Standards for Responsible Digital Financial Services Working Group Meeting:

Cybersecurity and Fraud

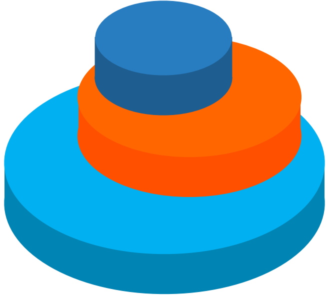
17 May 2022

cerise + SPTF

AFD

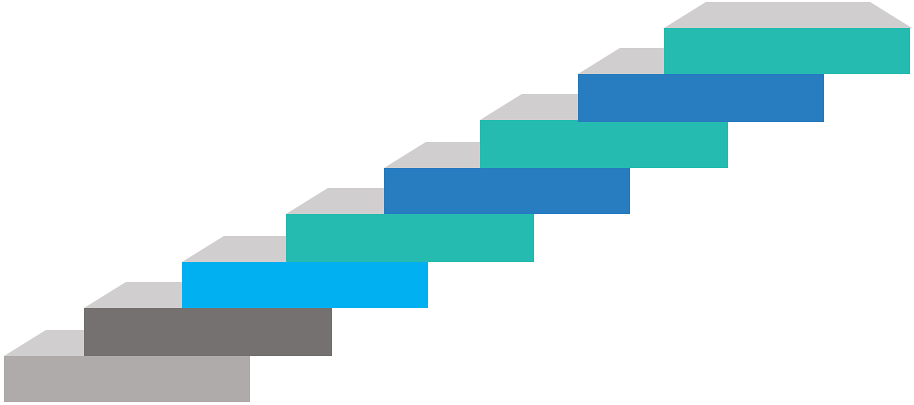
AGENDA

10:00 to 10:05	**INTRODUCTION AND UPDATES**
10:05 to 10:25	**DRAFT STANDARDS ON CYBERSECURITY**: review ideas so far
10:25 to 10:55	**EXPERT REFLECTIONS AND GROUP DISCUSSION OF CYBERSECURITY**
10:55 to 11:05	**DRAFT STANDARDS ON FRAUD**: review ideas so far
11:10 to 11:25	**EXPERT REFLECTIONS AND GROUP DISCUSSION OF FRAUD**
11:25 to 11:30	**NEXT STEPS** and conclusion



Updates

- Meeting minutes, recording, and notes are posted to the DFS Working Group page
- SPTF updated the Responsible DFS Standards document sections on complaints mechanism and fair and respectful treatment
- SPTF annual meeting in Paris, 28-29 September; full-day DFS working group meeting

