cerise + SPTF

Working Group on Standards for Responsible Digital Financial Meeting Minutes
Topic: Cybersecurity and Fraud

(*Tuesday, May 17, 2022*)

Meeting overview: In this meeting, we reviewed the content of the draft standards for two different topics, cybersecurity and fraud, and 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, began the meeting with quick introductions of attendees and updates.
    - Jean Louis Perrier, Program Director at ACRC (Senegal)
    - David Medine, Independent Consultant (USA)
    - Estrella Andres, ASHI Philippines
    - Mario Umpierrez, Independent Consultant (Uruguay)
    - Herminia Anago, SPM Manager of ASHI Philippines
    - Frederick Williams, CEO for Access Financial Services, Jamaica
    - Mediatrice Mukarugwiza, Independent Consultant (Rwanda)
    - Malkhaz Dzadzua, Independent Consultant, Board member of IMON Tajikistan and Board member of SPTF (Georgia)
    - Sandeep Panikkal, Healing Fields Foundation (India)
    - Ruth Dueck-Mbeba, Independent Consultant (Canada)
    - Sana Zehra, M-CRIL (India)
    - Isabelle Barrès, Independent Consultant, former director of Smart Campaign (USA)
- Meeting minutes, recording and notes are posted to the DFS Working Group page.
- SPTF updated the Responsible DFS Standards document section on complaints mechanism and fair and respectful treatment of clients.
- Schedule for virtual meetings: bi-monthly, 90 minutes, two topics
- SPTF annual meeting in Paris, 28-29 September; a full-day DFS working group meeting will take place on the 28th while the 29th will be for conference plenary sessions

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.
- Creating such DFS standards would:
    - Clarify what it means to have good management practices in DFS.

    - Enhance transparency
    - Encourage good practices to grow
    - Propose concrete solutions to the risks we observe
    - Enable stakeholders to distinguish between providers with a desire to create value for clients versus those focused solely on profits.
    - Facilitate partnerships between responsible providers.
- To develop the standards, SPTF conducted a literature review plus interviews with a broad cross-section of experts.
- SPTF reviewed the following principles/standards/guidelines that relate to responsible DFS while developing the draft DFS standards:
    - G20 High-Level Principles for Digital Financial Inclusion
    - IFC Guidelines for Responsible Investing in DFS
    - BTCA Guidelines for Responsible Digital Payments
    - GSMA Mobile Money Certification
    - Smart Campaign Digital Credit Standards
    - GOGLA Self-Assessment
- If you are interested in providing feedback, or if you know someone else who should, contact Amelia Greenberg (ameliagreenberg@sptf.info).
- The Universal Standards for SEPM apply to all FSPs including DFS. In the latest iteration of the Universal Standards, we did include some practices specific to the responsible provision of DFS. However, we had not yet identified a comprehensive set of responsible DFS practices. That is the work happening now, with the input of the working group. In the future, the goal is to have one fully integrated manual and one assessment tool. We do not know what this will look like but will be determined after we have identified all the management practices for the DFS standards.
- The DFS Working Group is open to all.
- Reminder: the standards say the *what* to do but not the *how*.

Cybersecurity: What is already in the Universal Standards for SEPM

- Two quotes to kick off our discussion are “People are sheep to slaughter with most of their personal information on the internet today.” – DFS expert A and “We are at the stage where what is involved is not only the protection of data of a single consumer in an institution or 10,000 consumers, but what is possible thanks to the skills of the hackers and the tools they have is they can really stop an institution almost any day.” – DFS expert B
- 2.A.3 The board makes strategic decisions based on social and financial data
    - 2.A.3.1 The board uses the following data, provided by management, to monitor client protection. Minimum frequency: Annually
        - 2.A.3.1.4 Reports on the provider’s systems for data privacy and security, particularly any failures or breeches.
- 4.D The provider secures client data and informs clients about their data rights
    - 4.D.1 The provider maintains the security and confidentiality of client data
        - 4.D.1.1 The provider has data security and confidentiality policies that cover the gathering use, distribution, storage and retention of client information.
        - 4.D.1.2 The provider maintains physical and electronic files in a secure system.
            - 4.D.1.2.1 System access is restricted to only the data and functions that correspond to an employee’s role (“least privilege” principle)
            - 4.D.1.2.2 The provider controls employee use of files outside the office and the provider keeps records of the names of employees who request/are granted access to client files.

