STANDARDS FOR RESPONSIBLE DIGITAL FINANCIAL SERVICES

3 November 2022

Cerise + SPTF
Standards for Responsible Digital Financial Services
(Draft as of 3 November 2022)

Target Audience
Financial service providers (FSPs) of all legal types seeking to offer digital financial services (DFS) responsibly.

Goals
At minimum, FSPs will implement the management practices related to consumer protection described in this document. As a result, customers will not experience harm from using digital financial services. Additionally, FSPs that are committed to helping customers use DFS to improve their well-being will implement that management practices in this document related to the "doing good" elements of social performance management.

How to Begin
Evaluate your FSP's current performance against the Universal Standards for Social and Environmental Performance Management ("Universal Standards") *and* against the standards for responsible digital financial services ("DFS Standards"). The Universal Standards describe in general the management practices for an FSP to implement to protect customers and achieve social and environmental goals. The DFS Standards describe additional management practices that help mitigate risk and promote better outcomes for customers who use digital channels. One expert suggested, "Split the DFS Standards between minimum requirements and aspirational standards to give a sense of sequenced implementation for those who need to prioritize. This may apply across the categories of standards."

Organization of this document
The document covers 13 different topics, organized into three main categories:

1. Risk management and consumer protection
    - Complaints mechanism
    - Cybersecurity
    - Data rights and privacy
    - Fair and respectful treatment of customers
    - Fraud mitigation
    - Prevention of over-indebtedness
    - Transparency
2. Promoting benefits for customers
    - Managing algorithm bias
    - Outcomes
    - Product design and delivery
    - Responsible pricing
3. Collaboration with third parties
    - Agent management
    - Partnerships

Risk Management and Consumer Protection

Complaints mechanism

1. Take responsibility to resolve a customer complaint even when it relates to an issue that a partner organization, but not the FSP, has the power to correct.
2. At the outset of a partnership, establish who will be your point(s) 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.
3. At the outset of a partnership, establish a reasonable period of time in which the partner will resolve customer complaints, with different delays agreed upon per type of complaint.
4. Encourage your customers to come to you with complaints about partners' service provision.
5. Train customer service employees on how your partner's complaints mechanism works.
6. Train customer service employees on how to respond to customers who voice complaints related to services offered by a partner.
7. Train agents on how to respond to complaints.
8. Create the right incentives for agents to handle complaints and not conceal them.
9. Train/encourage agents to use your complaints mechanism.
10. Equip the complaints mechanism to register complaints by agents.
11. Analyze complaints data for the following information:
    - to see if certain segments of customers are under- or over-represented among the customers who complain
    - to see if certain issues are under- or over-represented among the types of complaints
    - how long it took to resolve complaints, segmented by type of complaint
12. Research why some customers do not file complaints even when they have reason to complain, and address obstacles that prevent customers from complaining.
13. Proactively survey a statistically significant sample of customers to ask if they have complaints.
14. Monitor social media to see if customers are complaining about your services and respond as needed.
15. Do at minimum weekly trend analysis on the types of complaints you receive and share those reports with management.
    - NB: Many commenters suggested revising detail 4.E.2.3.3 of the Universal Standards ("The provider resolves at least 90% of complaints within one month. If the resolution takes longer than one month, the provider notifies the customer of the reason for the delay"). Some complaints take a month to resolve, but most take much less time, and the easiest ones can be resolved within a day.
    - NB: Indicator 4.E.3.3 of the Universal Standards ("If the provider partners with third parties, the provider helps its customers to resolve complaints they have with those third parties.") should mention the appropriate frequency/delay for complaints resolution.

16. Set an internal standard for what percentage of complaints must be resolved within what time frame,[1] by type of complaint, monitor whether the actual resolution of complaints meets the target, and take action if there are gaps.
17. If a partner organization is unresponsive about resolving a customer complaint, notify the national regulatory body to help address the issue.