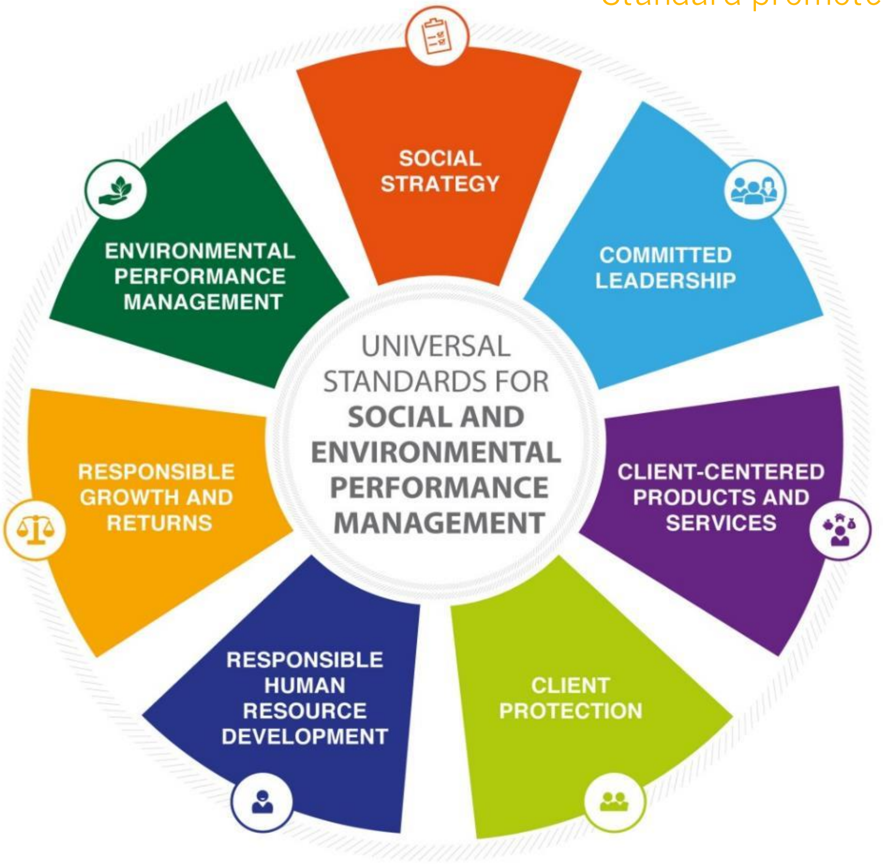


OUR WORK ON STANDARDS (1 of 2)

The Universal Standards for Social and Environmental Performance Management

Standard setter

Standard promoter


SOCIAL STRATEGY
COMMITTED LEADERSHIP
CLIENT-CENTERED PRODUCTS AND SERVICES
CLIENT PROTECTION
RESPONSIBLE HUMAN RESOURCE DEVELOPMENT
RESPONSIBLE GROWTH AND RETURNS
ENVIRONMENTAL PERFORMANCE MANAGEMENT
UNIVERSAL STANDARDS FOR SOCIAL AND ENVIRONMENTAL PERFORMANCE MANAGEMENT

A **complete guide** of best practices to help financial service providers (FSPs) put **clients and the environment at the center** of all decisions and **align** their policies and procedures with **responsible business practices**.

OUR WORK ON STANDARDS (2 of 2)
Standards for Responsible Digital Financial Services

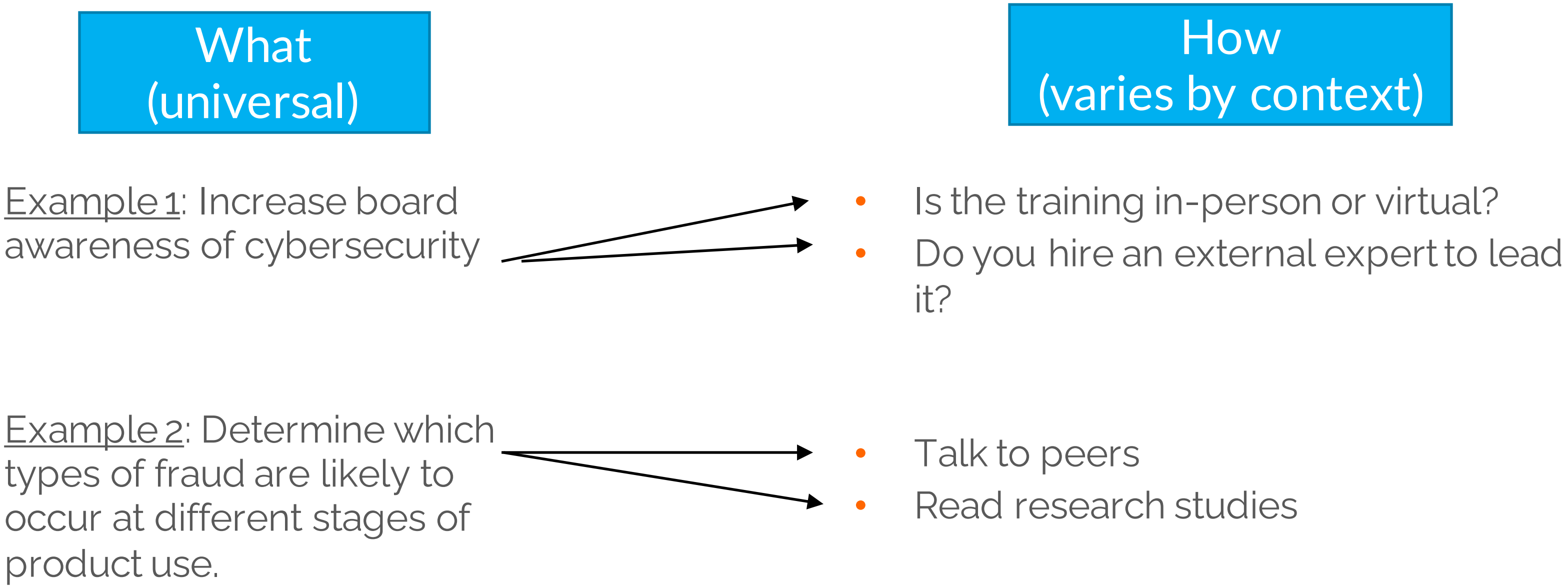
Why?

