in the financial sector to drive innovation and provide user choice ("**a competitive financial sector**").
- On the demand side, consumers are empowered when they are provided with sufficient and appropriate information from providers so they can understand the product or services and make informed choices ("**access to information**"). FSPs should also ensure customers can access adequate knowledge and skills to understand risks and provide advice and assistance ("**financial education**"). These first two principles refer to flows occurring from supplier to customers, but in the opposite direction, consumers should also be provided with mechanisms for consumers to raise complaints against FSPs ("**access to dispute and redress**").

- To create an enabling environment from a governance perspective, consumer protection should be included in all relevant forms of law and regulation ("**legal recognition**") and oversight bodies to monitor consumer protection should be created and provided with the resources needed to function ("**effective oversight and monitoring**"). In the figure, these are presented as foundational, cross-cutting components[8].

Consumer outcomes as the culmination of the FCP framework. Finally, the framework positions **fair consumer outcomes** as the principles to frame each element of the framework, as well as the ultimate outcome or measure of success across all the elements of the framework. This is based on CGAP's consumer outcome framework (explained in Box 5), which is in turn closely aligned to the Treating Consumers Fairly (TCF) framework[9].

Box 5: The customer outcomes framework

The CGAP (2020) consumer outcomes framework was published in 2020 and further develops the concept of consumer outcomes and how this can be measured. This framework expresses fair customer outcomes from the consumer point of view, as an ultimate outcome that should be achieved across all a financial institution's actions, rather than directly related to specific conduct topics. According to the CGAP framework, consumer outcomes can be measured across six core components:

1. **Suitability:** Has access to good quality, affordable and needs-appropriate services
2. **Choice**: Able to make an informed choice among a range of products, services, and providers.
3. **Safety and Security**: Money and information are kept safe, privacy is respected, and control is given over my data.
4. **Fairness and Respect**: Treated with respect throughout interactions, even when the situation changes, and due regard is given to customer interests.
5. **Voice:** Can communicate with the provider through a channel of the customer's choice and get problems resolved quickly at minimal cost.
6. **Meets purpose**: Using financial services means that the customer is in a better position to increase control over their financial life, manage a shock, or attain other goals.

8 In order for FCP to be defined, implemented or monitored adequately it needs to be included in all relevant forms of law and regulation and regulators need to be equipped with necessary authority and tools (AFI, 2021). Laws and regulations addressing financial consumer protection should be tailored to the specific country contexts and should consider global financial market and regulatory developments (OECD, 2011). Oversight bodies are responsible for monitoring market conduct and enforcing regulations as well as playing an important role in establishing coordination mechanisms across the different regulatory authorities. They should be clearly defined and given all necessary tools and authority (AFI, 2021).

9 The TCF framework was pioneered in 2006 in the UK by the Financial Services Authority and later adopted by the Financial Conduct Authority under the move to a twin peaks regulatory architecture. The TCF framework has already been adopted by several countries including Australia, Canada, India, Malaysia, New Zealand, Singapore and South Africa (World Bank, 2017; Faafoi, 2019; Izaguirre, 2020). The CGAP consumer outcomes framework takes the focus on consumer outcomes a step further than the TCF framework, which has a consumer outcome framing but is still conduct-oriented.

Translating into ten core elements. Together, the elements of the framework make up core elements of financial consumer protection that closely align to the *G20 High Level Principles on Financial Consumer Protection* (OECD, 2011), as outlined in the table below, and which culminate in fair consumer outcomes as a cross-cutting principle:

