cerise + SPTF

STANDARDS FOR RESPONSIBLE DIGITAL FINANCIAL SERVICES

10 June 2022

CERISE + SPTF
Standards for Responsible Digital Financial Services

(Draft as of 10 June 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*

ORGANIZATION OF THIS DOCUMENT

- **13 thematic categories for standards**:
  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 over-indebtedness
  11. Product design and delivery
  12. Responsible Pricing
  13. Transparency

DRAFT STANDARDS

/1/

Agent management

1. Define criteria to determine how many agents the FSP needs and in what locations, and apply those criteria when deciding which new agents to add to the network.
2. Have an agent code of conduct.
3. Sign a contract with each agent that includes at minimum the following information:
    a. what information that the agent must display in her place of business;
    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. the responsibilities of the agent in terms of participating in training;
    e. agent base salary and incentive structure;
    f. the consequences for violating the terms of the contract / under what conditions the FSP would sever the relationship with the agent.
4. Before launching an agent network, create a strategy for managing agent liquidity in each market, at minimum for urban versus rural markets.
5. 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.
6. Evaluate and mitigate the risk of harm that agents incur because of their work.
7. 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
8. Provider refresher trainings on key topic to agents, on an ongoing basis.
9. When introducing a new product, train agents on that product.
10. Assess the effectiveness of agent training.
11. Build agent buy-in to the mission and vision of the organization through continuous engagement
12. Monitor each agent's adherence to the terms of her contract. Use both in-person and remote channels for monitoring.
13. 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 request but the agent could not complete, and why
    c. frequency of transactions
    d. amount of transactions
    e. which platform/app the agent uses to conduct each transaction
14. Use data to monitor early warning sights of agent distress, rather than waiting for actual default or other bad behavior by agents.
15. Analyze customer complaints data for insights on agent behavior.
16. 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

17. 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.
18. Provide a channel that agents can use to ask questions/receive support on demand.
19. Conduct annual satisfaction survey with agents.
20. 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.
21. 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.
22. Consult agents about ideas for product design improvement.
23. Pay agents a base salary.
24. Have a business plan that allows for agents to make money.
25. Make it possible for customers to use agents with their same gender.
26. Notify clients when agent locations change or close.
27. 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.
28. 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?

/2/
Algorithm bias

1. The provider defines specifically what “fair” algorithmic function means.
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.
    - 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 clients, 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 clients, 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 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)
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 they are fair.

/3/
Complaints mechanism

1. Take responsibility to resolve a customer complaint even when it relates to an issue that the partner organization must correct.
2. 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.
3. Encourage your customers to come to you with complaints about partners.
4. Train customer service employees on how your partner's complaints mechanism works.
5. Train customer service employees on how to respond to customers who voice complaints related to services offered by a partner.
6. Train agents on how to respond to complaints.
7. Train/encourage agents to use your complaints mechanism.
8. Equip the complaints mechanism to register complaints by agents.
9. Analyze complaints data for the following information:
   i. to see if certain segments of customers are underrepresented among the customers who complain
   ii. to see if certain issues are underrepresented among the types of complaints
10. Research why some customers do not file complaints even when they have reason to complain, and address obstacles that prevent customers from complaining.
11. Proactively survey a sample of customers to ask if they have complaints.
12. Monitor social media to see if customers are complaining about your services, and respond as needed.
13. Do weekly trend analysis on the types of complaints you receive.

/4/
Cybersecurity

1. Define board and management responsibilities related to data security, including how the board will ensure risk management related to digital innovation and activities.
2. Include cybersecurity 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.
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.
12. Identify which person or team, either internal or external, is in charge of cybersecurity and, 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 (e.g., hack attempts, measures taken, new risks identified) to the board at minimum quarterly.
17. Report data on security activities to management at minimum weekly.
18. Notify customers within 24 hours if you do get hacked.
19. If customers lose money because your systems got hacked, refund the customer.
20. Notify other FSPs in your market of any attempts hackers make on your data security, including sharing the specific methodology they used.
21. Participate in any initiatives in your country or region involving information sharing about cybersecurity threats.
22. If you do not have the resources to invest in cybersecurity, then do not offer digital financial services.

/5/
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.
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
4. 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.
5. If you deny an application for a product, explain to the customer why you denied it.
6. The leadership of the FSP defines a strategy for how the FSP processes and uses data, and monitors the implementation of those practices.

/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 customer service, noting performance when responding to complaints both about the provider's services and complaints about third-party providers.
4. As part of the agent selection criteria, consider whether the personality, culture, and language(s) spoken will appeal to your target customers.
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 employees, agents, other partners.

/7/

Fraud

1. Create a strategy to mitigate fraud risk and address fraud if/when it does occur:
    - Quantify how much instance of fraud, as a percent of overall portfolio, the FSP will tolerate.
    - Research which types of 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.
    - Define the systems you will put in place to mitigate fraud risk.
    - 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 clients, 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 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 fraud.
6. Train employees and agents on how to detect and avoid fraud.
7. If you identify fraudulent activity, notify customers within 24 hours.

8. 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.
9. Monitor your response times each time you respond to fraud.
10. Share publicly what fraud attempts your FSP has confronted, to help others avoid it.
11. The board of directors oversees the implementation of fraud mitigation measures and monitors instances of fraud.

/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.

/9/
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 client 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 how the partner protects customers from fraud.
    - Ask how the partner keeps client 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 client 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 gets hacked; g) 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. Establish a direct line of communication and point of contact for your organization within the partner organization.
7. Define the indicators of success for the partnership. Agree on them with the partner and put them into the contract.
8. Meet annually with the partner to review what is and is not working and set expectation for the coming year:
    - 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
9. 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.

/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

/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)

/12/
Responsible Pricing:

1. Board and management create a pricing strategy and review it with at minimum [X] frequency.
2. Communicate the annual percentage rate (APR) and all fees.

3. Have a simple fee structure.
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. Do not pass on innovation costs, inefficiency costs, or poor loan portfolio costs, to customers.
10. Reduce prices for customers who have a demonstrated record of on-time payment.
11. 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.

/13/
Transparency

1. In addition to document and sharing key facts in an agreement, develop clear messaging, in local languages, to use to disclose key facts again in a quick and accessible manner.
2. 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.
3. Design digital interfaces to be simple and visual enough to be used even by those who are not digitally literate.
4. Give customers an option to speak to a live person.
5. 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.
6. 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.
7. 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.
8. Collect information about the digital channels to which your customers have access, so you know through which channels you can share information. / SIMILAR TO / Ask customers how they get information. Then deliver information through those channels. Segment the answers by customer type.