STANDARDS FOR RESPONSIBLE DIGITAL FINANCIAL SERVICES

15 February 2022

CERISE + SPTF
Standards for Responsible Digital Financial Services

(Draft as of 15 February 2022)

PURPOSE

Identify management standards for financial service providers (FSPs) seeking to offer digital financial services (DFS) responsibly. We see the risks. Let's find solutions.

> *"The idea of standards is very compelling. We have so many frameworks and so many principles. They are always focused around risks, but it's hard to orient them around solutions." – DFS Expert*

OVERVIEW OF SPTF'S WORK SO FAR

- Interviewed about 40 experts, from various countries and stakeholder groups
- Reviewed DFS guidelines, frameworks, and standards proposed by others
- Read research papers, blogs, case studies, and other related documents

ORGANIZATION OF THIS DOCUMENT

- **13 thematic categories for standards**. Each section contains both ideas for standards and some "Other thoughts" shared by experts that can nourish the discussion:
    1. Agent management
    2. Algorithm bias
    3. Complaints Mechanism
    4. Cybersecurity
    5. Data rights / privacy
    6. Fair and respectful treatment of customers
    7. Fraud
    8. Outcomes
    9. Partnerships
    10. Prevention of overindebtedness
    11. Product design and delivery
    12. Responsible Pricing
    13. Transparency
- **Additional discussion topics**. During the interviews, some common concerns arose that did not fit neatly into a single standards category but seemed important for the working group to discuss. This section presents ideas we heard in the following areas:
    a) financial inclusion of those who struggle to use technology
    b) responsible treatment of employees and DFS
    c) interoperability
    d) the role for country- or region-wide actors
    e) the importance of governance
    f) customer trust
    g) prioritization within standards development work

DRAFT STANDARDS

/1/
Agent management

1. Before launching an agent network, create a strategy for managing agent liquidity in each market, at minimum for urban versus rural markets. Some (optional) ideas:
    a. Figure out in advance before launching an agent network what you can do to help agents manage liquidity. Leverage technology in your solutions.
    b. Study in advance the liquidity in various businesses and choose the ones that have sufficient cash to be agents.
    c. Train customer service agents on what your liquidity shortage response actions and timeline will be, so when they receive complaints, they have a response.
    d. Figure out whose job it is to resolve the issue.
    e. Be aware of seasonal increases in demand. Knowing the level of activity, on average, per season, gives you data on how much liquidity is sufficient.
2. Raise awareness among customers that they may encounter insufficient liquidity among agents and the implications of that on how they plan or manage their financial lives.
3. Improve the IT system as needed to enable remote monitoring of agent activity.
4. Measure the level of activity for agents on a regular basis. This includes not only what types of transactions, how frequently, and in what amounts, but also which platform/app they use to conduct each transaction.
5. Monitor which agents have high cash outs and take action to ensure liquidity in places where there is a large volume of cashing in and out.
6. When a new digital product launches:
    a. Select agents for the pilot test that are among the most active in the network
    b. Establish targets, incentives
    c. Launch an awareness raising program
    d. Provide more than one round of training for agents on the new product
    e. Track data on how many agents are aware of or using the new product.
7. Use data to monitor early warning sights of agent distress, rather than waiting for actual default or other bad behavior by agents.
    a. (Optional) ideas for indicators to use to monitor whether an agent is successful:
        i. # opting in / registered
        ii. # active users
        iii. Default rate
        iv. Value ($) of total transactions
        v. Number of transactions per month
        vi. Revenue earned by agents
8. Conduct annual satisfaction survey with agents.
9. Invest in ongoing agent training and evaluation. (NB: Agent turnover can be high, and some agents are better than others.)
10. Provide refresher trainings to agents on important topics. Training them once on a key topic is not enough.
11. Train agents on how to avoid fraud.
12. Build agent buy-in to the mission and vision of the organization through continuous engagement

   a. Examples: share success stories via a newsletter; offer recognition awards
13. Have a business plan that allows for agents to make money. Considerations include what incentives the FSP will offer to agents and how many agents are appropriate in one area given demand. Assure that their work as an agent can give agents sufficient income.
    a. The FSP may need to cross-subsidize rural agents with urban ones.
    b. USAID case study: Lonestar Cell MTN (Liberia) negotiated the commission percentages that would work for the various actors involved while providing sufficient profit to Lonestar Cell MTN as well.
14. Offer agents a good base salary.
15. Invest in experiential learning. Have your staff who are going to be responsible for agent management go into the field and observe how agents work.
16. Make it possible for customers to use agents with their same gender, as evidence shows they prefer this.
17. Analyze customer complaints data for insights on agent behavior.
18. Tell customers that if agents ask you to pay fees that you do not understand, the FSP wants to know about it and here is the channel to use to report this.
19. Agents should have to enter data on all requested transactions, even ones they cannot do due to insufficient liquidity. The FSP should get this information on a daily basis, so they see how many transactions happened and how many transactions were requested but not processed due to insufficient liquidity.
20. Define a theory of change for agents. What does the FSP provide (e.g., trainings, incentives, oversight) and how do the agents perform as a result?
21. Have a probationary period with agents to test their performance before co-branding with them.

Other thoughts:

- This is an iterative process. After market research, pilot, and launch, expect to need more research and more adjustments with agent network
- Many advised that the FSP should train, recruit, and incentivize agents to position them best to help the FSP achieve customer-centric results, but noted that we need more specific ideas on how to do this.
- Make sure you're leveraging technology to help agents in the network.

/2/
Algorithm bias

1. If outsourcing algorithm development:
   - Inform your development partner of target customers and discuss a strategy to avoid algorithmic discrimination.
   - In the service agreement, do the following:
     i. Define parameters for algorithm
     ii. Require that the partner will annually check for algorithm's accuracy (e.g., check whether the algorithm's decisions on loan sizes for target customers are the same that traditional repayment capacity analysis would make).
     iii. Require the partner test for bias at least annually

iv. Either require the partner to share the process they undertook to design the algorithm OR require them to certify or demonstrate a lack of bias.