Element	Principle
1. Legal recognition	Financial consumer protection must be grounded in legislation and regulation in a manner that effectively addresses consumers' risks.
2. Oversight and monitoring	Oversight bodies should be created and empowered to enforce and monitor financial consumer protection, with explicit reference to the need for inter-governmental coordination.
3. Responsible market conduct	Responsible conduct by service providers and their agents should be integrated into FSPs' internal proceedings and in their engagement with customers.
4. Access to information	Regulation should entrench the need for customers to be provided with all relevant information, in an appropriate format, to allow for appropriate customer choice and usage behaviour.
5. Financial education	Dedicated financial education programs and strategies should be set up to increase consumers' knowledge of and skills in navigating financial services.
6. Dispute resolution	Consumers should have access to and knowledge of adequate complaints-handling mechanisms both within businesses as well as through independent or alternative dispute resolution structures
7. Prudential protection	Regulation should entrench the need for consumers' assets to be protected and for FSPs to remain financially sound. Such regulation should be enforced through risk-based prudential supervision.
8. Data protection and privacy	Consumers' financial and personal information should be adequately protected through appropriate control and protection mechanisms.
9. Cybersecurity	Financial service providers (FSPs) should have the relevant controls in place to evaluate, monitor, test and respond to cyber-security risks. Regulatory authorities should ensure that they have the scope and relationships with other authorities and jurisdictions to adequately manage and address cyber-risks.
10. Competitive financial sector	A competition regulatory framework should be in place to ensure a competitive and inclusive financial sector.
Cross-cutting: Fair consumer outcomes	Consumers should be treated equitably, honestly and fairly at all stages of their relationship with FSPs, to lead to fair outcomes from the consumer's perspective.

Table 2. Elements of financial consumer protection in the context of DFS

Source: adapted from OECD (2011), AFI (2010; 2021), CFI (2019), CGAP (2010; 2020), FMT (2016), Gibson (2011), UNCTAD (2016), World Bank (2017).

Equipping policymakers and regulators to address the range of DFS risks. The FCP elements presented above provide a holistic and consumer-centric framework for policymakers to mitigate against the risks presented by DFS. Below, the applicability of the framework elements to the main risk types outlined in Chapter 3 is discussed:

1. ***Increases in fraud risks heighten the need for sound prudential regulation and cybersecurity***. Prudential protection focuses on institutional safety and soundness and the stability of the financial sector. This forms the cornerstone of financial regulatory frameworks globally and is well entrenched in both developed and developing countries alike (OECD, 2018). Globally there has been a shift towards risk-based prudential regulation, however, regulators claim that implementation can be slow and challenging (Cenfri, forthcoming). Cybersecurity involves protecting FSPs and consumers against cybercrimes, a major risk for FSPs which also impacts the safety of consumers' data privacy and financial assets (NIST, 2018). The rise in fraud risk as a result of digitalisation in financial services heightens the need to ensure adequate prudential protection and cybersecurity measures. Prudential protection and cybercrime need to be continually revised in light of new kinds of market players and new ways of conducting financial services to stay relevant in light of trends such as the increasing prevalence of FinTech activity and the use of crypto assets as a medium of exchange (see Box 6). An indication of successful management of fraud risk through prudential protection and cybersecurity will be evident in consumers who feel that their data and assets are safe and secure.

Box 6: Prudential regulation of crypto asset exposure

Crypto assets depend mainly on cryptography and distributed ledger technology and are a digital representation of value which can be used for investment purposes or to purchase goods and services (BIS, 2021).

In response to rapid growth in crypto assets around the world, and the potential for crypto asset activity to cause severe financial market volatility and risks to FSPs, the Bank of International Settlements (BIS) underwent an extensive consultative process to find solutions to effectively address the risks and ensure market stability in line with the actual risks posed. Based on this process it was acknowledged that not all crypto assets pose the same level of market and credit risk and hence two distinct groups have been defined based on the following four core criteria:

1. Either a tokenised traditional asset or an asset with a stabilisation mechanism that effectively links its value to an underlying traditional asset, or pool of traditional assets, at all times.
2. Clearly defined rights, obligations and interests which are legally enforceable in relevant jurisdictions and ensure settlement finality.
3. The design and operation of the functions of the crypto asset, the network on which it operates and the technology on which it is based sufficiently mitigates and manages all material risks.

4. Regulation and supervision of all entities that execute redemptions, transfers, or settlement finality of the crypto asset.

Crypto assets which meet the above criteria should be subject to capital requirements in line with those faced by traditional assets, with further consideration for stabilisation mechanisms and capital add-ons. However, failure to meet the criteria implies a higher level of risk and should face more stringent capital requirements (BIS, 2021).