Cybersecurity

1. Define board and management responsibilities related to data security. These should include but would not necessarily be limited to the following:
    a. Creating a strategy to ensure risk management related to digital innovation and activities
    b. Identifying criteria to use to select a competent cybersecurity vendor
    c. Defining what data about cybersecurity (e.g., risks, problems, actions taken) the board needs to see, and what data management needs to see, and how often
    d. Developing a training plan for staff on cybersecurity
    e. Determining how the FSP will assess the cybersecurity of its partners and what level of cybersecurity by partners is adequate
2. Include cybersecurity / data protection costs in the budget every year.
3. Implement a cybersecurity system that has at minimum these features: physical security, daily (at minimum) data back-up, ongoing automated checks that flag any suspicious activity, and an always-operational data security system that detects attempts to hack into your files.
4. At least once every quarter, have a professional (either internal or external) try to hack your own data (aka, penetration testing).
5. When setting up a data security system, take the following actions:
    a. Increase awareness of management and the board.
    b. Get an external audit of your data security.
    c. Strengthen all gap areas.
    d. Train the technical team on risk management.
6. Identify what is core to business function versus what is less important, and implement the strongest security measures for the fundamental functions.
7. Take the following actions to achieve acceptable cyber-resilience:
    a. Develop threat scenarios for the kinds of incidents that relate to your organization's highest priority cyber risks.
    b. Have a response plan for cyberattacks.
    c. Build capacity to respond to those scenarios.
8. Any time you release a new digital product/service, assess data security for that product/service specifically, and implement new security measures as needed.
9. Monitor employees' use of computer systems and audit their activities.
10. Learn what cybersecurity measures any potential partner has in place, and work only with those with adequate cybersecurity systems.
11. If you work with a potential partner, assess cybersecurity risks that arise from the interconnection of your systems, and implement risk mitigation measures as needed.

[1] One commenter suggested that a digital product should have a more frequent complaints reporting system than a non-digital product.

12. Appoint a person or team, either internal or external, to be in charge of cybersecurity, including who is in charge when the main person is out of the office.
13. Train customers on cybersecurity, on an ongoing basis.
14. Train employees on cybersecurity, on an ongoing basis., covering at minimum their own responsibilities, how to talk to customers about cybersecurity, and how to direct customers to the right person if customers raise an issue.
15. Train board members on cybersecurity, on an ongoing basis.
16. Report data on cybersecurity to the board and to management
    a. For example: report hack attempts, measures taken, new risks identified to the board at minimum quarterly.
    b. For example, report data on security activities to management at minimum weekly.
17. Notify customers within 24 hours if you do experience a data breach that affects them. At minimum the notification must contain the following information: what information was breached and what the FSP will do as a response to this data leak.
18. If customers lose money because of a cybersecurity attack on your system, refund the customer in full for the money they lost.
19. Notify other FSPs in your market of any attempts hackers make on your data security, including sharing the specific methodology they used.
20. Participate in any initiatives in your country or region involving information sharing about cybersecurity threats.
21. If you do not have the resources to invest in cybersecurity, then do not offer digital financial services.

Data rights / privacy:

1. Inform customers of the benefits to them of agreeing to share their data and explain to customers the consequences of opting out of data sharing.
2. Make it an opt-in* option for customers to share their data.
   *define "opt-in" as the customer gives permission for the FSP to have access to her data and to use it in the ways that the FSP explained it would use it
3. Collect the minimum* amount of data you need from customers.
   *define the "minimum" data as the data you use to make a decision about whether to offer them a product or service, and at what price, as well as the data you need to segment customer data to analyze outcomes for customers as well as the customer's needs and experiences related to using financial products and services.
   NB: Should we specify that the minimum amount of data does not include data needed solely for marketing?
4. Define the minimum amount of data needed from customers, and revisit this definition, and update as needed, when the FSP introduces a new technology and/or a new products and/or a new partnership.
5. The leadership of the FSP defines a strategy for how the FSP processes and uses data, and monitors the implementation of those practices.
   - Related to the above: At minimum annually, management review the amount of data the FPS collects on customers to make sure it is aligned with the principle of collecting the minimum data needed, and make changes as needed.