2. If developing the algorithm in-house, credit officers and management take part in the development of algorithm design.
3. If you have information technology (IT) specialists developing your algorithm, train them on your mission and vision and target customers so they understand the context in which the algorithm will be deployed.
4. Before you launch using an algorithm, use synthetic or real data to test who gets approved for what product, and for what amount.
5. When testing whether your algorithm is biased, do the following:
   - Select customer segments that are relevant to you and analyze them separately to see whether the algorithm treats them equally (e.g., men vs. women, rural vs. urban)
   - Select the criteria you will use to understand whether the algorithm is biased.
     i. Example from WWB paper: "Statistical parity: Subjects in protected and unprotected groups have an equal probability to be in the positive predicted class.
6. Test whether your data are biased. Sometimes bias comes from the dataset, not the algorithm.
   - For example, if more men than women have Smartphones, the majority of the data you extract from phones will relate to men and not women.
7. Use information from customer complaints to inform your review of algorithm function.
   - Examples of relevant complaints: a) a customer complains she didn't get as big of a loan as her neighbor; b) a customer says it's been months and she hasn't been offered a larger loan size.
8. If you find that bias exists, determine if it is coherent with your social goals and strategy.
   - Note: It is not necessarily desirable to eliminate bias, as you may want to prioritize serving certain populations, and this is a form of bias.
9. Have at least one employee who is able to read any algorithm you use.
10. Monitor / check your data daily to determine whether there is no bias (done either in-house or by the algorithm provider).
11. Prepare reports, at minimum quarterly, on algorithm function. Analyze at minimum this:
    - Who is being approved, by customer segment, and compare who is actually being served with the market that you are wanting to serve.
    - Whether the algorithm is accurate (e.g., check whether the algorithm's decisions on loan sizes for target customers are the same that traditional repayment capacity analysis would make)
12. Share reports on algorithm function with senior management, credit department, the risk management team, and the board of directors; discuss results and identify potential bias.
13. In cases of a systemic shock (e.g., a pandemic), discontinue the algorithm and review it.
14. Management reviews the algorithm function at least once per [X time period] to make sure it is comfortable with the balance between fairness and efficiency that the algorithm achieves.
15. At least some members of the management team represent the population whose data are being scored by the algorithm. Their cultural knowledge can identify factors in the data that might bias or discriminate.
16. Do not use algorithms if you do not have the capacity to make sure they are not biased.

Other thoughts:

- Some reflections by individual experts:
    - Although a third-party evaluation of an algorithm's bias could be useful, avoid requiring it, as the expense is not feasible for many FSPs.
    - The probability that a third-party algorithm developer is going to show you its entire code is low. Do not require that third parties share this.
    - It is insufficient for the FSP to test only whether the right loan amount is going to the right customer. That analysis is important to credit risk, but FSPs also need to consider and remove bias.
    - "Our entry point is the know what I don't context – do you understand what AI is and how it works?" -an expert SPTF interviewed
- FSPs that are actively managing algorithm bias whom we might approach for case studies: Maha (Myanmar), Jumo (Zambia), and Tala (Kenya)
- The WWB paper recommends, "Build a fairness implementation team. This multidisciplinary team should bring a group of legal, business, and machine learning experts together. Legal advisors define what the legal constraints are or could be, identifying what the minimum threshold of compliance might be — and how to design for future regulation. Business experts think about what definitions of fairness fit well with their strategy."
- Implementation resource idea: "Women's World Banking recently created a Python-based toolkit to show how financial services providers can detect and mitigate gender biases in credit score models. The first step in the toolkit is a series of questions on portfolio size, sex ratios among customers, likelihood of women versus men applicants being extended credit, and a number of other factors. By asking these questions, the tool can model a particular institution's credit portfolio. Next, based on user input, the tool creates a synthetic dataset for the user and provides insight on both bias detection and mitigation. Visit the tool at github.com/WomensWorldBanking."

/3/ Complaints mechanism

A guiding principle is that it is the FSP's responsibility to help its customers get resolution for their complaints, even when the source of the problem (e.g., a network outage) is something over which the FSP has no control. Customers cannot be expected to know which partnerships an FSP has established, much less who is in charge of what.

> *"The customer tendency is if there's anything wrong with that gadget, they come to us [the FSP], even if it's a technical issue with the gadget and their warranty. Our customers should not be running from pillar to post trying to get the help they want… At no stage do we have a position that says look we give you just a loan, and if it's about the gadget, you need to talk to that provider. It's our customer through and through."* – an expert that SPTF interviewed

1. Offer multiple channels through which customers may register a complaint, including at least one that allows the customer to reach a live person at no cost.

2. The FSP must assist customers who have a complaint even when it relates to an issue that only the partner organization can fix.
3. Train customer service employees on how your partner's complaints mechanism works.
4. Train customer service employees on how to respond to customers who voice complaints related to services offered by a partner. The response cannot be passive, such as "call X phone number to reach Partner Org's complaints service," but must be active in helping the customer achieve resolution. Tip:
    - Write a script for call center or customer service staff employees for the top 3-5 most common issues, with advice on how best to handle it.
5. Train agents on how to respond to complaints. [NB: Some customers prefer to complain to agents.]
6. Encourage your customers to come to you with complaints about partners.
7. Have a strategy particularly targeted to helping women overcome obstacles to complain.
8. Train/encourage agents to use your complaints mechanism too.
9. At the outset of a partnership, establish who will be your point of contact within the partner organization, to help you resolve complaints by your own customers, but that are related to services provided by the partner.
10. Equip the complaints mechanism to register complaints by agents.
11. Analyze complaints data to see if certain segments of customers (e.g., rural, women) are underrepresented among the customers who complain.
12. Proactively survey a sample of customers to ask if they have complaints about services or products offered by your partner, as not everyone who has a complaint files one.
    - Qualitative consumer research in Bangladesh, Colombia and Uganda, revealed on average, only 11% of customers who experienced difficulties with mobile money reported them via formal complaints channels. (McKee et al. 2015); ii) In Tanzania and Kenya, only 5% and 10% respectively, of digital borrowers ever contacted customer care with a question, concern, or complaint about a digital loan (Kaffenberger et al. 2018).
    - In India, in 2019-20, 72% of all complaints…were from metropolitan and urban areas, while rural and peri-urban areas accounted for 10% and 18%, respectively.
    - Social norms limit some women's ability to complain about DFS issues.
    - IPA found underrepresentation of female customers in complaints data.
13. Monitor social media to see if customers are complaining about your services there.
14. Do weekly trend analysis for complaints.

