FMO
Entrepreneurial
Development
Bank

Mitigating Consumer Risks in a Digital Age

Recommendations for funders

The Hague | 16 December 2021

Authors:
Isabelle Barrès
Hema Bansal

Table of contents

Introduction

For the last decade, responsible financial service providers and funders have been working hard to mitigate consumer risks. Given the accelerating pace of deployment of digital financial services and digital business models, it is time to review and update existing guidance.

First, the good news. The Consumer Protection Principles[1], widely used in financial inclusion as a reference for mitigating consumer risks, are still relevant in a digital world. Digital financial services still need to meet client needs, be priced responsibly and be delivered in a fair and transparent manner. And, now more than ever, clients need feedback and complaints channels to continue to ensure that financial services provide the value intended. Another positive development is a growing global ecosystem of stakeholders which are concerned about protecting consumers from harm and ensuring that they truly benefit from increased access and usage of financial services. From regulators to funders and providers, there are a plethora of initiatives working to catch up to digital risks.

This brief complements the existing body of knowledge on consumer protection by providing a perspective on the main consumer risks linked to digital services and recommending a series of actions that providers and funders can start taking immediately. It is based on research conducted by FMO in 2021 that included a comprehensive desk review of the main business models for delivering digital payments, digital credit and Pay-as-you-Go (PAYGo) financing for the off-grid solar sector as well as consultations with industry experts and FMO portfolio companies. Starting in 2021 and going into 2022, FMO will integrate the recommendations into a flexible consumer protection framework.

1 Consumer risks and mitigation

A shift to a digital environment profoundly affects consumer risks in four main areas: product, partners & agents, technology, and data.

The digital revolution changes everything, for everyone. There are new providers, new business models, and new products flooding every part of the globe. These changes, while already significant, are taking place against the backdrop of three fundamental shifts that are particularly relevant for financial inclusion: 1) direct customer interactions with the financial product rather than the financial service provider and 2) increased reliance on customer data and 3) reliance on channels to move back and forth from cash to digital currency.

From a client perspective, the digital revolution has the potential to increase choice and access, but it also creates more confusion, raises issues of trust, and exposes customers to new forms of vulnerability and abuse. As we reflect on new risks, we are reminded of the

[1] https://www.centerforfinancialinclusion.org/detailed-guidance-on-the-client-protection-principles

importance to adopt a client-centered approach as ultimately policies and practices that matter the most are the ones that produce the desired client outcomes.[2]

1.1 Products

In an analog world, consumers interact with human beings when dealing with financial services, whether it's to inquire before making a purchase, get on-boarded, access the service or seek redress if something goes wrong. In a digital world, things are dramatically different. A key characteristic of a digital environment is the ability to automate transactions and as a result clients interact primarily with the product interface.[3] From a client perspective, the lack of interactions with human beings is the first key distinguishing factor of digital financial services and this has profound implications for consumer protection. As machines replace humans, we have an opportunity to program them to surpass human performance, correct human flaws and provide customized and excellent customer service. But we also run the risk of increasing harm to clients, by introducing new risks. Let's explore further.

1.1.1 What can go wrong?

- **Products don't include protection by design and by default**. Many client safeguards previously ensured through interactions with staff now need to be handled by the product itself. A key risk is that products don't adequately replace these functions. For example, digital credit product interfaces fail to convey complete information on the product terms and conditions, client rights, or complaints channels, or fail to confirm client understanding.
- **Humans are nowhere to be found.** Even in the best-case scenario with well-designed products, there will be instances where clients want or need to talk to someone. A key risk is that clients can't interact with a human being and can't use the product.
- **Products don't meet client needs.** Another key risk, especially relevant for vulnerable populations, is that the product is not 'fit for the target market'. For example, it uses technology that is not available to clients or uses a technology that clients are not comfortable with or do not trust.
- **Digital credit business models are built on high default rates.** Algorithm-based digital credit decisions anticipate high losses in the early days, when the algorithm is in 'learning' mode. Early defaulters face the consequences (i.e., fees, penalties, blacklisted in the credit bureau) when they should not have gotten approved in the first place.