Technological developments also provide new fraud risk mitigation opportunities. Whilst the discussion has highlighted how technological developments have introduced several new risks, technology is also offering new innovative solutions to sensitize consumers and FSPs to fraud risks as well as monitor and detect potentially fraudulent activity (see Box 7).

Box 7: Using technology to combat fraud risks

Around the world, regulators are finding new and innovative ways to cope with the increasing pressure to identify and create awareness of fraud risks. Some examples noted by CGAP include (Chalwe-Mulenga, et al., 2022):

- The use of AI and machine learning to analyse and identify suspicious transactions by the Monetary Authority of Singapore (MAS)
- The use of natural language processing (NLP) by the Australian Securities and Investments Commission (ASIC) to identify suspicious entities.
- The use of big data analytics and machine learning algorithms by the United States Securities and Exchange Commission (SEC) for fraud and misconduct detection
- A major awareness campaign launched by the central bank and police in the United Arab Emirates resulted in a significant drop in SIM swap fraud

2. ***Increasing pressure to share data needs to be balanced with effective privacy and data protection to manage data misuse risk***. The sharing of data has the potential to vastly improve financial service offerings both through open finance solutions and through feedback loops to policymakers to inform decision-making. However, as a result of increasing data misuse risk, the need for data privacy and protection has become an entrenched consumer right globally. Adequate data privacy frameworks should be grounded in legislation and the relevant regulator must ensure that FSPs and other relevant parties have appropriate controls and protection mechanisms in place to prevent improper use, management and storage by any data holder (OECD, 2011). Effective privacy and data protection will result in consumers feeling safe, respected and fairly treated. Box 8 notes the importance and difficulties of ensuring adequate data protection at the regional level.

Box 8: Regional harmonisation of data protection regulations – the European General Data Protection Regulation (GDPR)

Data protection can be a challenge for firms operating across different jurisdictions as needing to adhere with the most stringent regulation at the firm level can mean a loss of competitiveness in less stringent jurisdictions. Harmonization at the regional level can help to "level the playing field" in this regard (Cenfri, forthcoming).

The General Data Protection Regulation (GDPR) came into effect across the European Union in 2018 to harmonize and strengthen data privacy laws across the region. The regulation stipulates systems and security measures that must be put in place when processing personal data as well as reporting requirements, it gives consumers more control over their data and introduces accountability and sanctions to be imposed for violations (Deloitte, 2018).

3. ***Inadequate redress risk is addressed by giving consumers a more direct voice through various channels***. Effective recourse helps to prevent recourse risks emerging with DFS adoption and usage. Effective recourse channels are accessible, affordable, independent, fair, accountable, timely and efficient. Consumers should be made aware of the relevant recourse channels which should be available both within businesses as well as through independent or alternative dispute resolution structures (OECD, 2011). Recent research in the Southern African Development Community (SADC) noted a rise in the establishment of formal independent dispute resolution mechanisms in the form of financial ombudsmen (Cenfri, forthcoming). There has also been a global rise in the use of informal channels enabled through digital technology such as social media (see Box 9). From a policy perspective, one channel is not necessarily preferable to the other; the most appropriate channel will depend on the nature of the complaints. Rather, policies should focus on ensuring that consumers have access to a complete set of recourse options to ensure that their voice is heard and grievances can be effectively addressed.

Box 9: The use of social media to resolve customer complaints

Social media channels have become particularly effective at reaching wide audiences as they are suited to deliver simple and targeted messages and have become familiar interfaces, particularly for younger generations (OECD, 2021). Although more common in developed countries, the increase in mobile internet connectivity through rising smartphone adoption in the developed world is increasing the accessibility of social media platforms around the world (GSMA, 2022).

Twitter has become a particularly popular complaints channel and has the advantage of holding providers accountable by placing complaints in a public space and creating pressure for grievances to be resolved in very short timeframes. Recent customer service statistics indicate that 64% of Twitter

users prefer to message a dedicated support handle rather than call a business (Porter, 2022).