            - 4.D.1.2.3 The provider defines a clear process to safeguard client data when employees leave the organization
        - 4.D.1.3 The provider conducts a risk assessment to identify the data-related risks to clients. Minimum frequency: every year
        - 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
- Ideas for management practices so far:
    - 1. Implement a cybersecurity system that has at minimum these features: ongoing automated checks and flagging of anything suspicious, daily (at minimum) data back up, and a 24/7 data security system that detects attempts to hack into your files.
    - 2. Create a multi- year budget for projected cybersecurity costs.
    - 3. Take the following actions to achieve acceptable data security:
        - a. Increase awareness of management and the board.
        - b. Get an external audit of your data security
        - c. Train the technical team on risk management.
        - d. Strengthen all gap areas
        - e. Implement all software updates [*added recently]
    - 4. Any time you release a new digital product/service, assess data security for that specifically and implement new security measures as needed
    - 5. Adapt security measures based on what is core to business function versus what is less important, putting in place the strongest security for the most fundamental functions.
    - 6. If you work with partners, make sure you understand and are comfortable with their data security measures.
    - 7. Develop threat scenarios for the kinds of incidents that relate to your organization's highest priority cyber risks.
    - 8. Have a contingency plan for cyberattacks.
    - 9. Build capacity to respond to those scenarios.
    - 10. Have an expert on data security in charge of cybersecurity. The person could be internal or external. Have a plan to cover the work when that person is out of the office.
    - 11. Train the IT team on incidence response.
    - 12. Train customers on cybersecurity, on an ongoing basis
    - 13. Educate your entire staff about cybersecurity, on how to talk to customers about cybersecurity, and how to direct them to the right person if an issue arises.
    - 14. Define / clarify board and management responsibilities related to data security.
    - 15. Train board members on cybersecurity.
    - 16. Have a board committee that oversees risk management related to digital innovation and activities.
    - 17. Report data to the board on security activities (e.g., hack attempts, measures taken, new gaps or risks identified) at minimum quarterly.
    - 18. Report data to management on security activities at minimum [X frequency] (weekly?)
    - 19. Notify customers within X time (24 hours?) if you do get hacked
    - 20. If customers lose money because your systems got hacked, refund the customer.
    - 21. At least once every [X frequency] (month? quarter?), try to hack your own data.
    - 22. If someone tries to hack you, notify other FSPs in the same market, specifying the methodology the hackers used in their attempt.
    - 23. Participate in information sharing about cybersecurity threats between public and private entities like with the police.
    - 24. Have an "Internet Management Policy" and update it every six months

  - 25. If you don't have the resources to invest in data security, then don't offer DFS.
  - Some additional ideas:
    - Install physical security measures (e.g., could say more about locks and security cameras)
    - Monitor employees' use of computer systems and audit their activities (e.g., who logged in, for how long, and what did they do?

Expert Reflection:

- **Jean Louis Perrier, Africa Cybersecurity Resource Centre (ACRC)**
  - The "what" is very important. The language and awareness have improved significantly over the past 2-3 years. For example, the attendance at the Africa Microfinance Week from 2019 – 2021 increased. The deepness of the questions was much greater. This is in large part because the central banks have been made aware of the cybersecurity situation.
  - There are several cybersecurity frameworks that say you must work on the physical security, the information systems themselves, and the vendors (interconnection with vendors and customers). It is not easy to distinguish between what should be an obligation and not. There is a real need to establish a road map that exposes the risks institutions are exposed to. It is still necessary to give an overview and support the institution in their journey of cybersecurity.
  - This should also be adapted for the local regulation and specificities of the market.
  - Regulation may not be that good even if the intent is good (example of central bank in Africa that gave institutions only 6 months to comply)
  - Must take the size and resources of the institutions into account (example tier 3 MFIs are different from established banks) Even tier 1 MFIs are lagging far behind banks with the most maturity.
  - Important to note the concept of cybersecurity and cyber-resilience when it comes to stopping and restarting an organization. Example of a pipeline company in the US that stopped for 2 weeks and was hacked during this time.
  - Question from Amelia: If you are an organization that is brand new and you need to have a plan if you get hacked, what are the first steps? Is it talking to an expert organization to do an assessment? Sending staff to a training to build capacity? In practice, what have you seen?
  - Response: Having a backup in place is key, though the backup can be hacked. Double-check the reliability of everything. Taking the information or money from 1 account can be life threatening in fragile communities. If you do not have a guarantee in place the financial institution is at risk.
  - Question from Amelia: If you do not have the money to restore the funds if all accounts are stolen, do you have a responsibility to tell your customers the risk they are assuming, for example, by having an eWallet?
  - Response: Institutions need to have a process on how to inform the customer of what happened. Not knowing what happened or what has been stolen is the highest threat for an organization. A mix of external cyber-attacks and internal fraud is also a threat. Institutions should analyze what transactions have been made to be informed.
  - Summary from Amelia: Communication is less important preemptively but more to think about giving them information they could use if the institution is hacked.

Discussion:

- Comment from Amelia addressing Malkhaz Dzadzua to speak to the importance of informing the board of cybersecurity risk and requesting money be set aside to address cybersecurity.
- **Malkhaz Dzadzua, SPTF Board Member**

    - Many board members recognize the importance of cybersecurity only once something bad happens. Board members do not have the skillset or knowledge of cybersecurity. Providing the general information around cybersecurity helps. One board member should have IT skills.
- **Mario Umpierrez, Independent Consultant**
    - Mario has an IT background. He says that the last point in the presentation is the single most important – to inform the board of directors. It is particularly important that the board receives a proper introduction into digital and cybersecurity risks. You should not go digital if you do not have the right funds or tools (experts that can guide you through the process). Regulated institutions are already inheriting elements of cybersecurity (what is covered in the standards today). You are going to find institutions that are resilient towards cybersecurity because they have already had to protect their systems anyway.
    - The extra practice would be to have professional organizations test the resilience of these institutions and their digital infrastructure.
    - Less access is more secure.
    - Fintechs have a theme of having the minimum number of interactions with the user through their user interface to be as economical in the checks that they do. They will only check the ID against the credit bureau (rather than multiple forms of verification). This can inadvertently create pathways for impersonation. So, if someone gets hold of another person's ID, they can go through the system and apply for a credit.
- **Estrella Andres, ASHI Philippines**
    - ASHI moved from an external provider to a new provider. It would be advisable for ASHI to make an audit of the new system to ensure that data in the new system will be handled properly.
    - Question to Mario: Would it be helpful for ASHI to get an external expert to look at the reliability of the new system?
    - Response from Mario: Yes, of course. You need to be able to measure the reliability first. Doing a resilience check of the existing systems and infrastructure will be the first step. You need to assess your situation to cover your primary vulnerabilities and have a process in place to sustain these checks over the next few years.
    - Comment from Amelia: If you work with an expert, they can have structures to monitor your systems on an ongoing basis in real time. Even if you monitor it in house, it is important to have a relationship set up, so you know who to call if there is a problem.
- **Mario Umpierrez, Independent Consultant**
    - Comment from Mario: Has seen data breaches turn into physical breaches such as robberies, etc. Sometimes branches or headquarters breached from their own security cameras. If someone gains access to the cameras to monitor who enters, they have a window into your home. They can get significant insight on how money moves from one place to another. Also think about the security of your infrastructure.