<u>Other thoughts</u>:

- Much of what already exists in the Universal Standards around customer complaints resolution would apply to DFS as well as it applies to analog services. Examples:
    - Conduct campaigns to encourage customer use of complaints mechanisms
    - Categorize complaints by type of complaint and for which products
    - 90% of complaints must be resolved within one month
    - Report the most severe complaints immediately to senior management
    - Segment complaints data analysis by customer segment. At minimum, by gender, age, location, poverty/income level
    - Analyze what channels customers use to submit complaints

- Monitor average time per call at a call center

/4/
Cybersecurity

1. Implement a robust cybersecurity system, meaning it has at minimum these features: constant, ongoing automated checks and flagging anything suspicious, daily (at minimum) backing up of data, and security supervision, which is a 24/7 data security system that detects when someone is trying to hack into your files.
2. Create a multi- year budget for projected cybersecurity costs.
    - Tip: One expert recommended making a five-year budget.
3. Take the following actions to achieve acceptable data security:
    - First, increase awareness of management and the board.
    - Second, get an external audit of your data security
    - Third, train the technical team on risk management.
    - Strengthen all gap areas
    - Any time you release a new digital product/service, assess data security for that specifically and implement new security measures as needed
4. Adapt security measures to what is core to business function versus what is less important. The most fundamental functions have the strongest security. Put another way, "Use a risk-based approach to tailor your cybersecurity." -a DFS expert
5. If you work with partners, make sure you understand and are comfortable with their data security measures.
    - Tip: The IT team adds a paragraph to the contract with the vendor of its core banking system to require them to share a cybersecurity yearly assessment, to make sure the product has a secure development framework.
6. Develop threat scenarios for the kinds of incidents that relate to your organization's highest priority cyber risks.
7. Have a contingency plan for cyberattacks.
8. Build capacity to respond to those scenarios.
9. Have an expert on data security in charge of cybersecurity. The person could be internal or external. Have a plan to cover the work when that person is out of the office.
10. Train the IT team on incidence response.
11. Train customers on cybersecurity, on an ongoing basis (e.g., reminders via SMS every X time period)
    - Example of behavior a customer should not do: If the network is down, do not leave the customer's cash, PIN or phone with an agent for them to complete the transaction when the network is restored.
    - Studies also show that women are less likely to change the default PIN and more likely to use the same PIN as others in the community. Also, sometimes they hand over their phones to agents.
12. Educate your entire staff about cybersecurity, including the basics of how to talk to customers about cybersecurity and direct them to the right person if customers raise an issue.
13. Define / clarify board and management responsibilities related to data security.

14. Train board members on cybersecurity. They must understand it and agree it is necessary, so that they approve spending the money it takes to have a functional system.
15. Have a board committee that oversees risk management related to digital innovation and activities.
16. Report data on security activities (e.g., hack attempts, measures taken, new gaps or risks identified) to the board at minimum quarterly.
17. Report data on security activities to management at minimum [X frequency] (weekly?)
18. Notify customers within X time (24 hours?) if you do get hacked
19. If customers lose money because your systems got hacked, you have to refund the customer.
20. At least once every [X frequency] (month? quarter?), try to hack your own data.
    - NB: Some interviewees say you could do this with an internal team or hire an external party. Other experts however said that in-house staff are unqualified to monitor data security, and the FSP should have specialists in charge of this.
21. Share data on security hacks with other FSPs in the same market, to help each other avoid being victims of security breaches. Due to the sensitivity of the topic, you would not have to say, "I have been hacked and here is what I lost," but you could say, "Someone tried to hack us and here is the specific methodology they used."
22. Participate in information sharing about cybersecurity threats between public and private entities like with the police.
23. Have an "Internet Management Policy" and update it every six months
24. If you don't have the resources to invest in data security, then don't offer DFS.

Other thoughts:

- Cybersecurity is a necessity but very expensive for each individual FSP. A solution could be to set up regional cybersecurity centers. FSPs would share resources.
- Conduct a self assessment using the Africa Cybersecurity Resource Centre (ACRC) self-assessment tool: https://start.cyber4africa.org/. This survey will ask a few questions and provide recommendations. Keep in mind that it is a self-assessment tool which only touches the surface of information security. It provides a very basic maturity level estimate and some basic recommendations.
- Read ACRC's Incident Report Guide (Ask ACRC for permission to see it)
- Consult *Carnegie Endowment for International Peace Cyber Resilience Capacity Building Toolkit*. Has specifics of roles related to board and management, including Chief Information Security Officer, and processes for protection of the FSP, protection of the consumer, workforce development, incidence response.

/5/
Data rights / privacy:

1. Inform customers of their rights to see their own personal data.
2. Ask for the minimum amount of data you need from customers.
3. Explain to customers what data you are collecting about them.
4. Inform customers of how you use their data. Explain the benefits to them of agreeing to share these data. They need to feel certain that their data are not used against them.

5. Before you scrape data off customers' electronic devises, inform them of what you will do and how will use the information. Make it an opt-in option for customers to share their data this way; otherwise, the FSP may not scrape it.
6. If you provide an opt out option for data sharing, explain what the consequences are of opting out.
7. If you sell the customers' data, inform them about who is buying it and way.
8. Customers have to give consent before any of their data can be shared with third parties.
9. Have a system, and inform customers, of how customers can correct inaccurate information.
10. Once a year send the customers information saying this is the information we have on you. Please check whether the data are correct.
11. Explain to customers why their loan applications were denied.
    - Interesting ideas on what type of information to provide that would be sufficient, from research in Rwanda presented at CFI 2021: "Sixteen participants out of the 30 had the experience of being rejected for a digital loan, and 10 of those recalled receiving an explanation for the denial. A few rejected applicants described a somewhat basic explanation such as, "Your credit limit is zero," without further details, while others recounted more detailed instructions to "clear the balance on a previous unpaid loan," before reapplying. "I only saw a message saying that I need to use Mokash for at least three months before applying for a loan," said a 29-year-old female respondent. Six of the 10 participants who received an explanation were not satisfied with the provider's communication. Despite mixed reviews of the provider's explanation, eight out of the 10 respondents who recalled receiving explanations changed their behavior in response. Some began repaying their existing digital loans in a timelier fashion, while others increased savings and transactions within their mobile wallets."

