Working Group on Standards for Responsible Digital Financial
Meeting Minutes
Topics: Data Rights & Privacy and Partnerships

(*Wednesday, June 8, 2022*)

Meeting overview: In this meeting, we reviewed the content of the draft standards for two different topics, data rights & privacy and partnerships. Participants shared their ideas on what to add, delete, or refine.

Learn more: Visit the Working Group's webpage to download the latest draft of the standards for responsible digital financial finance, to find content from previous meetings and to see the dates of upcoming meetings, Contact ameliagreenberg@sptfnetwork.org with any questions.

Introductions and Updates

- Amelia Greenberg, SPTF's Deputy Director and head of the Responsible Digital Financial Services (DFS) Working Group led the webinar. Guest Speakers were Matthew Soursourian from the OECD on data rights & privacy and Julien Mahuzier, from Juakali, on partnerships.
- Meeting minutes, recording, and notes, as well as updated sections of the DFS standards based on working group input, have be posted to the DFS Working Group page.
- The DFS working group will host one summer meeting, on July 20, by popular demand. The topics will be reaching the hardest to reach, and outcomes.
- The Cerise+SPTF 2022 annual meeting will take place in Paris, 28-29 September. On Sep. 28th, a full-day DFS working group meeting. On Sep. 29th, the main conference.

Context: Overview of Cerise + SPTF's work on standards

- Over the past decade, SPTF published and has periodically updated the Universal Standards for Social and Environmental Performance Management ("Universal Standards"), which is a comprehensive guide of best practices to help FSPs put clients and the environment at the center of all decisions. SPTF and CERISE, with input from other stakeholders, have also developed an infrastructure of assessment tools and implementation resources for FSPs.
- With the rise of digital financial services, many of SPTF's stakeholders – including financial service providers, networks, investors, and regulators -- have asked Cerise+SPTF to identify best practices in DFS. In 2021, SPTF began interviewing experts in digital inclusive finance, and so far has conducted around 50 interviews.
- Reminder: the standards say the what, but not the how.

Three quotes from experts that SPTF interviewed to kick off the discussion on data rights and privacy:

- "What I've seen in Uganda and Kenya, they couldn't care less about their data. They are more worried about getting the money and putting food on the table."-DFS expert A
- "We're all signing away our data rights without thinking about it." -DFS expert B
- "People are sheep to slaughter with most of their personal information on the internet today." -DFS expert C

Data Rights & Privacy: What is already in the Universal Standards for SEPM?

4.D The provider secures client data and informs clients about their data rights.

- 4.D.2. The provider informs clients about data privacy and data rights.
  - 4.D.2.1 The provider explains to clients how it will use client data, with whom it will share the data, and how third parties will use the data. The provider receives clients' consent before using or sharing their data.
  - 4.D.2.2 Information about data use and consent is easy for clients to understand.

        - 4.D.2.2.1 When requesting consent from clients to use their data, the provider explains in simple, local language, either in writing or orally, how it will use the data. Internet links to disclosure statements are not sufficient.
        - 4.D.2.2.2 The provider trains clients on the importance of protecting their personal information including Personal Identification Numbers (PINs), savings account balances and information on repayment problems.
        - 4.D.2.2.3 The provider gives clients the right to withdraw their permission to use data and explains any consequences of withdrawal.
    - 4.D.2.3 The provider notifies clients of their right to review and correct their personal and financial data.

Ideas so far for additional management practices to add to the Universal Standards manual related to data rights & privacy:

1. If you provide an opt-out option for data sharing, explain what the consequences are of opting out.
2. Ask for the minimum amount of data you need from customers.
3. Inform customers of their rights to see their own personal data.
4. If you sell the customers' data, inform them about who is buying it and why.
5. Customers have to give consent before any of their data can be shared with third parties.
6. Explain to customers why their loan applications were denied. Could be the customer was denied because the data on the FSP has on them is inaccurate.