Fraud: What is already in the Universal Standards for SEPM

- Two quotes to kick off the discussion on fraud: "Over the past few years, several serious cases of fraud have been reported that have raised concerns within the industry. As mobile payments begin to scale in many markets and new products are introduced, there is growing need to address fraud conclusively." – MSC brief and "Based on available evidence, there is massive increase in volume of records exposed and frauds such as SIM swap fraud, account takeovers, and social media scams have also worsened. – CGAP research
- 2.A.3 The board makes strategic decisions based on social and financial data
    - 2.A.3.1.5 Reports on any fraud or corruption, including extorsion and bribery

- 2.B.2 Management makes strategic and operational decisions based on social and financial data
  - 2.B.2.1 Senior management analyzes the following data and assesses risks. Minimum frequency: Annually
    - 2.B.2.1.1 Analysis of client protection risks (over-indebtedness, unfair treatment, lack of transparency, privacy of client data, complaints, fraud, corruption, and bribery)
  - 2.B.2.2 Internal audit and/or risk management integrates the following criteria into regular monitoring activities:
    - 2.B.2.2.3 Compliance with code of conduct; prevention of fraud and corruption
    - 2.B.2.2.5 Client data misuse and fraud
- 5.C.2 The provider trains all employees on its social goals and on client protection
  - 5.C.2.2 The provider trains employees on client protection, in line with their roles and responsibilities. The training covers at minimum the following topics:
  - 5.C.2.2.5 Confidentiality and data sharing policies and fraud risks, including common frauds, fraud identification and fraud reporting
- 5.C.3. The provider evaluates and incentivizes employees based on social and financial criteria
  - 5.C.3.2 The provider reviews incentive schemes to check for negative consequences such as fraud, customer mistreatment, aggressive sales, over-indebtedness, or high employee turnover
- Ideas for management practices so far:
  - 1. Determine which types of fraud are likely to occur at different stages of product use. Segment this by driver of fraud:
    - a. Consumer-driven fraud
    - b. Agent-driven fraud
    - c. Business-partner fraud
    - d. System-administration fraud
    - e. Fraud related to mobile-financial services
  - 2. Each time the FSP introduces a new product, analyze where fraud is most likely to occur.
  - 3. Put corresponding risk mitigation measures in place that at minimum include a system of checks and balances, scheduled audits, mystery shopping, and independent audits.
  - 4. Study which types of fraud are the most common at different points in a product lifecycle.
  - 5. Invest in fraud mitigation hardware/software/capacity building
  - 6. Share publicly about the fraudulent activity that your FSP has experienced, to help others in the sector avoid it
  - 7. Use data analytics to search for and identify fraudulent activity in real time.
  - 8. If you flag possible fraudulent activity, notify customers immediately. [NB: This idea is repeated as a suggestion for an element of an FSP's fraud response plan, in #14 below, but other experts said it should be a requirement, so SPTF is also listing it here as a possible standalone standard idea.]
  - 9. Have a daily dashboard that reports any exceptional activity
  - 10. Train customers on how to protect themselves from fraud, using more than one channel (e.g., radio, SMS).
  - 11. Train women customers especially carefully on how to protect themselves from fraud.
  - 12. Train customers specifically on the types of fees that are legitimate versus fraudulent.