- Clarifies what “good” practice means
- Enhances transparency
- Encourages good practices to grow
- Proposes concrete solutions to the risks we observe
- Enables stakeholders to distinguish between providers with a desire to create value for clients versus those focused solely on profits
- Facilitates partnerships with responsible providers

How?

- Review of existing resources: research, articles, blogs, codes of conduct
- Expert interviews: ~50 so far
- Harmonization with existing principles and standards: GSMA, BTCA, IFC, GOGLA, G20 High-Level Principles for Digital Financial Inclusion
- DFS Working Group: open to all, provides a forum to share information and debate

Reminder: the standards say the what, but not the how



What (universal)

How (varies by context)

Example 1: Increase board awareness of cybersecurity

- Is the training in-person or virtual?
- Do you hire an external expert to lead it?

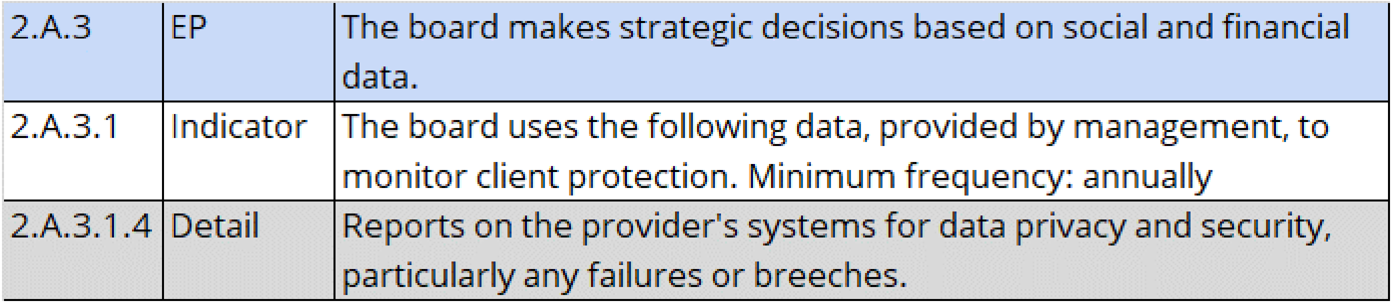
Example 2: Determine which types of fraud are likely to occur at different stages of product use.