Other thoughts:

- Interviewees had split opinions about consent. Some said customers should tick a box to give permission for every type of data the FSP wants to gain access to, while others said nobody is ever going to read that and it's up to the provider to be responsible.
- One expert suggested the FSP should have customers practice their rights around data and data privacy, but we did not have time to discuss specifically how to do this.
- Rwanda "is on the cusp of finalizing a Data Protection and Privacy Law. Emulating many aspects of the General Data Protection Regulation (GDPR), the law would give consumers new data rights such as the right to object, the right to information that a provider has about a subject, the right to correct or delete personal data, the right to explainability, and the right to data portability." – from CFI 2021
- Possible case study: Tala informs customers of what data it collects on them and how it uses it. For example, it offers explanations with icons to help customers understand why it is asking for their contacts list.

/6/

Fair and respectful treatment of customers:

1. Inform your customers of the top risks they incur if they use the products or services offered via a partner.
2. Incorporate human touch at minimum at the following points in a customer's journey:
    a. Onboarding/receiving information about the product
    b. Resolving a problem or complaint
    c. Answering customer questions
3. Record calls made to the call center to monitor whether employees are handling complaints well, even about third-party providers, and that in general employees are helpful to customers.
4. As part of the agent selection criteria, consider whether the personality of the person will appeal to your target customers, and whether they speak your target customers' local language.
5. When you educate customers about a product, teach not only how the product works but also what behaviors are good/bad from the service providers, which can be agents or other partners.

Other thoughts:

- CGAP has a market monitoring toolkit for the regulator, and one tool it recommends is mystery shopping of providers in part to identify when discrimination is happening. It says in Zambia, a provider was discriminating against pregnant women and mystery shopping confirmed this.
- Could or should FSPs inform customers of the power of leaving reviews on digital platforms? Social media does elevate consumer voice and give them power to demand fair and respectful treatment and functional services.
    - One interviewee noted, "Google reviews are a huge measure of accountability that did not exist before DFS."

/7/

Fraud

1. Determine which types of fraud are likely to occur at different stages of product use. Segment this by driver of fraud:
    - Consumer-driven fraud
    - Agent-driven fraud
    - Business-partner fraud
    - System-administration fraud
    - Fraud related to mobile-financial services
2. Each time the FSP introduces a new product, it analyzes where fraud it most likely to occur.
3. Put corresponding risk mitigation measures in place that at minimum include a system of checks and balances, scheduled audits, mystery shopping, and independent audits.
4. Study which types of fraud are the most common at different points in a product lifecycle. [NB: Different types of fraud are more likely at different stages of the product.]

- Example: fake registrations in new deployments / launch of a product, then fraud related to agents earning transaction fees per transaction once customers have been acquired. After several years, customers typically want to do more, like pay utility bills, pay merchants, receive salaries, and the FSP has to take on new systems/partners to make that happen, which opens up new avenues for fraud.

5. Invest in fraud mitigation hardware/software/capacity building
    - From MSC: "Investment costs necessarily include capital investment, infrastructure, platform development, human resources and capacity building to respond to fraud"
6. Share publicly about the fraudulent activity that your FSP has experienced, to help others in the sector avoid it
7. Use data analytics to search for and identify fraudulent activity in real time
8. If you flag possible fraudulent activity, notify customers immediately
    - NB: This idea is repeated as a suggestion for an element of an FSP's fraud response plan, in #14 below, but other experts said it should be a requirement, so SPTF is also listing it here as a standalone standard idea.
9. Have a daily dashboard that reports any exceptional activity
10. Train customers on how to protect themselves from fraud, using more than one channel (e.g., radio, SMS).
11. Train women customers especially carefully on how to protect themselves from fraud, as they tend to be more of a target.
12. Train customers specifically on the types of fees that are legitimate versus fraudulent.
13. Train employees and agents on how to spot/avoid fraud
    - From MSC: "The rewards and consequences of noncompliance must be defined and communicated to all agents in advance."
14. Define what your fraud response will be, including the specific responsibilities of various employees when the FSP is responding to fraud. Suggested elements:
    - Flag the issue – notify the internal fraud monitoring team
    - Notify customer immediately
    - Freeze account
    - Ask the customer to come to a physical branch to verify credentials and reset pin
    - Inform law enforcement
    - Inform regulator
15. Monitor your response times each time you respond to fraud
16. Use complaints data to inform anti-fraud measures. Collecting and monitoring customer feedback, and having an effective complaints mechanism, also helps the FSP to identify and manage fraud.
17. Define a strategy to avoid fraudulent fees charged by agents as this is a common source of fraud. Suggestions for the strategy:
    - Improve monitoring and enforcement of fee structures;
    - Revisee incentive and commission structures where they may lead to extra charges and fees.
    - Increase consumer awareness of official fees and encourage customers to resist paying extra charges
    - Change which agents you use
    - Note that proximity appears a strong driver of customers' choice of agents.

18. The FSP should help customers who have experience fraud [that they were not trained on how to avoid], including fraud by agents or sub-agents. Further ideas about this:
    - At minimum, this involves giving customers the information about how to contact the correct authorities to report the fraud.
    - Reschedule loans for customers who were victims of fraud.
    - On a case by case basis, the FSP can also consider helping the customer financially if s/he lost money.
    - One FSP suggested a principle of not refunding a customer if she engaged in behaviors you informed her not to do, like sharing her PIN, but thinks the FSP should help customers financially who have been a victim of fraud that was sophisticated, where it was unreasonable to expect the customer to avoid it.
    - NB: GSMA principle 3 is "People management," under which standard 3.3.2, says, "Providers shall assume responsibility for actions taken on their behalf by their agents (and any sub-agents) under the provider-agent contract."
19. Quantify how much instance of fraud, as a % of overall portfolio, you can tolerate vs when you will intervene.
    - For example: If 95% of the customers have this problem, the FSP needs to address it. If it's only 1%, maybe you tolerate that risk.
20. Have a board committee charged with fraud oversight.