6. Have a system for how to receive and process customer requests to correct inaccurate information you (the FSP) have about them and inform customers of this system.
7. If the FSP denies an application for a product, inform the customer of the specific information or data that were the reason for the denial.
8. Give customers an unsubscribe option to cease receiving digital communications from the FSP.
9. Define and implement a policy for when and how to discard data at minimum in the following circumstances:
    - when someone ceases to be a customer;
    - when someone applied and is rejected;
    - when data you have on a customer are no longer relevant to decisions the FSP makes because of changes in how the FSP operates.
10. When working with third parties, specify the following:
    - For what purposes the third party is allowed to use the data, and that in all other contexts use is prohibited of the data shared by the FSP;
    - If the partnership ends, the steps the partner will take to safeguard the data while it still keeps it, as well as when and how it will delete the data.

Fair and respectful treatment of customers:

1. Inform your customers of their rights if they use the products or services offered via a partner, as well as how to complain.
2. Incorporate direct human engagement 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. Make customers aware that they can reach a live person if they wish and inform them how to do it.
4. Record calls made to the call center to monitor customer service, noting performance when responding to complaints both about the provider's services and complaints about third-party providers.
5. As part of the agent selection criteria, consider whether the personality, culture, and language(s) spoken will appeal to your target customers.
6. When you educate customers about a product, teach not only how the product works but also what behaviors are acceptable and which are not acceptable from the service providers, which can be employees, agents, other partners.
7. The internal audit department monitors adherence to FSP policies concerning respectful treatment of customers.
8. When designing digital products or services, consider how to make the technology that customers must use inclusive for persons with disabilities.

Fraud mitigation

1. Create a strategy to mitigate digital fraud risk and address fraud if/when it does occur:[2]
    - Quantify how much instance of digital fraud, as a percent of overall portfolio, the FSP will tolerate.

[2] One person commented that this standard "may benefit from being reworded in terms that are more aligned with the usual risk management vocabulary (risk assessment, appetite, matrix, etc) as this is in fact the application of risk management processes to DFS."

- Research which types of digital fraud are likely to occur at different stages of product use, and which segments of stakeholders perpetrate the fraud, and use this information to inform the fraud risk mitigation strategy.
- Identify what investments in hardware, software, data analytics, and/or capacity building are necessary.
- Design and implement systems to mitigate digital fraud risk. These should include but may not be limited to the following:
    - Providing digital literacy training to customers
    - Collecting customer feedback, starting with market research and continuing through the pilot and full launch of digital products, to identify potential for fraud or cases of actual fraud
    - Defining the responsibilities of each department (e.g., marketing, customer service, audit) with regards to fraud risk mitigation
- Define what your fraud response will be, including the specific responsibilities of various employees. The plan at minimum should state how the FSP will notify affected customers, inform the authorities, and stop the fraudulent activity, as well as defining what actions, if any, the FSP will take to assist customers who were victims of fraud, and what actions, if any, the FSP will take against the perpetrators of the fraud.

2. Implement fraud risk mitigation measures that at minimum include a system of checks and balances, automated data analytics that identify suspicious activity, using customer complaints data for insight into potential fraudulent activity, and audits. If the FSP works with third party partners, the system should also include mystery shopping.
3. Each time the FSP introduces a new digital product, analyze where fraud is most likely to occur and implement fraud mitigation measures as needed.
4. Report daily any possible fraudulent activity detected by data analytics to senior management.
5. Train customers using at minimum two different channels on how to protect themselves from digital fraud.
6. Inform customers of how to report suspected fraud to the FSP and request help.
7. Train employees and agents on how to detect and avoid digital fraud.
8. If you identify fraudulent activity, notify customers within 24 hours.
9. If a customer is a victim of fraud despite adhering to good practices for fraud avoidance, the FSP restores to his/her account any lost funds.
10. Monitor your response times each time you respond to fraud.
11. Share publicly what fraud attempts your FSP has confronted, to help others avoid it.
12. The board of directors oversees the implementation of fraud mitigation measures and monitors instances of fraud.
13. The person in charge of monitoring fraud (e.g., the Risk Manager) reports directly to the Board and not the CEO.