- Talk to peers
- Read research studies

- "People are sheep to slaughter with most of their personal information on the internet today." – DFS expert A

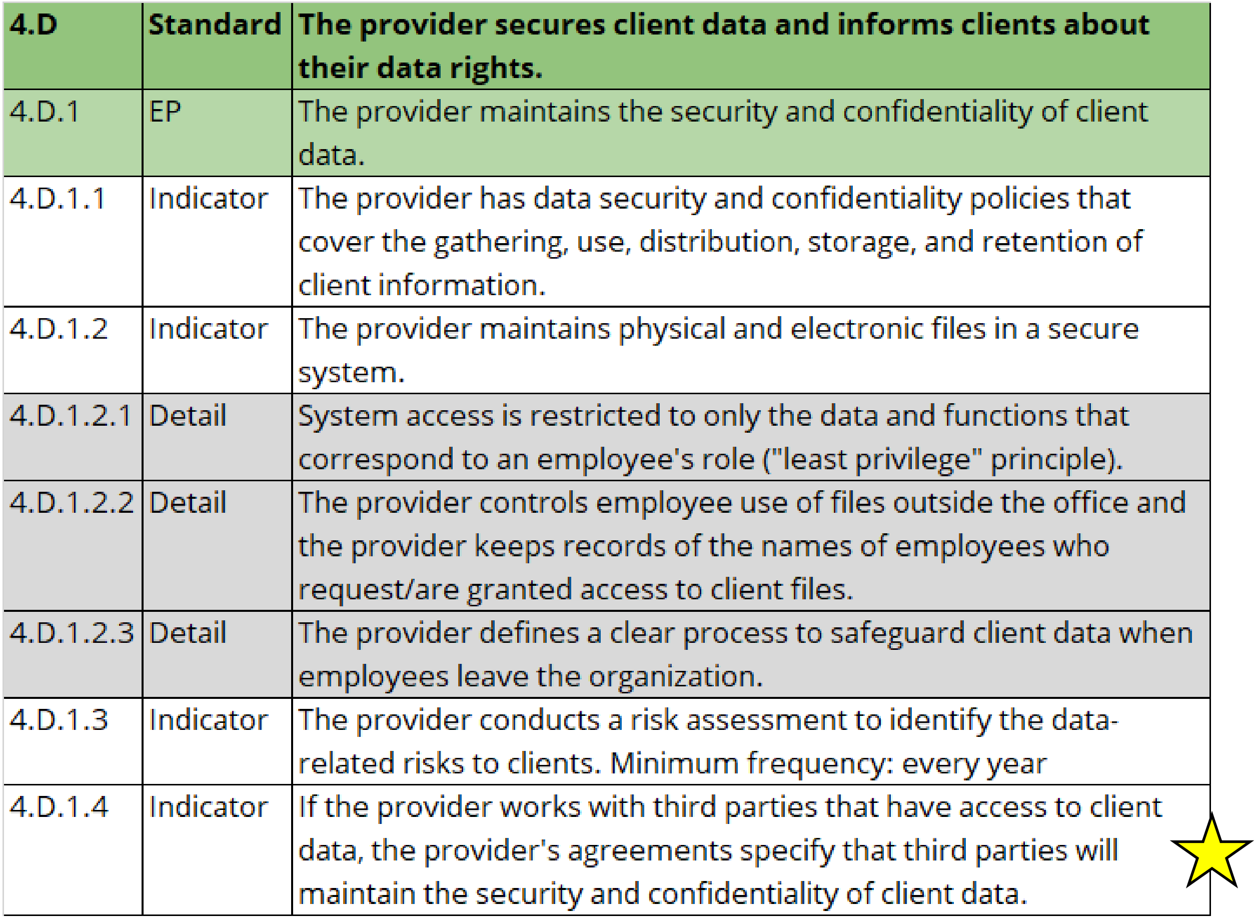
- "We are at the stage where what is involved is not only the protection of data of a single consumer in an institution or 10,000 consumers, but what is possible thanks to the skills of the hackers and the tools they have is they can really stop an institution almost any day." – DFS expert B

What is already in the Universal Standards for SEPM related to cybersecurity (1 of 2)



2.A.3	EP	The board makes strategic decisions based on social and financial data.
2.A.3.1	Indicator	The board uses the following data, provided by management, to monitor client protection. Minimum frequency: annually
2.A.3.1.4	Detail	Reports on the provider's systems for data privacy and security, particularly any failures or breeches.