Other thoughts:

- The types of fraud that we see change over time. They are sophisticated and variable. So, standards likely cannot focus on how to prevent a specific type of fraud, so much as general measures for identifying and managing fraud risk.
- Some types of fraud the currently exist are biometric identity fraud, push payment fraud, mobile app fraud, SIM card swap fraud, phishing (now done via voicemail and SMS and emails), data breaches, unlicensed digital investment, and synthetic identity fraud.
- Though interviewees generally agreed that if the fraud is something the customer was specifically trained about how to detect/avoid, and the customer didn't follow that training, then it is not the responsibility of the FSP to refund the customer, still several interviewees said that in practice the FSP will determine how much to help a customer who was defrauded, and in what way, on a case by case basis.
- In more mature markets, there is a higher likelihood of B2C or C2B fraud.
- "Fraud in the context of mobile money is the intentional and deliberate action undertaken by players in the mobile financial services ecosystem aimed at deriving gain (in cash or e-money), and/or denying other players revenue and/or damaging the reputation of the other stakeholders." -definition from MSC

/8/
Outcomes data

1. Collect data on which customers are using digital products and which are not, by customer segment
2. Verify accuracy of customer data via automated, digital checks.
3. Have annual discussion at the management level to review data and identify potential concerns related to digital products (e.g., low liquidity among agents).

4. Continue to track each customer's journey.
    - Tip: Use technology (e.g., call centers, SMS, IVR)
    - Tip: You can combine into one survey questions related to outcomes and questions related to digital literacy and digital demand of customers.
5. Track data on mobile phone usage, by gender. There is still a much lower use by women.
6. When building the strategic plan for DFS, identify simultaneously what is the business case for the FSP and what is the value that the customer will gain.
7. Identify which outcomes you need qualitative data to monitor and which you don't.
    - Example: If your goal is to promote savings, you can see quantitatively whether customers are using as savings product. But you would do quantitative calls to understand why certain customers are dormant.
8. Use outcomes data to inform product design.

Other thoughts:

- Regarding qualitative feedback, so far, most interviewees agreed it was important, but were split on whether FSPs would/could do it.
- Some outcome indicators to consider:
    - Have you experience a positive change in quality of life attributable to [provider]?
    - Decrease in the amount spent on bank fees?
    - Expanded access to financial services?
    - Improved ability to digitally transact?
    - Improved ability to receive money?
    - Increase in savings since you began saving with [provider]?
- Be innovative in using digital tools to collect qualitative data.
    - "Previously, I would have said phone surveys are not helpful. But during COVID, we've had deep qualitative interviews over the phone. I'm trying to adapt my mindset. There are digital tools that can be used." – a DFS expert

/9/ Partnerships

1. In advance of discussions with potential partners, prepare a case for why it's a win-win for the partner to adapt their offer to your customers, if your customers are different from their typical ones.
2. Ask potential partners if they already had plans to serve the specific segment of customers that you (the FSP) currently serve, and if so, what those plans are.
3. In advance of entering into discussions with potential partners, do research to identify the problems that customers typically have with that partner. Write a list of the top 3-5 common problems that customers tend to have.
    - Example: IPA research in Nigeria found these issues with DFS providers:
        - extra or unexpected/unclear charges
        - phishing or scam attempts
        - agent overcharging
        - missing money

- Example: A common mobile network operator (MNO) problem is network downtime.

4. During contract negotiations, bring up the common problems you previously identified and ask what steps this potential partner is taking to reduce the risk of these problems. As needed, strengthen the plan to manage the top 3-5 common problems or risks, so that if they occur, a plan is already in place and can be quickly activated.
    - If you partner with an MNO, it is mandatory that the agreement specify what the steps are that the MNO must take if its service goes down.
    - Can the FSP specify the acceptable length of time to resolve the problem?
5. During contract discussions, ask how the partner resolves complaints. Use specific examples taken from common complaints.
    - Examples: a) funds transferred in error to the wrong account; b) ATM processes a transaction, debits the account, and issues a receipt but does not dispenses cash; c) account debited but no funds transferred due to network failure
6. During contract discussions, ask how the potential partner trains its staff on customer care.
7. During contract discussions, ask how the potential partner assures the security of its own data systems.
8. During contract discussions, ask what systems the potential partner has in place to prevent its customers from being victims of fraud.
9. Have a plan to manage data privacy concerns before beginning the partnership. Ensure transparency and agreement before the work gets underway.
10. Have a service-level agreement (SLA) with each partner that includes the following:
    - For MNOs specifically, they must share certain key data:
        - Transactions data (e.g., who transacts, when, how much)
        - Complaints data (who complained, about what, when was it resolved)
        - Network downtime
    - For all partners:
        - Define who handles customer complaints Be clear about who specifically in the staff responds.
        - Define <u>how</u> complaints will be handled, taking into account considerations like if the partner organization does not speak your language and/or is located in a different country. What is a realistic time frame and process for the partner to deal with different problems?
        - Clarify pricing
        - Exit clauses – under what conditions do you cancel the agreement. Include terms about bad customer service that would lead to contract termination.
        - Data reporting – how does the partner report its data? How does the FSP have access?
        - In general, identify the potential areas for there to be problems. Don't focus just on the benefits that will accrue to each party.
    - If you partner with fintech providing credit scoring based on an algorithm, agree with them on what parameters they will put into their algorithm.
    - If you partner with an organization that is providing an online system/application for you or your customers, specify who is responsible for what if the system gets hacked.

- Structure the agreement so the FSP has the ability either to resolve the complaint or to terminate the contract with the third party provider if only they can resolve the problem and they don't do it.

11. Create a contractual relationship that allows you to iterate.
12. Define the indicators of success for the partnership. Agree on them with the partner and put them into the contract.
13. Establish a direct line of communication and point of contact for your organization within the partner organization.
14. Verify that the potential partner has enough human resources capacity to do the work that you are asking them to do, securely, in the timeframe you have in mind.
    - NB: Some newer/smaller fintechs can be technically savvy and innovative but not have a large enough team to ensure cybersecurity of their own systems and/or to implement your project in a timely fashion.
15. If you partner with an MNO, select one that achieved GSMA certification.
16. Do not sign a long-term agreement with a partner. Make it a 1-2 year agreement, and use whatever issues came up and needed to be resolved to inform adjustments in the SLA for the next agreement.
17. Field test new products/services with your partner. Use this to test not only the product but also the partnership. Do not commit to a long term partnership until you experience working with the partner in a field test.
    - Idea from an expert: If you hire a vendor, can you create a relationship where you test whether this is working and can pivot to other models? Can you test numerous protoypes before you pay for a second tranche?
18. Understand what terms and conditions your potential partners would impose on your customers.
19. If the FSP's customers lose money because of a failure in a partner's system, the FSP must restore the funds to the customers' accounts and then take on the job of having the partner organization refund the FSP.
20. Annually, review and refresh the projections of how many customers will be using the product/service that is offered via the partnership, and the projection of revenue from it.
    - NB: This information is critical for contract renegotiation, which should happen every year or two instead of the FSP being locked into long-term contracts, as noted above.