4. ***Lack of transparency risk can be combatted through the disclosure of information and financial education.*** FSPs and their authorised agents should be required to provide consumers with information on the fundamental benefits, risks and terms of the product, as well as their rights and responsibilities as consumers. Appropriate information should be provided at all stages of the relationship with the customer (OECD, 2011). To ensure that all information is interpretable, consumers should receive adequate education to gain the necessary knowledge and skills to be able to understand the disclosed information. Consumers should also be able to access competent and professional advice and assistance where needed (UNCTAD, 2016). Taken together information disclosure and financial education of consumers work to reduce the risk of lack of transparency. Regulations must be enacted to ensure adequate transparency in this regard and avoid damaging risks such as misleading information or hidden prices (see Box 10). This increases trust in DFS and will result in consumers who feel they can make informed choices.

Box 10: Mandating mobile money price transparency in Kenya

In response to increasing concerns over hidden and unfair pricing of mobile money services, the Competition Authority of Kenya in 2016 mandated all mobile financial service providers to fully disclose transaction costs via users' mobile handsets. A survey of 664 consumers interviewed before and after the regulations had taken effect revealed that whilst previously consumers had thought that the use of financial services was free, despite actually having significant costs attached to them, the new regulation contributed to consumer protection through increasing price awareness across the different financial products and services. Disclosure should be on the same channel through which the transaction is occurring, before execution, in a specified channel and in a manner which can be easily digested and understood by consumers. Mandating transparency is a very low-cost and easy-to-implement policy option (Mazer, 2018).

5. ***Responsible conduct extends from the FSP to also cover the provider's agents and the associated agency risks***. Measures to ensure responsible conduct of FSPs should be tailored appropriately to the contextual setting and the main consumer risks in the market. Responsible conduct of FSPs entails ensuring not only that providers' actions are in the best interests of customers, but also that they are accountable to ensure that all their agents have responsible conduct conducive to fair consumer outcomes. This will help to reduce agency risks which are cross-cutting across the DFS ecosystem. There has been an observed move towards risk-based market conduct supervision, a forward-looking approach borne out of the growing complexity supervisors face in an increasingly interconnected marketplace (see Box 11).

Box 11: Risk based market conduct supervision

Risk-based market conduct is a relatively new concept where supervisory efforts are focused on areas which pose the greatest market conduct risk for FSPs. The approach has become popular in the developed world and is seeing also increasing application in developing countries (AFI, 2016). Out of the available international guidance three key building blocks towards a risk-based market conduct system (Cenfri, forthcoming):

1. **Identify and categorise a set of key market conduct risks** through a consultative process among regulatory authorities and with industry.
2. **Set and track core indicators for market conduct**
    a. Evaluate and adjust onsite and offsite supervisory templates to account for the key risks identified at the individual regulated financial institution level
    b. Also consider alternative data sources such as examinations of the industry environment, product approval requirements, monitoring of financial innovation developments, press releases, contracts, mystery shopping and analysis of customer complaint data, alongside qualitative engagements with market participants themselves
3. **Develop a supervisory strategy to tailor supervisory responses to the risk profile** of the market and individual regulated financial institutions. Consider lower-tiered, proportionate requirements corresponding to low identified risk, and not just heightened requirements for higher-risk institutions or categories of actions.

6. ***Impact on consumer trust from network downtime risks can be managed through effective implementation across the FCP framework.*** Network downtime risk relates primarily to infrastructure quality, rather than financial service provider conduct or financial services oversight. Nevertheless, the fallout on consumer trust of interruptions in service offerings leading to loss of money or failed transactions can be addressed through effective dispute resolution. Likewise, a financial sector characterised by responsible conduct and sound competition is likely to reduce the risk of network downtime impacting consumer outcomes.

5. Policy implications

Ensuring adequate consumer protection in the use of DFS is critical for sustainable development. This policy brief has shown that consumer protection is a core component of the sustainable development agenda, both directly and indirectly, through preventing further marginalisation of vulnerable groups such as women and rural dwellers. With DFS proliferating around the world, appropriate consumer protection measures must be enacted to manage the associated risks and ensure optimal collective socio-economic outcomes.