Expert Reflection: Matthew Soursourian, of the OECD Financial Consumer Protection team

- An OECD Task Force helped develop the G20 high level principles on financial consumer protection in the wake of the global financial crisis in 2011. These principles are the leading international standards for financial consumer protection regulatory frameworks. The document has ten high-level principles, one of which focuses on consumer data and privacy. This principle talks about how financial and personal information should be protected, including that there should be protection mechanisms that dictate why data can be collected, how it's held, processed, used, and disclosed, especially to third parties. There should be acknowledgement of the rights of consumers to be informed about data sharing.
- The G20 OECD Task Force on Financial Consumer Protection also has created documents called "effective approaches to support the implementation of the high-level principles." These are practical and non-binding policy guidance that discuss how the principles can be implemented, drawing on actual examples from around the world.
- OECD began a review of the principles in 2021 and expects to publish by the end of the year a revised set of principles. For now, though, the principles on data and privacy have not changed significantly.
- Regarding the standards that SPTF proposes, it is good that the language is very strong on emphasizing disclosure and transparency and giving customers agency to make choices about how they want their data to be used. Being transparent about what is collected and used and giving consumers the ability to make decisions is very important. There are clear parallels between this section and the G20-OECD Principles.
- The Universal Standards also say that the language requesting consent should be clear and understandable; not overly technical. We agree this is very important.
- Additionally, it is important for the governance within an institution to make structural choices that ultimately favor the customer. For example, both the SPTF standards and the OECD principles promote data minimalization and privacy-friendly default settings, such as a default setting that the customer has to opt-in to share data, rather than needing to opt-out. [Side note: it's true there are two sides to this. On one hand, you want to give customers agency to decide. On the other hand, you don't want to overburden them with having to make too many choices.] In terms of themes that could be added to the SPTF standards, it's good to give consumers choice, but underneath those options there should be a baseline governance system that ensures that the providers are using data responsibility. The SPTF standards

could highlight this a bit more.

- [Reply from Amelia] Dimension 2 of the Universal Standards does say that the board and the management need to review consumer protection data regularly, including adherence to consumer protection practices that are mandated in company policy. The three sources of data that the board and management can use to monitor consumer protection practices are reports from internal audit, complaints data, and client satisfaction survey data. Are there other governance mechanisms that should be in place?
- [Reply from Matthew]: I did not review dimension 2 before the call today. It could be useful to reference governance again in the data rights and privacy section, to remind the reader that there should be an internal governance system that sets the overall framework for how customer data is processed and used so there is clarity throughout the organization on what is okay and not okay. It is good to have internal audits and other mechanisms to make sure that those standards are being adhered to.
- [From Matthew]: Regarding the minimum amount of data, the SPTF standards could spell that out a bit more. For example, say collect only data that is used for legitimate purposes.
- [From Amelia]: How much data you need for “legitimate purposes” can be grey. For example, CFI did a small study talking to thin-file customers about the data they collected on them. Customers initially said they understood why the financial service provider (FSP) needed data on whether they paid utilities or rent, but were less sure the FSP needed information like how many people were in their contact list or whether they send a lot of texts at 3 am. But when the FSP explained that their algorithms show correlations between those data and risk, and that if they use those data too in the algorithm, the customer might appear as lower risk and then get a lower interest rate, the customers were more inclined to share those data that at first seemed not closely related to their credit worthiness. So this seems like a gray area, in that yes the FSP could make a decision with less data, but perhaps it could make a better decision with more data.
- [From Matthew]: It is gray. I don’t know the answer, but I would consider is that there are probably diminishing returns on the data you collect. The big things that are going to help a FSP know about your credit worthiness are how you pay your bills and what your income is. This other stuff maybe helps at the margins, but I personally feel a little skeptical about collecting everything. But if the FSP can make the argument that this data is being used for legitimate purposes, because it’s an input into our model that’s going to assess your credit worthiness, then it’s ok. Don’t collect things that have nothing to do with what you are going to do for the customer.
- [From Amelia] That was our rule. If the data feed into the algorithm, then they are relevant. We did not say you should design an algorithm that uses fewer data points. But if you’re not using the data to make decisions, then do not collect it.
- [From Amelia] We heard a debate about best practice for informing people that they can correct the data about them that at FSP stores. One side points to the United States, where some FSPs do contact customers annually to say here are the data we have about you (e.g., address, beneficiary), and will you check these for accuracy? The other side said that is too expensive, and it is okay for the FSP to have a less expensive system that tells clients at the time they onboard for example, just so you know if you ever want to see what data we have for you, you can call our complaints and make that request. What do you think?
- [From Matthew] I think it depends on the context. It’s likely easier for multinational banks operating in the U.S., but I can see it would be very challenging for smaller FSPs. At a minimum, consumers should be aware that they have the option to request data, similar to tech companies like Facebook (Meta), Amazon, where you can reach out to them and say you want to extract all your data. Customers should be sensitized to this right.
- [From Amelia] What is an effective mechanism to inform people about their data rights? Sending a link to a document detailing rights is not the solution because a) not everyone has a smartphone and b) people don’t read contracts. Another mechanism could be sending SMS messages, but if phones can have data storage maximums that prevent them from receiving another text message. Another idea is to call a sample of customers to assess how aware they are of their data rights.