1.1.2 How to prevent consumer risk and support good outcomes?

- **Embed protections and balance "tech and touch" in product design.** Products should be designed to give clients a voice and allow them to make informed choices. Terms and conditions should be complete, transparent and easy to understand, and feedback and complaints channels easy to use. While clients can be encouraged to use automated systems or chatbots, they should have the choice to access human assistance.

[2] https://www.cgap.org/blog/its-time-change-equation-consumer-protection
[3] https://www.centerforfinancialinclusion.org/what-is-lost-in-a-digital-financial-world-and-how-to-get-it-back

- **Adopt a client-centered approach to product development**.[4] Financial service providers should be sensitive to the extent to which their target market is "digital-ready": What communication networks and devices do they have access to? Do they own or borrow the devices? What is their level of comfort with technology? How is product design increasing financial capability?

1.2 Partners & Agents

Technology innovations are making it both possible – and sometimes necessary – for financial service providers to partner with others. While this increases the range of services available to consumers, it also leads to more dependencies amongst partners and more complexity. Two notable partners for digital financial services are mobile network operators (MNOs) and agent networks. Agents are key when considering consumer risks, as they directly support consumers in moving cash to and from digital channels. Many of the key risks and recommendations are therefore focused on client interactions with agents.

1.2.1 What can go wrong?

- **Choosing the wrong partners.** An overarching risk when dealing with external partners is that they will not uphold the same consumer protection standards as your own. Finding good partners to work with is more difficult in environments with low levels of competition. It is also harder to hold partners accountable if the financial service provider has no ownership stake (i.e., hired vs owned agent networks) or if the partner is not incentivized by other players to uphold consumer protection standards (i.e., MNOs that are incentivized to be certified by GSMA)[5].
- **Lack of accountability.** A key risk in business models that rely on multiple partners is confusion on who is accountable when things go wrong, and confusion on the client part of who to reach out to if there are questions or complaints.
- **Abusive behaviour from agents**. A key risk with agent networks is misaligned incentives and resulting abusive behaviour, for example in the case of sales and recovery targets that incentivize agents to oversell and adopt abusive collection practices. As for providers, incentives should encourage quality growth and distinguish intent and ability to repay in case of late payments.

1.2.2 How to prevent consumer risk and support good outcomes?

- **Protect and train agents.** Agents need to be supported in meeting their own challenges so that they are equipped to protect clients. They should be remunerated fairly, treated respectfully and adequately incentivized. Agents should be trained to interact with clients in a respectful way that upholds their own code of conduct and financial service providers should monitor agent practices to confirm adherence to the code of conduct and take corrective action if needed.

[4] http://customersguide.cgap.org/
[5] https://www.gsma.com/mobilefordevelopment/mobile-money/certification/

- **Partner with responsible players.** When there is a choice, favour partners that have demonstrated commitment to consumer protection (i.e., certified financial service providers)[6].
- **Inform clients on who is accountable.** Clients need to have clarity as to who they should interact with if something goes wrong, who they have a contractual relationship with and who is responsible for what. Without clear accountability, clients are at risk of being referred back and forth amongst partners who do not want to deal with the issue.

1.3 Technology

Financial services innovations are based on two main underlying technologies: Distributed Ledger Technology (DLT) (i.e., blockchain, crypto assets, etc.) and Artificial Intelligence (AI) (i.e., machine learning for decision making and advising, algorithms, chatbots, etc.).

1.3.1 What can go wrong?

- **Innovations are not client centric.** A key risk with some innovations is that they don't consider the client perspective. An example is the use of machine learning algorithms to automate credit decisions, which don't adequately capture debt capacity and debt stress. Rather than aiming to avoid over indebtedness, they are designed to minimize losses and protect lenders. In the excitement around the potential to increase access and reduce costs, the risk of increased over-indebtedness is overlooked.
- **Technology is leveraged for unethical purposes.** The use of technology makes it easier for unscrupulous providers to take advantage of human biases and benefit the company vs clients (i.e., through aggressive push marketing or through data privacy defaults options that are set to share all client data with partners).
- **Technology amplifies harm**. Technology can do as much harm as it does good depending on what it is used for, and it can amplify bad decisions or bad behaviours, by allowing them to scale very quickly (i.e., bias and discrimination).
- **Excitement around technology is blindsiding.** Using technology for "good" requires up-front commitment and on-going monitoring. Beyond purposefully using technology to manipulate clients and engage in predatory sales or deceptive marketing, even some well-intentioned uses of technology can backfire. Examples include using machine learning algorithms to create credit files for the "credit invisible" and unintentionally discriminating on the basis of protected variables such as age, gender or race; or leveraging the immutable nature of blockchain records to make transactions safer while at the same time preventing the correction of legitimate errors.