Need for a risk-based approach focused on principles for positive consumer outcomes. Achieving the financial consumer protection balancing act requires an approach to financial consumer protection that is risk-based, principles-based and centred on positive consumer outcomes. Doing so allows for policies and strategies to remain relevant as DFS evolve and across different country contexts, with minimum restriction being placed on the consumer's ability to access and use DFS. This report has laid out a framework of ten such FCP principles, which culminate in fair consumer outcomes as a cross-cutting principle:

1. Recognition of the importance of consumer protection in the legal and regulatory framework
2. Effective oversight of consumer protection, including market monitoring by regulators
3. Responsible conduct by service providers
4. Access to information by consumers
5. Financial education to build financial literacy
6. Accessible dispute resolution and redress
7. Protection of consumers' assets through effective prudential regulation
8. Privacy and personal data protection
9. Effective cybersecurity measures
10. A competitive financial sector

Coordination and exchange are key for effective principles-based FCP implementation. As technology cuts across boundaries, implementing a holistic and principles-based FCP framework requires a cross-cutting approach spanning several financial sectors and broader government fields. This highlights the need for coordination and exchange within a specific jurisdiction: between different financial regulatory authorities, coordinated by the financial sector policymaker, as well as between the financial sector policymaker and its counterparts in the competition and broader economy-wide consumer protection spheres. It also calls for dialogue involving different stakeholder groups – policymakers, regulators, providers and, importantly, consumers themselves – at the national as well as global levels.

There has already been very positive work in establishing knowledge-sharing platforms to engage on issues relating to FCP. These can form the springboard for even more policy-level engagement and collaboration across countries and stakeholder groups.

Box 12: Knowledge-sharing platforms of relevance to DFS consumer protection

Whilst not the only incidence of such platforms, there are two examples which are particularly noteworthy in the sharing of knowledge on consumer protection as if relates to DFS use:

The Fair Digital Finance Forum

The Fair Digital Finance Forum, hosted by Consumers International, serves to highlight the key challenges facing digital finance consumers. The forum brings together digital finance experts from consumer advocacy, civil society, government, business, and academia through which it aims to accelerate progress towards fair digital finance and to present consumer protection as a catalyst for change (Consumers International, 2022).

The Responsible Finance Forum

The Responsible Finance Forum (RFF) was conceptualized as a community of practice in 2009 through a collaborative effort between the Federal Ministry of Economic Cooperation and Development (BMZ) and the Gesellschaft für Internationale Zusammenarbeit GmbH (GIZ) in Germany together with CGAP the International Finance Corporation (IFC) and the Netherlands Ministry of Finance, in partnership with the wider G20 Global Partnership for Financial Inclusion community. The first annual meeting took place in Berlin in 2010. In 2015, IFC launched the RFF website as a platform to foster information sharing among the community (CFI, 2022).

In 2022 the convening role was transferred to e to the Centre for Financial Inclusion (CFI) who undertook an extensive consultative research process into how the forum can offer more value to its members, how it could be more relevant to DFS trends and macro shocks, how the consumer voice can be more prominent and how discussion outcomes can be taken further to ensure change. The research resulted in three main proposals: (1) to create a platform to aggregate all research on FCP, (2) to continue with the annual convening of the forum but to make it more dynamic by deep diving into specific pertinent topics, and (3) to build extensive partnerships which include consumer bodies and “big techs” (Venkatesen & Totolo, 2022).

The 2022 RFF convening took place virtually on 30th June 2022 with discussions centred around the widening gap in access to finance and financial health, as well as the potential of new avenues to promote innovation in regulating financial services such as regulatory sandboxes and text prints. In light of the new developments in the objectives of the RFF, it should be seen less as an annual event and more as an ongoing platform for engagement and dialogue.

References

AFI, 2010. *Consumer Protection: Leveling the Playing Field in Financial Inclusion,* Kuala Lumpur: Alliance for Financial Inclusion (AFI) Policy Note.

AFI, 2016. *Market Conduct Supervision of Financial Services Providers: A Risk-Based Supervision Framework,* Kuala Lumpur: Alliance for Financial Inclusion.

AFI, 2021. *Consumer Protection for Digital Financial Services: A Survey of the Policy Landscape,* Kuala Lumpur: Alliance for Financial Inclusion (AFI) Survey Report.

AfricaNenda, forthcoming. *The State of Instant and Inclusive Payments in Africa 2022,* Nairobi: AfricaNenda.