Prevention of Over-indebtedness:

1. Analyze instances of aggressive sales[3] (tracked via customer complaints) and poor portfolio quality by the channel through which the FSP recruited the customer (e.g., Facebook) and/or through which the FSP delivers services.
2. Offer a cooling off period of at minimum 48 hours after a loan approval, meaning the loan is approved but the funds are not yet deposited into the customer's account. During the cooling off period, the customer can choose not to take out the loan, without penalties. The exception would be loans of a short tenure.[4]
    - NB: Some interviewees agreed with this idea and others did not.
3. Estimate a customer's monthly income level, and therefore appropriate loan size, even if providing a digital loan, and offer loan sizes that are affordable given the customer's income.[5]
4. Educate customers about what data they need to assess whether the terms and conditions of a loan meet their needs, and about their rights to transparent disclosure of loan information, and about their rights to refuse aggressive sales.
5. Remind credit customers regularly of their obligations.[6]
6. Pro-actively seek feedback periodically from customers who are getting automated loan increases, including at the moment when a customer is applying for a loan, to check on positive or negative effects from taking out loans.[7]
7. Define when, if ever, parallel loans are allowed and adhere to this policy.
8. Define and implement safeguards so that the management information system flags and reports automatically likely instances of customers gaming the system.
    - NB: detail 4.A.1.1.2 from the Universal Standards ("Loan approval decisions are made by at least two people, one of whom does not interact directly with the client") does not apply in a digital context.

Transparency

1. Design a solution for delivering a key facts document to costumers digitally.
    - NB: The standards would not prescribe how to do this, but the implementation guidance could give ideas. For example, do NOT email a link to a long online contract. DO offer to print a version for customers able to come to a branch office to pick it up.

[3] A commenter requested that the guidance define what "aggressive sales" means.
[4] Would need to define "short." Also, if a cooling off period is not appropriate to micro/nano loans, then the guidance should define "micro/nano loans."
[5] This concept already exists in the Universal Standards. But the DFS experts' point was that even if the FSP is no longer visiting customers' places of business, it still should be estimating the client's capacity to repay. In a digital context, this could be done by using electronic data (e.g., transactions with suppliers, retail transactions, mobile transactions if the MNOs will share it) to estimate the customers' monthly expenditure or income.
[6] "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
[7] "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

2. Develop clear messaging, in local languages, to use to disclose key facts *again* in a quick and accessible manner.
    - NB: This idea supplements what is already in the Universal Standards about the initial disclosure of key facts: Indicator 4.B.1.1 says "The provider gives a Key Facts Summary Document to borrowers before they sign a contract."
    - For implementation guidance, consider recommending a standardized template for a key facts document. If all FSPs used the same template, it would make it easier for customers to use and understand the document.
3. Define a strategy for how and when to share messages with key information. This strategy should include a different system for how many messages you send to first time users versus to those who have used the same product multiple times.
4. Design digital interfaces to be simple and visual enough to be used even by those who are not digitally literate.
5. Provide local language options within digital interfaces.
6. Give customers an option to speak to a live person.
7. Do a spot check on a statistically significant sample of customers to test whether customers understand key elements of the terms and conditions. If not, improve disclosure processes.
8. Every time the customer conducts a digital transaction, the customer should receive a digital receipt and the credit officer (or equivalent) should receive on his/her device a confirmation message for that same transaction.
9. If the provider is working with a third-party partner to provide payments, each time the customer makes a digital payment, both the third-party partner and the FSP must provide the customer with a receipt.
10. Train staff on how to communicate effectively with digitally illiterate customers.
11. Collect information about the digital channels to which your customers have access, and segment answers by customer type.
    - NB: Implementation guidance could be once you have asked customers how they get information, then deliver information through those channels.
    - NB: In the Universal Standards, indicator 4.B.1.1 lists all the information that a key facts document should contain, as shown below. Consider adding to that list two additional pieces of information:
        - how to file a complaint
        - how to speak to a live person