    - 13. Train employees and agents on how to spot/avoid fraud
    - 14. Define what your fraud response will be, including the specific responsibilities of various employees when the FSP is responding to fraud (e.g., inform law enforcement)
    - 15. Monitor your response times each time you respond to fraud
    - 16. Use complaints data to inform anti-fraud measures. [NB: Collecting and monitoring customer feedback, and having an effective complaints mechanism, also helps the FSP to identify and manage fraud.]
    - 17. Define a strategy to avoid fraudulent fees charged by agents as this is a common source of fraud.
    - 18. Help customers who have experience fraud that they were not trained on how to avoid, including fraud by agents or sub-agents. Further ideas about this:
        - a. At minimum, this involves giving customers the information about how to contact the correct authorities to report the fraud.
        - b. Reschedule loans for customers who were victims of fraud.
        - c. On a case-by-case basis, the FSP can also consider helping the customer financially if s/he lost money.
            - GSMA principle 3 is “People management,” under which standard 3.3.2, says, “Providers shall assume responsibility for actions taken on their behalf by their agents (and any sub-agents) under the provider-agent contract.”
    - 19. Quantify how much instance of fraud, as a % of overall portfolio, you can tolerate vs when you will intervene.
    - 20. Have a board committee charged with fraud oversight.

Discussion:

- **Isabelle Barres, Independent Consultant**
    - One major challenge is having the appropriate resources given the financial cost. There are pooled resources that institutions have access to get the support that is required.
    - Jean-Louis shared a link to a free online assessment tool from ACRC for SME/MFI that is a good first step for making the board aware https://start.cyber4africa.org/
    - Ruth Dueck-Mbebe commented” I love the resource Jean-Louis. Carnegie Endowment has also put together a great toolkit that is free of charge https://carnegieendowment.org/specialprojects/fincyber/guides
    - Jean-Louis Pierre commented “The Fincyber guides are excellent, though high level”
- Comment from Amelia: Recommends FSPs do research for pooled resources available in their regions. Spread the information of fraud within your sector. Is there a vehicle to share this type of information? Look to see if the central bank is playing that role or another national association.
- Comment from Amelia: The types of fraud will continue to evolve. Inclination for the standards is not to be too specific, but general to address all types of fraud.
- Question from Amelia to Frederick Williams: Has Access put in fraud mitigation strategies?
- **Frederick Williams, CEO for Access Financial Services, Jamaica**
    - Access offers access to services digitally. They use technology to support identifying fraud risks. For MFIs you will be presented documents that need to be validated. How do you best use technology to validate this rather than asking team members?
    - The cost of cybersecurity monitoring can be significant for small companies. Does pooling resources together through cyber4africa lower costs for entities utilizing the services?
    - Comment from Amelia: Yes

    - That is useful in our environment. There are several small companies in the financial services space that have important data.
- Comment in the chat from Jean-Louis Pierre: “For Fraud, from my experience you would also greatly benefit from coordination with your peers on the market and train together the law enforcement, as most of the time they don't understand well financial frauds.”
- Comment in the chat from Ruth Dueck-Mbebe: “Institute of Internal Auditors and related partner GTAG (internal audit for technology) have detailed resources too”
- Comment in the chat from Jean-Louis Pierre: “For fraud, as for cyberthreats, and mixes, as Amelia stated, the number of diverse types of fraud is so huge and evolving that you have little possibility to follow the pace by yourself. Only sectoral collaboration will allow this at a cost. This is the way the telecom network work within the GSMA Fraud and Security Group (FASG)”
    - There is a huge trend of spending a lot of money on the technology and not on the security. You must approach this where technology is only a small part of the bigger picture.
- Comment in the chat from Mario Umpierrez: “This is an overall non-specific resource on Cybersecurity that can be an interesting entry point that gives you a broad picture of the things you might need to cover.” www.sans.org is another excellent resource.
- Comment from Jean-Louis Pierre: Investors also have a responsibility. The due diligence should include a larger part of cybersecurity. Financial inclusion institutions must also be funded for their cybersecurity by social investors.
- Comment from Amelia: We have a tool called ALINUS that any social investors use for due diligence. As the standards are finalized, the ALINUS tool will be updated, and cybersecurity will be included. But I understand your point as well is to ask, “Who is going to pay for this?” Likely this will be a partnership between FSPs and their investors.

Next Steps:

- Save the date for the next Working Group meeting.
- Invite your colleagues to join
- Read the draft DFS standards document.
- Send written comments on the document to Amelia Greenberg at ameliagreenberg@sptfnetwork.org.