<u>Other thoughts</u>:

- Avoid saying the FSP should monitor its partners' behavior. An FSP typically lacks the capacity or access that would be required to do this.
- Avoid saying the FSP should enforce that its partners train their staff in a certain way. An FSP would not have this leverage.
- Several interviewees advised to pay partners in tranches instead of all up front.
- Resources to reference: UNCDF toolkit on service level agreements

/10/

Prevention of Over-indebtedness:

1. Offer a cooling off period, during which the customer can choose to return a loan without penalties. The exception would be for micro/nano loans.
    - NB: Some interviewees agreed with this idea and others did not.
2. Use electronic data (e.g., transactions with suppliers, retail transactions, mobile transactions if the MNOs will share it) to estimate a customer's monthly expenditures/income, and therefore appropriate loan size.
3. Educate customers about risks of taking out loans from unscrupulous actors.
4. The FSP should interact with credit customers regularly to remind them of their obligations.
    - "Best portfolio performance is in places where the credit officer has the best training and they're interacting with customers to remind them of their obligations." – a DFS expert
5. Pro-actively seek feedback periodically from customers who are getting automated loan increases, to check on positive or negative effects from taking out loans.
    - "Be very careful with any strongly automated underwriting. At the end of the day, I don't think a fully digital banking system for customers who have a certain level of financial literacy is a responsible thing to do. Personal touch has to remain in place. It means you understand what's happening in the other person's life. Even if you're standardizing and segmenting, you have to understand what's happening. There's a chance of putting them in a worse situation by giving them automated loan increases." – a DFS expert

Other thoughts:

- "Evidence shows that digital platforms such as mobile applications and peer-to-peer (P2P) lending platforms have exposed consumers to several risks that lead to over-indebtedness. Unauthorized digital lending apps and P2P platforms, which mimic genuine ones obtain customer data intrusively and offer hassle-free but expensive digital loans to desperate customers." – a DFS expert
- "There is a fundamental risk of oversupply of capital." – a DFS expert
- Implementation resource idea: Walla – created a FB community (about 500,000) in SSA to reinvent a village bank but on a digital platform. People talk to each other and give insight about how to manage their money.
- "Just with digital, there are studies – people spend more wildly when there aren't physical cash. That matters and you have to factor that in." – a DFS expert
- We hear experts arguing both sides in the debate about whether very short term loans are good for customers.

/11/

Product design and delivery

1. Start product development with the discussion of what is not working well for customers and how to solve it.
    a. Should be bottom-up, not top-down. Example: Select partners that have found ways to use technology to address the pain points your customers experience.

   b. Don't start with technology and then develop a product around it.
2. Use the data you have to identify problems (e.g., no liquidity among agents)
3. Build the digital literacy of your customers enough for them to use the digital products and services you offer safely and effectively. Some tips:
   a. Figure out who customers trust and deliver training for customers through them
   b. View training as ongoing, not one-time
   c. Embed the tools that are used to build digital financial capability into the product delivery process. Providers should see this as part of their service provision.
   d. Use a lot of step-by-step guides and a lot of visuals.
   e. Leverage peer learning.
      i. "The beauty is once one customer learns, then they teach the others. Usually after they learn, it's a straightforward process." – a DFS expert
      ii. "The FSP needs to identify who the customers trust. We tried having partner orgs who knew the tech best offer awareness raising and digital literacy training. Then we switched to a model where there were early adopters, they trained them, and then the early adopters trained customers." – a DFS expert
4. Design digital products around technology that target customers already know how to use OR build capacity of target customers to use a technology before implementing it.
5. Research levels of digital literacy, by customer segment, during market and pilot research
6. Design digital pilot testing to be done quickly (about 3 months), with a focus on pilot testing solution ideas but not a fully developed project.
   a. This requires a break from traditional thinking, which involves spending a lot of time building and testing a single solution.
   b. Drop things quickly that do not work.
   c. Consider conceptually testing a piece of the solution, then if it preliminary signs are that it could work, develop it more and pilot further.
      i. "Piloting needs to change – the FSP needs to be like a startup – trying a bunch of things and constantly upgrading internal technology." – a DFS expert
7. Integrate strengthening digital literacy as a part of product design and delivery, in multiple stages:
   a. At the point of onboarding, when a customer first uses financial services.
   b. Refresher digital literacy training
   c. [optional] In between, there could be business development services where users build capacities on different aspects of digital literacy.
      i. Note: Technology allows for innovative and effective ways to deliver trainings to customers, including over videos or via IVR
8. When training customers on new products, make it clear not only how to use the product but also how this product brings value to the customer.
9. Provide confirmation to a customer immediately after she makes a transaction. If customers are paying from a mobile wallet, they get two confirmations (from the MNO and the FSP) that the transaction happened.
10. Offer technology in an opt-in way, not mandated.
11. Design digital interfaces as simply as possible, so that even those unfamiliar with numbers can use them.

12. Design your products for the hardest to reach customer, who is likely a poor woman. If the product design works for the hardest to reach person, it will work for anyone.
13. Design products to address the four main barriers:
    a. Affordability (This is not just price, but infrastructure – does she have a phone? Can she buy minutes?)
    b. Availability (Note: women tend to need to be in their homes most of the day)
    c. Ability (Consider social norms too, meaning, understand not only whether she is able to use a phone, but also whether she thinks technology is for her.)
    d. Appetite (Does the product meet her needs? Does she trust it?)
14. Design products iteratively with customers. Select a small group of customers for this.
15. Use data to inform product design, from all stages of the customer journey, meaning even before they become customers. Examples:
    a. Analyze data from potential customers that started applying for a product and then quit, to see where in the process people exit. (Example: on an app, if your onboarding is two pages long and they start but don't finish, you can check at which question on page 1 or page 2 they stopped filling in the form.)
    b. Track dormancy and reach out to dormant customers to understand why they have stopped using your products.
16. Make KYC questions and requirements as simple and easy for customers as possible. Think through the purpose of every question you ask to be sure it is necessary.
17. Engage employees and/or agents in product design:
    a. Raise awareness – what are the benefits of this product?
    b. Train employees on all products
    c. Pilot test new products with employees first
        i. "If my staff have to go out and convince the customers, it becomes easier if they are going out and talking about something they know and that they have tested." – a DFS expert
    d. Define incentives. Are employees incentivized to sell in the right way?
18. Assign a unique identifier to each customer.
    a. Note: A phone number is not always a unique identifier, as people share phones.
19. Adapt design and marketing strategies for products to customer segments (e.g., rural women, rural young adults)