4.B	Standard	The provider gives clients clear and timely information to support client decision making.
4.B.1	EP	The provider is transparent about product terms, conditions, and pricing.
4.B.1.1	Indicator	The provider gives a Key Facts Summary Document to borrowers before they sign a contract. The document contains the following information: - Total loan amount - Pricing, including all fees - Total cost of credit: all principal, interest, and fees plus cash collateral - Disbursement date and loan term - Repayment schedule with principal and interest amounts, number, and due dates of all repayment installments - All deductions from principal disbursement (eg: first installment, commissions, fees, cash collateral, taxes), if applicable - How cash collateral / manadatory savings can be used in case of default, if applicable - Moratorium interest rates, terms, and conditions, if applicable

Promoting Benefits for Customers

Managing algorithm bias

1. The provider defines specifically what "fair" algorithmic function means for their needs.
2. The provider shares the definition of fair with its board of directors.
3. The board of directors hold management accountable for fair algorithmic function.
4. 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. Define what specific tests the partner will run to check that that the algorithm is "fair" according to your definition
        iii. Require the partner to check annually the algorithm's fairness, according to the definition determined by the provider, and make corrections, as needed.
5. If developing the algorithm in-house, credit officers and management take part in the development of algorithm design.
6. 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.

    - Before you launch the use of algorithm, test whether your *data* are biased, including whether certain potential target customer segments do not have any data.
    - Before you launch the use of an algorithm, use synthetic or real data to test the following:

i. Whether the algorithm is "fair," according to your definition of fairness
ii. Whether the algorithm is treating equally men compared with women
iii. Whether the algorithm is treating equally any other customer segments that are relevant to your social goals (e.g., rural vs. urban)

7. Before you launch the use of an algorithm, take the following steps to solicit feedback from stakeholders:

    i. Identify the stakeholders involved in the use of this algorithm

    ii. For stakeholders who are not customers, speak with representatives from each of the stakeholder groups to identify any concerns they have about the use of the algorithm

    iii. For stakeholders who are customers, interview representatives from each segment of customer that the FSP identifies as important (e.g., women/men)

    iv. Document what you've learned in a way that makes it clear which stakeholder group had which concerns.

    v. Qualify risks in terms of which would be high or low priority to mitigate, and then decide which you will address and which you will not

    vi. Take action to mitigate the risks you are going to address

8. Analyze your algorithm function for fairness on an ongoing basis, according the frequencies below:

    i. If the algorithm is learning continuously, check function at minimum monthly.

    ii. If an algorithm function is fixed, check function at minimum annually.

9. If you find that bias exists, determine if it is coherent with your social goals and strategy.
10. 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 want to serve
    - Whether the algorithm is working as intended (e.g., check whether the algorithm's decisions on loan sizes for target customers are the same that traditional repayment capacity analysis would make)
    - In the case of loans, assess whether the loan amount approved by the algorithm is appropriate for customers. Check this by not only repayment records but also investigating customer stress levels.
11. Share reports on algorithm function with senior management, credit department, the risk management team, and the board of directors; discuss results and identify any corrective action needed.
12. Use information from customer complaints to inform your review of algorithm function.
13. In cases of a systemic shock (e.g., a pandemic), discontinue the algorithm and review it.