What is already in the Universal Standards for SEPM related to cybersecurity (2 of 2)



4.D	Standard	The provider secures client data and informs clients about their data rights.
4.D.1	EP	The provider maintains the security and confidentiality of client data.
4.D.1.1	Indicator	The provider has data security and confidentiality policies that cover the gathering, use, distribution, storage, and retention of client information.
4.D.1.2	Indicator	The provider maintains physical and electronic files in a secure system.
4.D.1.2.1	Detail	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	Detail	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	Detail	The provider defines a clear process to safeguard client data when employees leave the organization.
4.D.1.3	Indicator	The provider conducts a risk assessment to identify the data-related risks to clients. Minimum frequency: every year
4.D.1.4	Indicator	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. ★

★ = text incorporates the idea of third-party providers

Cybersecurity: ideas for management practices so far (1 of 3)

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.

Cybersecurity: ideas for management practices so far (2 of 3)

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?)

Cybersecurity: ideas for management practices so far (3 of 3)

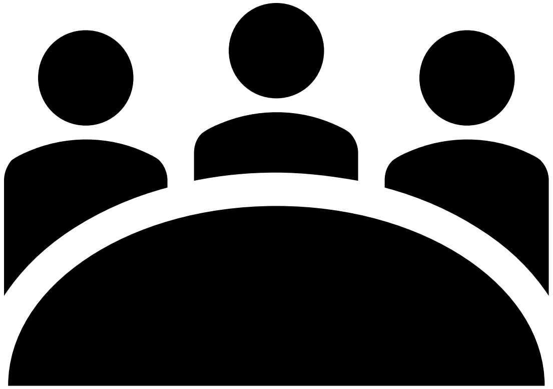
19. Notify customers within X time (24 hours?) if you do get hacked
20. If customers lose money because your systems got hacked, refund the customer.
21. At least once every [X frequency] (month? quarter?), try to hack your own data.
22. If someone tries to hack you, notify other FSPs in the same market, 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
- Monitor employees’ use of computer systems and audit their activities (e.g., who logged in, for how long, and what did they do?)

What do you think? Expert commenters will start off the discussion.

- Africa Cybersecurity Resource Centre (ACRC)
  - Jean Louis Perrier
- MicroSave Consulting (MSC)
  - Anup Singh
    - Update: regrettably unable to attend



- “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

- “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

What is already in the Universal Standards for SEPM related to fraud? (1 of 2)

2.A.3	EP	The board makes strategic decisions based on social and financial data.
2.A.3.1.5	Detail	Reports on any fraud or corruption, including extorsion and bribery.

2.B.2	EP	Management makes strategic and operational decisions based on social and financial data.
2.B.2.1	Indicator	Senior management analyzes the following data and assesses risks. Minimum frequency: annually
2.B.2.1.1	Detail	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	Indicator	Internal audit and/or risk management integrates the following criteria into regular monitoring activities:
2.B.2.2.3	Detail	Compliance with code of conduct; prevention of fraud and corruption
2.B.2.2.5	Detail	Client data misuse and fraud

What is already in the Universal Standards for SEPM related to fraud (2 of 2)

5.C.2	EP	The provider trains all employees on its social goals and on client protection.
5.C.2.2	Indicator	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	Detail	Confidentiality and data sharing policies and fraud risks, including common frauds, fraud identification, and fraud reporting
5.C.3	EP	The provider evaluates and incentivizes employees based on social and financial criteria.
5.C.3.2	Indicator	The provider reviews incentive schemes to check for negative consequences such as fraud, customer mistreatment, agressive sales, over-indebtedness, or high employee turnover.

Fraud prevention: ideas for management practices so far (1 of 3)

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.

Fraud prevention: ideas for management practices so far (2 of 3)

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.]*

Fraud prevention: ideas for management practices so far (3 of 3)

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.