- [From Matthew] I don't have an exact mechanism, but I think the principle should be that all of this should be as simple as possible. If you cannot explain it simply, then the product or policy is itself too complex. Products/policies should be straightforward.

Transition to Discussion on Partnerships

Three quotes from experts that SPTF interviewed kicked off our discussion on partnerships:

- "If you build your business on partnerships, you need to understand the risks…If you are at the point where you need to dissolve the partnership, the damage is already done." -DFS expert A
- "The biggest problem was defining the project well." -DFS expert B
- "The partners promised to deliver something that they did not really have. Their intention was that when you pay them money, then they get more staff." -DFS expert C

Partnerships: What is already in the Universal Standards for SEPM?

- The manual does not yet include guidance on how to select the right partner or write an effective partnership agreement, but the Universal Standards do include thoughts on how to ensure client protection and promote positive outcomes for clients in the context of working with partners. Some examples:
    - Code of conduct (4c14: If the provider partners with third parties, it reviews the third party's code of conduct prior to signing.)
    - Complaints resolution (4.E.1.3.2 The provider informs clients on how to submit a complaint both to itself and to any third-party partner and 4.E.3.3 If the provider partners with third parties, the provider helps its clients to resolve complaints they have with those third parties.)
    - Data security (4.D.1.4 If the provider works with third parties that have access to client data, the provider's agreements specify that third parties will maintain the security and confidentiality of client data.)
    - Offering green products (7.1.C.3.5 Entering into partnerships with third parties to increase the provider's ability to offer high quality green practices and technologies to its clients.)

Partnerships and DFS: ideas for management practices so far

1. 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.
2. In advance of discussions with potential partners, if your customers are different from their typical ones, prepare a case for why it's a win-win for the partner to adapt their offer to your customers.
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.
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.
5. During contract discussions, ask how the partner resolves complaints. Use specific examples taken from common complaints.
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. Ask potential partners what systems they have to protect customers from 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:
    a. For MNOs specifically, they must share certain key data:

i. Transactions data (e.g., who transacts, when, how much)
ii. Complaints data (who complained, about what, when was it resolved)
iii. Network downtime

b. For all partners:

i. Define who handles customer complaints Be clear about who specifically in the staff responds.
ii. Define how 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?
iii. Clarify pricing
iv. Exit clauses – under what conditions do you cancel the agreement. Include terms about bad customer service that would lead to contract termination.
v. Data reporting – how does the partner report its data? How does the FSP have access?
vi. In general, identify the potential areas for there to be problems. Don't focus just on the benefits that will accrue to each party.

c. For partners that provide algorithms, agree on what parameters they will put into their algorithm.

11. 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.
12. 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.
13. Create a contractual relationship that allows you to iterate.
14. Define the indicators of success for the partnership. Agree on them with the partner and put them into the contract.
15. Establish a direct line of communication and point of contact for your organization within the partner organization.
16. 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.
17. If you partner with an MNO, select one that achieved GSMA certification.
18. 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. / SIMLAR TO / 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.
19. Understand what terms and conditions your potential partners would impose on your customers.
20. 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.
21. 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.

Expert Reflection: Julien Mahuzier, CEO at Juakali (financial inclusion startup)

- Julien has worked in the financial inclusion sector for 15 years. He started Juakali three years ago. It is a tech provider that equips microfinance banks with cloud-based solutions for data collection and to automate workflows. Covers everything from the loan origination data to the bad debt recovery.
- Similar to Matthew, I wanted to talk about the amount of data that should be shared amongst partners. On our side, we are going to partner with microfinance banks, ranging from Tier 3 to Tier 1 institutions. In some cases, we inject data into their system that has been collected through ours, or we are going to read information from their systems, or from third-party systems with which they contract, such as credit bureaus.