1.3.2 How to prevent consumer risk and support good outcomes?

- **Adopt a client-centered approach to technology.** Do a comprehensive analysis of both value and risks to consumers. Formulate desired outcomes (i.e., expand access while reducing over indebtedness), monitor (i.e., track level of debt stress) and adjust parameters as needed. Also ensure that tech staff is sensitized to consumer risks.

[6] https://sptf.info/client-protection/client-protection-certified-institutions

- **Commit to ethical use of technology.** Ethical guidelines for various technology applications, such as the "Ethics guidelines for trustworthy Artificial intelligence"[7], are increasingly being developed and ethical considerations are gaining traction. Concrete recommendations are emerging on what is "ethical AI", and a growing body of work is calling for "responsible, inclusive, equitable design".[8] Another growing consideration is the impact of technology on the environment (i.e., the blockchain use of energy).
- **Increase awareness on technology-related risks.** Evaluate the extent to which financial service providers are aware of potential issues linked to the technologies they are using, and how they are mitigating for the related risks, especially when regulatory frameworks are nascent or inexistent. For example, providers wanting to expand their savings mobilization should pay special attention to the client facing risks of unregulated savings mobilization (i.e., apps allowing clients to store their savings in crypto assets that are not backed up by reserve funds) and ensure that client funds are not at risk.
- **Evaluate the suitability, feasibility and appropriateness of a given technology**. To get beyond the hype, there should be a "fit for purpose" analysis and a clear understanding of how technology will help financial service providers reach their objectives.[9]
- **Increase transparency on intended value creation with technology.** Providers should state their intentions clearly and demonstrate how they will protect client interests. For example, providers who heavily discount their pricing to gain early market share should be clear in how pricing will evolve as the product matures.

1.4 Data

Automated processes and interactions rely on data. Data is what enables to take humans out of the equation and teach machines what to do when human beings are not involved. Whether it's to teach machines how to support customers (via the use of chatbots) or to teach machines who to lend to (via the use of algorithms), we need data. To offer a wider range of digital financial services to existing clients and to extend digital financial services to new clients, we are leveraging more and more client data (whether it's personal, behavioural, transactional) to attempt to program the best possible decisions. Potentially everything clients do, whether or not it's related to their financial transaction, can generate data that could be used for making financial decisions. We are already seeing this with how they interact with their friends and family (with social network data or phone records). As there is an increased reliance on data, it is critical to handle and use it responsibly.

1.4.1 What can go wrong?

- **Providers sell client data.** A key risk linked to data privacy is the incentive for financial service providers to sell client data and put clients at risk of financial loss or security issues.

[7] https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

[8] https://www.usaid.gov/sites/default/files/documents/Vital_Wave_USAID-AIML-FieldGuide_FINAL_VERSION_1.pdf

[9] https://www.usaid.gov/sites/default/files/documents/15396/AI-ML-in-Development.pdf; https://www.usaid.gov/digital-development/digital-finance/blockchain-primer

- **Increase in fraud and cybercrime.**[10] Cyber-related risks are the most challenging for financial service providers to tackle alone. Challenges are due to many factors, including a lack of awareness of the vulnerabilities that financial services are exposed to (and exposing their clients to) and the lack of internal resource and know-how to tackle the issue. Central Banks and Fintech associations are well-aware of key vulnerabilities within their markets even if they cannot properly measure the extent of the risks. Getting consistent and comprehensive data is very difficult and is a key blind spot for financial inclusion.[11] This key risk is compounded by the fact that financial service providers are ill-equipped to handle the sophistication and complexity of systems that need to be put in place to prevent fraud and cybersecurity attacks.
- **Customers make uninformed decisions related to their data**. Clients make decisions not fully understanding the trade-offs of giving up their rights or make decisions out of lack of real options. This issue has been highlighted for example with disclosures: it is not sufficient to disclose when and how data will be shared if clients don't have options to choose from (i.e., if the decision is a binary decision to share all data and access the service or not). We need to move away from a 'buyer beware' mentality.