DISCUSS AND DEBATE

What do you think?

MARK YOUR CALENDARS

Responsible Pricing and Transparency
May 31, 10 a.m. - 11:30 a.m. EDT

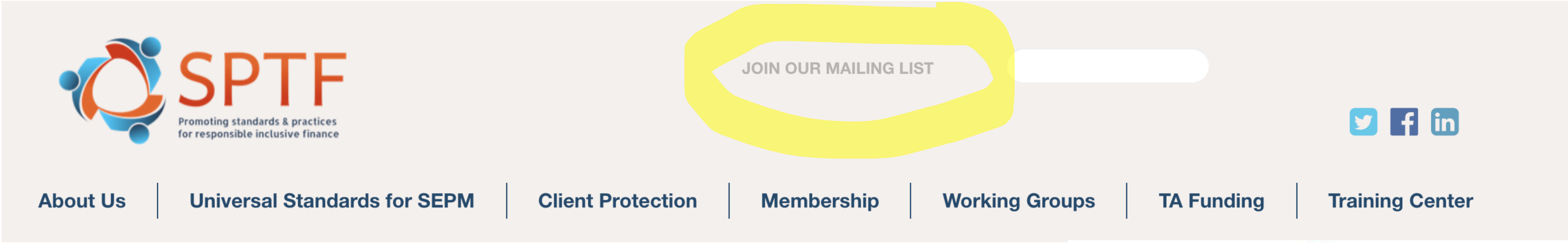
Data Rights & Privacy and Partnerships
June 8, 10 a.m. - 11:30 a.m. EDT

For further information, contact **ameliagreenberg@sptfnetwork.org**

Concluding Announcements

Stay connected!

Would you like to receive the notifications of upcoming events, tools and resources? Sign up for our newsletter at



SPTF

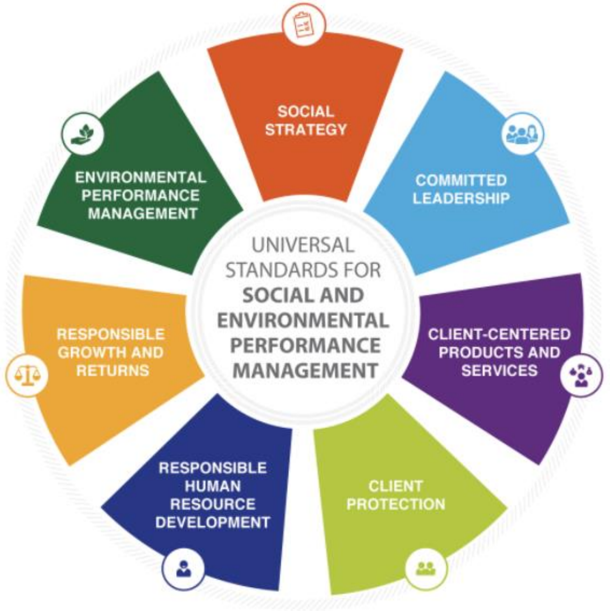
Promoting standards & practices for responsible inclusive finance

JOIN OUR MAILING LIST

About Us | Universal Standards for SEPM | Client Protection | Membership | Working Groups | TA Funding | Training Center

New Universal Standards released in February 2022!

Download the newest standards: https://sptf.info/universal-standards-for-spm/universal-standards


UNIVERSAL STANDARDS FOR SOCIAL AND ENVIRONMENTAL PERFORMANCE MANAGEMENT
SOCIAL STRATEGY
COMMITTED LEADERSHIP
CLIENT-CENTERED PRODUCTS AND SERVICES
CLIENT PROTECTION
RESPONSIBLE HUMAN RESOURCE DEVELOPMENT
RESPONSIBLE GROWTH AND RETURNS
ENVIRONMENTAL PERFORMANCE MANAGEMENT

Thank you!

cerise + SPTF

AFD