Bates, R., 2017. *Banking on the Future: An Exploration on Fintech and the Consumer Interest,* London: Consumers International.

Bates, R., 2017. *Banking on the Future: An Exploration on Fintech and the Consumer Interest,* London: Consumers International.

BDO, 2020. *An Introduction to Robotic Process Autmation,* Cape Town: BDO SouthA Africa.

BIS, 2021. *Prudential treatment of cryptoasset exposures,* Basel: Bank for International Settlements.

Brignull, H., 2010. *Deceptive Design.* [Online]
Available at: https://www.deceptive.design/
[Accessed 06 07 2022].

Cenfri, forthcoming. *Consultancy To Develop Market Conduct Guidelines On Financial Consumer Protection For SADC In Line With International Best Practice,* Cape Town: Centre for Financial Regulation and Inclusion.

CFI, 2019. *Handbook on Consumer Protection for Inclusive Finance,* Washington DC: Centre for Financial Inclusion (CFI), Accion.

CFI, 2022. *History of RFF.* [Online]
Available at: https://globalrff.org/history-of-rff
[Accessed 23 06 2022].

CGAP, 2010. *Consumer Protection Regulation in Low-Access Environments: Opportunities to Promote Responsible Finance,* Washington, DC: Consultative Group to Assist the Poor (CGAP).

CGAP, 2020. *Customer Outcomes to Strive For.* [Online]
Available at: https://www.cgap.org/research/reading-deck/customer-outcomes-strive
[Accessed 03 06 2020].

Chalwe-Mulenga, M., Duflos, E. & Coetzee, G., 2022. *The Evolution of the Nature and Scale of DFS Consumer Risks: A Review of Evidence,* Washington DC: Consultative Group to Assist the Poor (CGAP).

Chio, M., Collins, M. & Patel, M., 2021. *The Internet of Things: Catching up to an Accelerating Opportunity,* San Francisco: McKinsey and Company.

Consumers International, 2021. *The Role of Consumer Organisations to Support Consumers of Financial Services in Low and Middle Income Countries,* London: Consumers International.

Consumers International, 2022. *Fair Digital Finance Forum 2022.* [Online]
Available at: https://www.consumersinternational.org/fair-digital-finance-forum-2022/programme/#welcome--opening-plenaries---1403-
[Accessed 23 06 2022].

Deloitte, 2018. *The General Data Protection Regulation: Long Awaited EU-wide Data Protection Law is Now Applicable,* s.l.: Deloitte Netherlands.

Demirguc-Kunt, A., Klapper, L., Singer, D. & Ansar, S., 2022. *Financial Inclusion, Digital Payments and Resilience in the Age of COVID.* Washington DC, World Bank Group.

Faafoi, H. K., 2019. *New financial conduct regime makes banks and insurers treat their customers fairly.* [Online]
Available at: https://www.fma.govt.nz/news-and-resources/releases-from-the-minister-of-commerce/new-financial-conduct-regime-makes-banks-and-insurers-treat-their-customers-fairly/
[Accessed 24 January 2021].

FMT, 2016. *Consumer protection in SADC Report,* Johannesburg: Finmark Trust.

Gibson, K., 2011. *Case Study: Strengthening Consumer Protection in the South African Microinsurance Market.* [Online]
Available at:
https://finmark.org.za/system/documents/files/000/000/360/original/SACase-Study-Cons.pdf?1614837912
[Accessed 01 November 2021].

Gray, J. et al., 2022. *Open Finance: Prerequisites and considerations for fit-for-context implementation in Africa,* Cape Town: Cenfri.

GSMA, 2022. *State of the Industry Report 2022,* London: GSMA.

GSMA, 2022. *State of the Industry Report on Mobile Money 2022,* London: GSMA.

Herrle, J. & Hirsh, J., 2019. *The Peril and Potential of the GDPR.* [Online]
Available at: https://www.cigionline.org/articles/peril-and-potential-gdpr/?utm_source=google_ads&utm_medium=grant&gclid=CjwKCAjwtIaVBhBkEiwAsr7-c2q_FHRlaFJ39togLEAKeYNRf73QU7jm6ipTQ4sD3FfPoNGvnv04UBoCVaYQAvD_BwE
[Accessed 11 07 2022].