<u>Other thoughts</u>:

- How is digital part of the overall strategy? The customers' needs, demands, and capabilities from the financial literacy and technology point of view should factor into the product and channel design.
- It would be easier for customers if all FSPs harmonized the look of the key functions of their apps (e.g., what the icon is for checking an account balance) so customers do not have to learn each individual set of functions depending on which provider's app they are using.
    - "Think of ATMs. The screens look the same no matter what country you're in. Could we have a standard way of doing things that make it simpler for customers, for example for loan repayments." – a DFS expert
- One expert said that all the mobile money has the same features, so it doesn't matter from a functionality standpoint which provider the customer chooses. The question is,

are you communicating well with her? Does she understand how to use the product and how it relates to her needs?

/12/
Responsible Pricing:

1. Do not pass on the early costs to customers. The FSP has to invest in capital expenditure as if it is starting a new business and amortize the investment accordingly. Poor customers cannot and should not subsidize this investment. Some tips:
    - Launch new partnership with venture capital or other entities to share the upfront costs so you don't pass it onto customers.
    - The board enables experimentation and manages risks with product design. For example, it sets aside a percentage of money as risk capital and does not hold that to the same risk standards. Its attitude would be, "Let's invest in learning more and building our confidence in these newer models."
    - Take advantage of open source software for requisite updates to their IT systems. One example is Mifos for core banking.
2. Board and management create a pricing strategy and review it regularly [X frequency].
3. Communicate the annual percentage rate (APR) and all fees.
4. Disclose penalties up front, at the time the customer is taking out a loan. It is not ok to wait until the customer will be charged, and then disclose it.
5. Eliminate punitive fees. Have a single price for a product, and do not charge anything else.
6. When a customer defaults, do not charge compounding interest or late fees. The penalty for default is losing the ability to access loans on the platform.
7. Do not have a minimum balance requirement for a savings account.
8. Do not charge fees for overdraft.
    - Use technology to identify when an account balance is not sufficient for a transaction and then deny the transaction rather than allowing overdraft. OR
    - Have in place a system to allow for overdraft up to a small modest amount, and to notify the customer in real time when s/he has an overdraft.
9. Clearly state the consequences of not paying.
    a. Examples: seize collateral, refuse a new loan, report to credit bureau
10. Reduce prices for customers who have a demonstrated record of on-time payment.
11. The algorithm should get more effective over time, leading to better ability by the FSP to price appropriately given actual customer risk and repayment probability
    a. "The best practice should be that pricing is not uniform across the board. It's calibrated to that person's risk level." -a DFS expert
12. For loans, the interest rate and repayment schedule should never be such that the customer ends up paying more in interest than s/he received in loan capital.
13. Cross-subsidize, using funds earned from higher-end customers to serve lower-end customers at affordable prices.
14. Do not use revenue earned from good customers to subsidize the costs of customers who default.

Other thoughts:

- Even if the financial product is affordable, it is possible that other costs might be exorbitantly expensive, like the price of mobile internet.
- "DFS is exorbitantly costly…I have not seen prices go down. If customers are willing to pay because of the quick access, we should let the market forces work on it." -a DFS expert
- There is a balance between affordability and convenience to the customer. Often something more convenient is also more expensive.
- Generally, interviewees are not in favor of price caps.
- Much of what is in the original Universal Standards document likely still applies. For example, it says to define "responsible" pricing according to what costs you incur and what level of profit you seek (e.g., avoid passing on the cost of inefficiencies, avoid charging too much just so you can pay investors high dividends); do not rely solely on benchmarking.

/13/
Transparency

1. Write agreements that customers have to review/sign in the local language.
    - Idea: Have someone from customer services write the contract, not a lawyer.
2. Decide what key facts need to be disclosed. Minimum to disclose up front for a loan: Loan amount, loan term, repayment frequency, total cost of credit, APR, penalty fees.
3. In addition to the agreement, develop clear messaging, in local languages, to use to disclose key facts again in a quick and accessible manner. Some tips:
    - Do this via multiple channels, such as SMS, IVR, a call center, and a poster
    - Have diverse touch points with customers and give them information at each of those times. Move away from the mentality of giving customers all the information at the time of contract signing, and then the FSP never has to give information again.
4. Have a different system for how many messages with key information you send to first time users, vs to those who have used the same product multiple times. All should get the information, but first-time users should get more messages about it, and more repeat information.
5. For all messages, follow this guidance: make it small (bite sized) and engaging.
6. Every time a customer buys a credit product, communicate at least once, clearly, about the importance of repaying on time and the consequences of default.
7. Collect information about the digital channels to which your customers have access, so you know through which channels you can share information.
8. Give customers an option to speak to a live person.
9. Use an IVR chatbot to respond to customer questions. It must use local languages. The call must be free.
10. Do a spot check on a sample of customers to test whether customers understand key elements of the terms and conditions. If not, improve disclosure processes. Some tips:
    - Can be done via call center or SMS survey or by the internal audit team
    - Weight the sample heavily toward those who recently started using a product
11. Design digital interfaces to be simple and visual, promoting use even by those who are not digitally literate

12. Provide customers with a receipt of digital payment from both the partner and the FSP.
    - Example: If a customer uses a mobile wallet to pay a loan installment, the MNO will send an SMS that says you paid X and here's the balance in your mobile wallet, but the FSP also needs to send a second SMS to say we've received a payment and your loan balance is now X.
13. Every time the customer conducts a digital transaction, the customer should receive a digital receipt/confirmation message and the credit officer (or equivalent) should receive the same transaction confirmation message on his/her device.
14. [NB: This is a repeat standard from fair and respectful treatment of clients] In general, FSPs should offer customers the possibility of talking to a human at minimum in three contexts: explaining new product, answering questions, helping with complaints
15. Ask customers how they get information. Then deliver information through those channels. Segment the answers by customer type.
    - Example: One FSP noted that its urban customers are more likely to say they get information from tv or radio, whereas rural customers are more likely to get information by word of mouth.