- Generally, Juakali gets access to too much data, even when it works with Tier 1 institutions that are pretty good at managing their IT systems. We are trustworthy but still if we were to get hacked, then the hackers could get all this data. The less data you have access to, the better for us and the better for you. There are a lot of ways to anonymize or obfuscate data. One option is to use third-party middleware that allows the FSP to provide only a certain amount of data and no more. From the beginning, give as little access as need be.
- [From Amelia] Sometimes, when your company enters into conversations with possible partners, you find they are not very knowledgeable about cybersecurity and/or did not budget for it. Do you recommend they do their research? Or if that's not realistic, do you have tips for how to inform them and make those conversations more productive?
- [From Julien] We do not have those conversations because these are our clients, and we want to have their business. Serious security problems we would address up front, but otherwise it is over time that we share with them how best to use our technology. However, the best clients are accompanied by some third-party consultancy, that does project management and/or security assessments on their behalf.
- [From Amelia] When hacking occurs in a partnership, it can be the case that each side says to the other, you have to fix this. Have you had the discussions where you decide in advance who does what, such as informing clients, informing law enforcement or the regulator.
- [From Julian] We have never been hacked. We do have a lot of legal jargon around this in our contracts. In general, the FSP is in charge of solving the issue because they are the customer-facing entity. It is true the resolution mechanisms are not always clearly defined. If our service were customer-facing, we might have more responsibility to take action.
- [From Julian] When you start partnering with a third-party company that is going to manipulate some of the data, then you have to make sure that this data is going to be addressed and used the way the regulatory body prescribes. You have to understand the regulation. It could be in certain countries that the regulation is so restrictive that it inhibits partnerships. And if the regulation is gray, then you need to have a connection with the regulator. Perhaps if they trust you, you can make it work, or you simply don't work there.
- [From Julien] Regulation can be complicated. We are a Europe-based company, so we must respect the EU General Data Protection Regulation (GDPR), but it only applies to data subjects that are European citizens or European residents. If I work with someone in Nigeria, some of the clients of my clients could be French citizens and therefore subject to the GDPR.
- [From Amelia] Should an FSP looking to partner put in the time to get knowledgeable about its own regulatory environment, or can it rely on potential partners to inform them?
- [From Julien] You are the one signing the contract. You are in charge of the data. You are the one who is regulated. So frankly don't trust anyone. The FSP should be informed.
- [From Amelia] What tips do you have about conversations to have up front to create effective partnerships?
- [From Julien] I did some of the GSMA certification on the technical side. The level of complexity in some cases is overwhelming. I'm bringing that up because when we dealt with our first large client, they came up with a list of requirements to meet around security. All of our staff, for example, had to get a specific type of antivirus software for their computer. We had to ensure that our staff working remotely can get safe access to different parts of our platform. FSPs are good at assessing risk. This was something the FSP did to reduce risk.
- [From Mario Umpierrez (Co-founder PACTO!)] Regarding service level agreements (SLA), which we all agree is the main tool to manage relationships with partners. I wouldn't put the emphasis on avoiding entering into long-term partnerships. Instead, focus on having intermediate steps or milestones, and if those conditions are not met, then you can cancel the partnership. Each year, you check whether you are meeting the conditions to continue. It ends up being costly if you have to write new contracts and lawyers are involved.
- [From Mario] I recommend a bilateral committee. Both parties in a partnership should meet to discuss what things have been good and what things were not so good, and what measures can be taken to solve or prevent them. Schedule this as a standing meeting. You could have check half-way through the year whether you are in line with projections and raise issues, as

well as the year-end meeting. There also has to be space for on-demand interaction.

- [From Julien] I think this sort of meeting would be useful. We would likely charge more for a shorter contract than a longer one, so it makes more sense to add in an exit clause to a longer contract instead of saying the contract will be one or two years. Remaking the contract can get expensive.
- [From Amelia] To summarize the discussion: a) Getting as informed as possible before your contract negotiations is useful; b) You don't want to get stuck in a partnership that doesn't work. It's still possible to do that in an agreement that is longer than 1 or 2 years, but the way you do that is you have defined metrics of success, regular lines of communication, and a scheduled annual check-in. The contingences in the SLA allow for an exit if the contract is not working well, and not meeting the definition of success you set in advance.

Final Thoughts:

- If you are interested in providing feedback, or if you know someone else who should, contact Amelia Greenberg (ameliagreenberg@sptf.info).
- 20 July, 10AM-11AM EDT: Reaching the hardest to reach; outcomes
- 28 September, 9AM-5PM CET: DFS Standards Working Group Meeting (in person)