IDC, 2022. *Worldwide Artificial Intelligence Spending Guide.* [Online]
Available at: https://www.idc.com/promo/customerinsights
[Accessed 03 06 2022].

IFC, 2020. *Artificial Intelligence Innovation in Financial Services,* Washington DC: International Finance Corporation (IFC), World Bank Group.

IMF, 2022. *World Economic Outlook Database April 2022.* [Online]
Available at: https://www.imf.org/en/Publications/WEO/weo-database/2022/April
[Accessed 06 07 2022].

ITU, 2021. *Connectivity in the Least Developed Countries: Status Report 2021,* Geneva: International Telecommunication Union.

Izaguirre, J. C., 2020. *Making Consumer Protection Regulation More Customer-Centric,* Washington, D.C.: CGAP.

Mathur, A., Mayer, J. & Kshirsagar, M., 2021. *What Makes a Dark Pattern... Dark?.* Yokohama, CHI Conference on Human Factors in Computing Systems (CHI '21), May 8–13, 2021.

Mazer, R., 2018. *Does Transparency Matter? Assessing the impact of improved disclosure in digital financial services in Kenya,* Washington DC: CGAP.

McKee, K., Kaffenberger, M. & Zimmerman, J., 2015. *Doing Digital Finance Right: The Case for Stronger Mitigation of Customer Risks,* Washington DC: Consultative Group to Assist the Poor.

Microsoft, 2021. *Microsoft Digital Defense Report,* Washington DC: Microsoft.

Mohammad, G. & Pelupessy, A., 2017. *Emerging Risks and Customer Protection in Digital Financial Services in Indonesia,* Lucknow: Micro Save Consulting.

NIST, 2018. *Cybersecurity Framework Version 1.1.* [Online]
Available at: https://www.nist.gov/cyberframework/framework
[Accessed 15 01 2022].

OECD, 2011. *G20 High-Level Principles on Financial Consumer Protection,* Paris: Organisation for Economic Co-operation and Development.

OECD, 2011. *G20 High-Level Principles on FInancial Consumer Protection,* Paris: OECD.

OECD, 2016. *Consumer Protection in E-commerce,* Paris: Organization for Economic Co-operation and Development (OECD).

OECD, 2018. *Financial consumer protection risk drivers: a framework for identification and mitigation in line with the high-level principles on financial consumer protection.* [Online]
Available at: https://one.oecd.org/document/DAF/CMF/FCP/RD(2017)3/FINAL/en/pdf
[Accessed December 2021].

OECD, 2021. *Digital Delivery of Financial Education: Design and Practice,* Paris: OECD.

Porter, S., 2022. *How Twitter has become a key customer support channel.* [Online]
Available at: https://business.twitter.com/en/blog/how-twitter-has-become-a-key-customer-support-channel.html
[Accessed 07 06 2022].

Remolina, N., 2022. *The Role of Financial Regulators in the Governance of Algorithmic Credit Scoring,* s.l.: Singapore Management University, Centre for AI and Data Governance Working Paper 2/2022.

Statista, 2022. *Retail e-commerce sales worldwide from 2014 to 2025.* [Online]
Available at: https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/
[Accessed 06 07 2022].

UN DESA, 2021. *World Social Report 2021: Reconsidering Rural Development,* New York: United Nations Department of Economic and Social Affairs.

Una, G., Allen, R., Pattanayak, S. & Suc, G., 2020. *Digital Solutions for Direct Cash Transfers in Emergencies,* Washington DC: International Monetary Fund.

UNCTAD, 2016. *United Nations Guidelines for Consumer Protection,* Geneva: United Nations Conference on Trade and Development.

UNCTAD, 2016. *United Nations Guidelines for Consumer Protection,* Geneva: The United Nations Conference on Trade and Development.

UNCTAD, 2017. *Achieving the Sustainable Development Goals through Consumer Protection,* Geneva: United Nations Conference on Trade and Development.

United Nations, 2015. *Transforming Our World: The 2030 Agenda for Sustainable Development,* Geneva: United Nations.