1.4.2 How to prevent consumer risk and support good outcomes?

- **Use data responsibly**. Whether for design, underwriting, marketing and cross sell, use data responsibly and for the benefit of clients. For example, while there can be significant incentives for providers to share and monetize client data, responsible providers should not adopt practices linked to monetizing client data and should keep client data private.
- **Go beyond data protection policies.** Data policies are only as good as the outcomes they generate, and despite the advancements in data protection frameworks (i.e., the European Union's Global Data Protection Regulation or GDPR), there is still much to do to ensure that clients have agency around their data. For example, "client consent" as we know it is broken.[12] Providers should give clients a real, meaningful choice when asking for consent rather than trading privacy for basic access.
- **Get help to keep data secure.** Protecting the security and integrity of client data is an enormous challenge for financial service providers who are not equipped to handle the sophistication and complexity of systems that need to be put in place to prevent fraud and cybersecurity attacks. Providers should leverage joint resources (i.e., ACRC-Cybersecurity Resource Centre[13]) to support adequately handling the risks without jeopardizing their sustainability. It is recommended that Fintech companies and off-grid solar PAYGo companies leverage pooled resources to tackle these risks, and that more research be done to highlight the sector's vulnerabilities. Investees could also be linked with ACRC to have access to much needed and often missing data security and integrity know-how, as ACRC aims to provide collective resources to strengthen the cyberhealth of

[10] https://www.cgap.org/blog/evolving-nature-and-scale-consumer-risks-digital-finance

[11] https://cyber4africa.org/articles/what-are-the-cybersecurity-challenges-for-the-african-financial-sector/

[12] https://www.cgap.org/blog/data-protection-and-financial-inclusion-why-consent-not-enough

13 https://cyber4africa.org

the financial inclusion sector in ways quite similar to what the Smart Campaign[14] did for consumer protection over the last decade.

2 Recommendations for funders

Following are a few key recommendations for funders trying to address increasing consumer risks in a digital world. Funders have both an opportunity and responsibility to act quickly.

With a lack of adequate regulatory frameworks to protect digital financial consumers, a growing offer of innovative products at a global level and new actors chasing the next unicorn and pushing for quick returns and fast growth, the digital finance environment is both full of promise and risks for consumers, especially vulnerable consumers new to finance or digital. Funders should use their influence to foster a responsible ecosystem and encourage responsible practices by providers, starting with influencing digital(izing) providers to align with guidance to mitigate consumer protection risks as highlighted in the previous section. A few additional recommendations follow.

2.1 Increasingly analyze context

Understanding the market conditions for digital financial services is critical to identify where funding can be most catalytic, by helping to answer the following questions: Where can providers improve products and practices? Where are they limited by lack of a common playing field that puts them at a disadvantage if they are first movers? What is outside of their sphere of influence and should be addressed at the market level?

- **Digital readiness and capability.** Demand estimates should not only consider appetite for products, but also client segmentation and level of "digital readiness" of targeted clients (i.e., access to communication networks and devices). Trends on access to communication technology can be indicative of how demand is likely to evolve and should also be taken into consideration. Digital capability also matters a great deal for companies targeting low-income populations.
- **Partnerships.** An analysis of the landscape of potential partners (MNOs, agent networks, Fintechs) is particularly important, as financial service providers often rely on a variety of partners to bring their digital product to market, whether to outsource activities (i.e., complaints management, underwriting, collections, etc.) or access the technology rails needed to support the product (i.e., MNOs). Understanding the universe of companies available for financial service providers to partner with helps to understand the extent to which they can choose partners and influence their practices.
- **Competition and market saturation**. An analysis of the competitive landscape and market saturation should consider whether consumers have access to responsible

[14] https://www.centerforfinancialinclusion.org/about/what-we-do/the-smart-campaign

providers and products. A market saturated by harmful products leaves room for new responsible products to replace them.

- **Funding landscape**. The excitement around digital innovations is attracting a new wide range of funders with more commercial orientation and less knowledge and understanding of unbanked and underbanked populations. Attracted by the promise of high returns and serving a very large untapped mass market, they are particularly risky for low income, vulnerable populations. An analysis of the funding landscape can help orient responsible funders where there is more urgent need for such funding.