14. At least some members of the team that define algorithmic "fairness," and determine what analyses to conduct to test fairness, represent the population whose data are being scored by the algorithm.
15. Do not use algorithms if you do not have the capacity to analyze whether their outcomes are fair.

Outcomes

1. Collect data on which customers are using digital products and which are not, by customer segment.[8]
2. Collect data on each digital customer's journey, including both quantitative data (what products did they use, how, when) and qualitative data (stress, areas of (dis)satisfaction).
    - 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.
3. Define what outcomes data to collect on digital customers and why, and then collect it.
4. Verify accuracy of customer data:
    - via automated, digital checks.
    - via spot-checks by humans
5. Have annual discussion at the management level to review data and identify potential concerns related to digital products (e.g., low liquidity among agents).
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 a savings product. But you would do quantitative calls to understand why certain customers are dormant.
8. Use outcomes data to inform product design.

Product design and delivery

NB: The DFS Working Group felt that some of the early ideas that emerged from expert interviews and document review were more guidance on how to implement than universally mandatory practices. Therefore, this section preliminary groups ideas into two sub-sections: those for standards, and those for the implementation guide:

Ideas for standards:

1. Research levels of digital literacy, by customer segment, during market and pilot research
2. Build the digital literacy of your customers enough for them to use the digital products and services you offer safely and effectively, at multiple stages of product use:
    - At the point of onboarding, when a customer first uses financial services.
    - Refresher digital literacy training
3. Pilot test digital products, using a stratified sample of customers so each major customer segment is represented
4. 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.
5. 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.
6. Offer technology in an opt-in way, not mandated.
7. Design digital interfaces as simply as possible, so that even those unfamiliar with numbers can use them.

[8] Related to this, some commenters mentioned that it could be useful to track data on customers' mobile phone usage, by gender, because there is still a much lower use by women.

8. Engage employees, customers, and agents as applicable, in product design.
9. Train employees on digital products, both how they function and what the benefits to customers are
10. Define incentives for product sales that incentivize employees and agents to sell in a way that is consistent with the benefits to customers that the FSP is trying to achieve.
11. Use data to inform product design, from all stages of the customer journey, meaning even before they become customers. Examples:
    - Data on problems you have already identified (e.g., no liquidity among agents)
    - 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.)
    - Track dormancy and reach out to dormant customers to understand why they have stopped using your products.
12. Adapt design and marketing strategies for products to customer segments (e.g., rural women, rural young adults)
13. If using a digital product or channel designed by a partner, verify that the FSP has the technical capacity to manage all aspects of the product
14. If using a digital product or channel designed by a partner, confirm that the product design develop by the partner adds value to the FSP's target customers

Ideas for the implementation guide:

- Remember not all clients have a Smart phone. Some have an old phone.
- Start product development with the discussion of what is not working well for customers and how to solve it.
    - One approach is bottom-up, not top-down. Example: Select partners that have found ways to use technology to address the pain points that your customers experience.
    - Another approach is top-down: conceive of a purpose for a product. The FSP may know of a product design that would be useful to customers even if they are not asking for it.
    - Don't start with technology and then develop a product around it.
- Some tips on building the digital literacy of your customers enough for them to use the digital products and services you offer:
    - Figure out who customers trust and deliver training for customers through them
    - View training as ongoing, not one-time
    - 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.
    - Use a lot of step-by-step guides and a lot of visuals.
    - 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
    - There could be business development services where users build capacities on different aspects of digital literacy.
- 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.
- 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.
    - This requires a break from traditional thinking, which involves spending a lot of time building and testing a single solution.
    - Drop things quickly that do not work.
    - 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
- Take advantage of technology allows for innovative and effective ways to deliver trainings to customers, including over videos or via IVR
- 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.
- Design products to address the four main barriers:
    - Affordability (This is not just price, but infrastructure – does she have a phone? Can she buy minutes?)
    - Availability (Note: women tend to need to be in their homes most of the day)
    - 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.)
    - Appetite (Does the product meet her needs? Does she trust it?)
- Design products iteratively with customers. Select a small group of customers for this.
- 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.
- Pilot test new products with employees first
    - "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
- Assign a unique identifier to each customer.
    - Note: A phone number is not always a unique identifier, as people share phones.