Venkatesen, J. & Totolo, E., 2022. *Interview with CFI Accion as Convenors of the Responsible Finance Forum* [Interview] (30 05 2022).

Visa, 2021. *eCommerce developments across Sub-Saharan Africa (SSA),* s.l.: Visa Consulting & Analytics.

World Bank, 2017. *Good Practices for Financial Consumer Protection, 2017 Edition,* Washington DC: The World Bank.

World Bank, 2020. *Digital Financial Services,* Washington DC: The World Bank Group.

World Bank, 2021. *The Global Findex Database 2021,* Washington DC: The World Bank.

World Bank, 2022. *Financial Inclusion and Consumer Protection.* [Online] Available at: https://responsiblefinance.worldbank.org/en/responsible-finance/financial-consumer-protection#:~:text=Financial%20consumer%20protection%20encompasses%20the,consumers%20in%20the%20financial%20marketplace.
[Accessed 03 06 2022].

Appendix: DFS consumer risk framework

The table below provides a more detailed breakdown of the CGAP digital financial services consumer risk framework published in 2022:

Broad risk types

Fraud	Data Misuse	Lack of Transparency	Inadequate redress
• Mobile app fraud / phone espionage*	• Artificial intelligence (AI)-related risks - Algorithmic bias*	• Incomplete/unclear pricing information	• Incomplete/unclear pricing information
• Biometric identity fraud*	• Unfair practice	• Unfair practice (e.g., selling unsuitable product, aggressive marketing/cross-selling, abusive debt collection practice such as social shaming)	• Unfair practice (e.g., selling unsuitable product, aggressive marketing/cross-selling, abusive debt collection practice such as social shaming)
• Authorized push payment (APP) scams*	• Privacy intrusion	• Complex / confusing interface / menu	• Complex / confusing interface / menu
• Synthetic identity fraud*	• Opaque decision making	• Inaccessible terms/fees, including complicated disclosure format	• Inaccessible terms/fees, including complicated disclosure format
• SIM swap / account takeover fraud	• Data breach (+ amplified cyber risk)	• Inability to compare products	• Inability to compare products
• Internal fraud	• Uninformed consent	• Unexplained / hidden / undisclosed fees	• Unexplained / hidden / undisclosed fees
• Card fraud	• Inaccurate profiling and no data integrity	• Data handling practices not disclosed	• Data handling practices not disclosed
• Unlicensed digital investment / Ponzi scheme	• Matthew effect	• Complex legal language and excessive information that overloads/confuses consumers	• Complex legal language and excessive information that overloads/confuses consumers
• Social engineering fraud	• Liability allocation risk	• No notice regarding referrals	• No notice regarding referrals
• Social media scam	• DFS provider failure to safeguard customer personal data	• Product's inherent risks not communicated to customer	• Product's inherent risks not communicated to customer
• Money transfer	• Customer failure to safeguard personal data - Business Email Compromise scam victims	• Misleading advertisement	• Misleading advertisement
• Mobile browser fraud/pharming	• Data handling practices not disclose		
• Counterfeit device			
• Infrastructure compromise			
• Mobile device theft/sharing of devices			

Cross-cutting risk types

Agent issues	• Fewer female agents • Social norms • Fewer rural agents • Fraud/overcharging/fee markup/unauthorized fees • Access to customer PIN (theft/compromise) • Poor dispute resolution by agents • Limited product awareness	• Manipulation of customers • Unfair treatment of customers/discrimination based on social status • Insufficient agent liquidity that may lead to transaction splitting, denial of transactions, or bulk payments • Untrained and unmonitored agents
Network downtime	• Distributed denial of service (DDS) attacks • Inadequate DFS infrastructure • Insufficiently tested system upgrade • Power outages • Inadequate disaster recovery and business continuity plans • Risky customer behavior (e.g., leaving cash, PIN, or phone with others)	• Incomplete and interrupted transactions/inaccessible funds • No confirmation message – duplicate transactions • Unresolved complaint (e.g., agent/service provider fails to check transaction status or connect with provider

Figure 4. Detailed breakdown of DFS risk categories

Source: (Chalwe-Mulenga, et al., 2022)