Other thoughts:

- Many of the ideas in the original Universal Standards manual also apply in a digital context. Examples: use simple language; use local languages; make opt in/out options clear.
- There is a tension in DFS coming from the fact that customers should understand all the terms and conditions, but all they want to do is scroll and accept, and many DFS providers make it very easy to scroll and accept.
- Some feature phones have a maximum amount of SMS messages they can store, and if customers do not delete old messages, the inbox fills and customers can't receive new SMS messages. This would inhibit transparency via sending SMS.
- IPA research showed, "Extra or unclear fees and charges were experienced by consumers across the different DFS products and channels. This signals there may be common challenges of extra or hidden fees, and/or consumers not understanding fully the terms of the products they use in DFS."
- Consider having two sets of transparency ideas: one for customers on feature phones and ones with Smart phones.
- Do not rely on check boxes. People will go through and check every box.

ADDITIONAL DISCUSSION TOPICS

Financial inclusion of those who struggle to use technology:

SPTF is concerned that technology can lead to a digital divide, where those who have access to an electronic device and are both literate and numerate stand to benefit enormously from DFS, but those who do not have unrestricted access to a device, and/or who are illiterate and/or innumerate, may be excluded. How do we avoid this? Some thoughts from interviewees:

- This problem isn't as big as we might fear. People adapt, and people live in communities where those who can't use DFS themselves can get help from family members or neighbors. One FSP in Africa said 65% of women in rural areas in the country are

illiterate and don't know how to use a mobile phone, but they can all make it work by relying on family members to help with mobile transactions.

- The FSP can and should offer financial education, including technology training, to customers so they learn how to use Smart devices
- Design interfaces to be easily understood by customers: use local language, limit the amount of text per screen, use icons of images that are familiar to the target population
- One FSP said: "In this part of the world, as much as we'd want 100% of our customers to access through the new phone, the actual availability…can be an issue. It can be that the customer doesn't have the right type of phone to have the application running. It can be that your customers are keen to move on to the new product but they don't have the right type of resources or the right gadget."

Responsible treatment of employees and DFS

Experts shared a wide array of thoughts about employees, some related to managing digital transformation, and some related to human resources in a digital context on an ongoing basis.

- Quotes from various interviewees regarding challenges during digitization:
    - "The idea of risk models in most MFIs very stuck in the older model than in how things ought to be. It's important to help the risk and compliance officers come along in the digital journey."
    - "The main thing that comes to my mind that the FSPs themselves are pretty immature and ignorant with regards to anything digital. This applies not only to the smaller MFIs but also quite larger groups…In terms of solutions based on that, it's a lot about education. For the providers, their level is quite appalling in terms of their understanding of IT security."
    - "We didn't have the technical expertise to translate things from the raw ideas of what we want to do to what actually needs to happen."
- This person mentioned workplace diversity as a component of DFS success: "If you want to design products for different types of people, you want a diverse workforce. A more balanced workforce is really important."
- This person tied higher over-indebtedness due to easy access to digital credit to higher employees stress: "Burnout - really hard for customer services agents to deal with what they have to hear. Money is emotional."

Interoperability

A starting premise is that interoperability is a digital right. Some experts suggest that individual FSP can play a role in moving the sector toward interoperability.

- "What can an FSP do? If it's a small cooperative, you have to be real and say they have no power to make interoperability happen. But if it's an MNO or a bank, I'd argue that they have tremendous power to push forward interoperability." – a DFS expert
- FSPs can initiate and/or participate in industry-level interoperability initiatives around sharing customer data for credit checks.
- Advocate for all FSPs of any legal structure to be connected to any new digital infrastructure that a country is putting into place.
- Advocate for interoperable structures to be governed by the participants (the FSPs).

  - "What are the rules of it? How is settlement going to happen? What are going to be the fees? The participants and the regulators should have a role in that." -a DFS expert
- Case study: Myanmar, where MFIs had been excluded from the design of the credit bureau, the MFIs formed their own initiative to share data in a way that is interoperable so all members can do credit checks.

The role for country- or region-wide actors

Several interviewees reflected on work that would be best done at a country or regional level.

- "Maybe there's a missing middle. How do you get all the banks together in a room to talk about harmonization? What is the first step? Do you need to have data to say there are real inefficiencies when we ask customers to learn totally different systems to use different digital services?"
- "Do we all agree that we should make it easier for people to transact? Can you come up with five practices that we're all doing the same anyway? The process of facilitating conversation among people who are doing this is under discussed as a skill in and of itself."
- "At a market level across providers you can absolutely do benchmarking [of complaints data] across providers."
- Some operators are expected to follow the customer protection practices and some are not. An important message to communicate to regulators is the need for a level playing field.
- Envision a broad financial literacy campaign supported by a donor.

The importance of governance

- Regulation is a flawed lever to change behavior in this sector because technology evolves faster than regulation. Regulation follows innovation. An interviewee noted, "The first cars didn't have seatbelts."
- The most immediate sources of influence are investors and the board of directors.
- An interviewee recommends, "Need to put people in management and boards who have the best interests of the customers and are ideally *like* them in some way."
- For responsible DFS standards to be implemented, we have to build commitment to self-regulation.

Customer trust

- Many experts mentioned that if providers of DFS do not build and maintain the trust of their customers, particularly those who have been financially excluded and are using both formal finance and digital services for the first time, then DFS will fail. Some quotes:
  - "There is an urgent need for proactive measures that maintain customers' trust in DFS and ensure positive outcomes."
  - "High confidence will lead to high usage."
- People who try DFS and have a bad experience will be more reluctant to try it again.

Prioritization within standards development work

- Research and experience have revealed many consumer protection risks linked to the provision of digital financial services. Given how varied and complex the problem is,

should we focus our attention first on a smaller set of risks, and choose to begin with those that are the most dangerous? If so, which would they be?

- One interviewee said the three areas of biggest risk are responsible pricing, transparency, and prevention of over-indebtedness.
- Several interviewees stated that cybersecurity and fraud are monumental risks.