Responsible Pricing:

1. Board and management create a pricing strategy and review it with at minimum [X] frequency.
    a. NB: Should this be an indicator located within standard 1A ("The provider has a strategy to achieve its social goals.")?
2. Communicate to customers the annual percentage rate (APR) and all fees.
3. Have a simple* fee structure.

    a. *Define "simple" as easy for any customer to understand.

4. Disclose the fee structure at the time the customer is choosing to use a product, not only at the moment when the customer is being charged a fee.
5. Do not have a minimum balance requirement for a savings account.
6. Put systems in place to protect customers from overdraft fees.
7. When a customer defaults, do not charge compounding interest or late fees.
8. Structure interest rate and repayment schedules for loans so that the customer never ends up paying more in interest than s/he received in loan capital.[9]
9. Do not pass on innovation costs, inefficiency costs, or poor loan portfolio costs, to customers.
10. When the FSP realizes cost savings thanks to DFS, it reduces prices for customers.
11. Reduce prices for customers who have a demonstrated record of on-time payment.
12. Monitor credit scoring algorithms to make sure they get more effective over time, leading to better ability by the FSP to price appropriately given actual customer risk and repayment probability.

Collaboration with Third Parties

Agent management

1. Define criteria to determine how many agents the FSP needs and in what locations. Apply those criteria when deciding which new agents to add to the network.
2. Define criteria for agent recruitment, including eligibility criteria and fair, non-discriminatory factors to guide the selection process.
3. Have an agent code of conduct.
4. Sign a contract with each agent[10] that includes at minimum the following information:
    a. what information that the agent must display in her place of business;[11]
    b. the code of conduct the agent must follow when interacting with customers;
    c. the responsibilities of the agent in terms of recording and reporting transactions data;
    d. that the partner/agent confirms that they have read and agreed to all applicable data privacy laws;
    e. the responsibilities of the agent in terms of participating in training;
    f. agent base remuneration and incentive structure;
    g. the consequences for violating the terms of the contract / under what conditions the FSP would sever the relationship with the agent.
5. Before launching an agent network, create a strategy for managing agent liquidity in each market, at minimum for urban versus rural markets.

[9] One commenter wrote, "Rules out long tenure products."
[10] One commenter wrote, "Note: For simplicity, agents can also be bound by a contract that refers to various policies also binding on agents, which may be amended over time in a simplified manner (instead of re-contracting agents)."
[11] One commenter suggested that the FSP should also display information about the agent's business since the agent is displaying information about the products and services offered by the FSP.

6. 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.[12]
7. Evaluate and mitigate the risk of harm that agents incur because of their work.
8. Train agents up front on the following topics, at minimum:
    a. the provider's policies, processes, products and services
    b. the risks involved in the mobile money business, notably how to avoid fraud, and the mitigation strategies
    c. good customer service
9. Provider refresher trainings on key topic to agents, on an ongoing basis.
10. When introducing a new product, train agents on that product.
11. Assess the effectiveness of agent training, evaluating at minimum both whether the agent retained the information and whether the agent is applying the lessons communicated via training.
12. Build agent buy-in to the mission and vision of the organization through continuous engagement
13. Monitor each agent's adherence to the terms of her contract. Use both in-person and remote channels for monitoring.
14. Measure the level of activity for agents on a regular basis, at minimum in the following areas:
    a. what types of transactions the agent completed
    b. what types of transactions were requested but the agent could not complete them, and why
    c. frequency of transactions
    d. amount of transactions
    e. which platform/app the agent uses to conduct each transaction
15. Use data to monitor early warning sights of agent distress, rather than waiting for actual default or other bad behavior by agents.
16. Analyze customer complaints data for insights on agent behavior.
17. Implement a system of performance evaluation of agents. This system will include at minimum the following elements:
    a. Defining the performance indicators to be used for evaluation
    b. Defining the agent monitoring system
    c. Sharing with agents what the evaluation criteria are and how the FSP will monitor agent performance
    d. After an evaluation, share the results with the agent and provide suggestions for how to improve in weaker areas
18. 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.
19. Provide a channel that agents can use to ask questions/receive support on demand, including an opportunity to talk to a live human.
20. Conduct annual satisfaction survey with agents.
21. Check at minimum annually whether the information displayed at the agent's location about the FSP's products and services is up to date.