2.2 Build knowledge

Consumer protection standards for digital financial services are only emerging. There is therefore a higher level of uncertainty around risks and proven mitigation strategies. In this context, it is more important than ever to encourage sharing of experiences to contribute to emerging standards and improve mitigation strategies.

- **Create internal feedback loops and document learnings.** This is needed to ensure that funders consumer protection frameworks benefit from the collective experience of the various internal teams as well as from investee feedback. Staff should share consumer protection advances and learnings across internal teams, with investee and with shareholders and be a champion for consumers when representing the funder on companies' boards. Learnings about products, business models, providers, channels and their corresponding consumer risks and mitigation should be documented and added to the funder consumer protection framework over time and create a pathway for embracing consumer protection in the investment cycle.
- **Review and restate expectations with portfolio companies**. Acknowledge that for some areas (i.e., technology-related risks), we are in earlier experimentation mode in terms of risk identification and mitigation. This implies a stronger focus on transparency, which is critical to understand emerging business models. Potential investees should be ready to share as much information as needed on their business model, projections, and intentions (i.e., what are they programming their technology to do, their machine learning algorithms to optimize?)
- **Sensitize investees and partners to consumer protection.** This is especially important if they are new to the financial inclusion space and less familiar with the industry conversations. Encourage investees to join industry initiatives (see next section) to demonstrate their commitment to consumer protection and contribute to shared learning to advance standards. While it is not expected that all investees will be able to do this at all stages of the company's life, they should demonstrate that they take these efforts seriously.
- **Develop and agile consumer protection framework.** Adopt more frequent consumer protection tools update cycle where the guidance can be amended on a regular basis (i.e., semi-annually) to reflect the feedback from due diligence, investees and new industry standards.

2.3 Support and leverage industry efforts

As standards for digital financial services and their providers are still evolving, there are various ways in which financial service providers and funders can support industry efforts and demonstrate their commitment and alignment with consumer protection best practices.

- **Encourage investees and grantees to contribute to industry initiatives.** There are many on-going initiatives to develop guidance and standards and these initiatives need the participation of companies involved in providing services to the end clients. There is a tremendous need for information on practices and pricing and funders should encourage their investees (even require if possible) to participate in these efforts by sharing their pricing and performance data, even if on an anonymized basis. Industry efforts vary widely at the local level but are increasing. At the global level, the main industry initiatives are: 1) Digital financial services consumer protection guidelines, led by the global non-profit organizations Social Performance Task Force (SPTF)[15] and CERISE[16]; 2) Transparent pricing, led by MFR through the ATLAS project[17]; 3) Consumer protection for off-grid solar financing sector, led by GOGLA, the global association for the off-grid solar energy industry[18].
- **Share insights and experience with the industry**. The due diligence process is a great opportunity for learning and documenting risks and practices (good and bad) to inform future standards. This provides an opportunity to contribute to the knowledge base around emerging industry standards for digital financial services.[19].
- **Fill research gaps.** Commission research on under-researched consumer risks (i.e., joint research with the ACRC-Cybersecurity Resource Centre for Inclusive Finance to identify the level of cyber risk that investee companies are exposed to).
- **Support cyber risk mitigation**. For example, a funder could partner with the ACRC-Cybersecurity Resource Centre for Inclusive Finance[20] to assess the maturity of pool of its Fintech portfolio companies and identify the most frequent weaknesses and needed action plan. The Cybersecurity Flash diagnosis offered by ACRC is a very interesting tool to raise awareness in a very practical way for boards and provide concrete recommendations for companies. Given the lack of standards in this area, it would also help to determine what is reasonable to add in the due diligence process, and the project could result in the identification of appropriate synthesis KPI that have to be included in the due diligence.

[15] https://sptf.info
[16] https://cerise-spm.org/en/about/
[17] https://www.mf-rating.com/products/atlas/
[18] https://www.gogla.org
[19] The effort to develop industry led standards for financial consumer protection in a digital world is currently led by SPTF and CERISE, who are overseeing the work of the Smart Campaign since the end of 2020, when the Smart Campaign closed and the body of knowledge was transferred to them.
[20] https://cyber4africa.org/