[12] One commenter said this is "impractical to implement."

22. If the FSP operates in a country where the regulator or another stakeholder hosts a database of fraudulent agents, the FSP reports agents that it has blacklisted to that database and uses that database to conduct due diligence before signing a new agent.
23. 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.
24. Consult agents about ideas for product design improvement.
25. Pay agents a certain fixed base amount.
26. Have a business plan that allows for agents to make money.
27. Make it possible for customers to use agents with their same gender.
28. Notify customers when agent locations change or close.
29. Inform customers of the principal ways in which agents can defraud customers (e.g., unauthorized fees) and what channel the customer can use to report any concerns.
30. 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?

Partnerships

1. Research the 3-5 most common problems that customers tend to have with any partner organization you are considering and ask the partner what steps it is taking to address these problems.
2. During contract discussions, ask about the potential partner's consumer protection practices:
    - Ask how the partner receives and resolves complaints.
    - Ask if the partners has a code of conduct policy and how the partner trains its staff on customer care.
    - Ask if the partner has a policy to prevent aggressive sales.
    - Ask how the partner protects customers from fraud.
    - Ask how the partner keeps customer data secure.
    - Ask what terms and conditions the partners imposes on its customers.
3. If potential partners do not yet serve the segment of customers you serve, discuss their strategies for serving them, and make the case why doing so would benefit them:
    - Ask potential partners if they already have plans to serve your customer segment and, if yes, what those plans are.
    - Prepare a case for why it's a win-win for the partner to adapt their offer to your customers
4. Have a service-level agreement (SLA) with each partner that includes at minimum the following: a) Complaints handling – who is responsible for what, and how do they resolve complaints; b) A plan to manage customer data privacy given the data that will be

shared between partners; c) Pricing; d) Data reporting – how does the partner report its data? How does the FSP have access?; e) If the partner uses algorithms, agree on a definition of what a "fair" algorithm function would be; f) If you are partnering to offer some online service to customers, specific who is responsible for what if that online system experiences a data breach; g) Exclusivity rules for activities like cross-selling and up-selling. Who owns the customer? h) Performance monitoring and reporting; i) Exit clauses – under what conditions do you cancel the agreement;

5. If you partner with an MNO, if possible, select one that achieved GSMA certification.
6. If you partner with a debt collection agency, ensure that the partner protects customers' rights to respectful treatment during the loan collection process.
7. Establish a direct line of communication and point of contact for your organization within the partner organization.
    - On suggestion is that for each partnership, there is a designated person within the FSP whose job it is to manage that partner relationship.
8. Define the indicators of success for the partnership. Agree on them with the partner and put them into the contract.
9. Meet on a regular basis (at minimum: semi-annually) with the partner to review what is and is not working and set expectations for future activities:
    - Review and amend as needed the projections for revenue and numbers of customers related to the product/service that is offered via the partnership
    - Analyze performance according to the indicators of success for the partnership
10. If customers lose money because of a failure in a partner's system, it is nonetheless the FSP's responsibility to restore funds to the customers' accounts. The FSP can pursue a refund from its partner organization separately.