STANDARDS FOR RESPONSIBLE DIGITAL FINANCIAL SERVICES: FRAUD PREVENTION STANDARDS SECTION

20 May 2022

CERISE + SPTF
Draft Standards: Fraud
(as of 20 May 2022)

Standards for Fraud Prevention

1. Create a strategy to mitigate fraud risk and address fraud if/when it does occur:
    i. Quantify how much instance of fraud, as a percent of overall portfolio, the FSP will tolerate.
    ii. 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.
    iii. Identify what investments in hardware, software, data analytics, and/or capacity building are necessary.
    iv. Define the systems you will put in place to mitigate fraud risk.
    v. 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.

Guidance on fraud: concepts, examples of real practice, and questions to address

Concepts

- Different types of fraud are more likely at different stages of the product. Example: fake registrations in new deployments / launch of a product, then fraud related to agents earning transaction fees per transaction once customers have been acquired. After several years, customers typically want to do more, like pay utility bills, pay merchants, receive

salaries, and the FSP has to take on new systems/partners to make that happen, which opens up new avenues for fraud.

- Fraud prevention requires investment of many types: capital investment, infrastructure, platform development, human resources and capacity building to respond to fraud.
- Examples of channels to use to communicate with customers about fraud are radio and SMS.
- MSC lists the key segment of stakeholders who perpetrate fraud:
  - Consumer-driven fraud
  - Agent-driven fraud
  - Business-partner fraud
  - System-administration fraud
  - Fraud related to mobile-financial services
- Train women customers especially carefully on how to protect themselves from fraud, as they tend to be more of a target.
- Currently, a common kind of fraud is fraudulent fees. Training should therefore be very detailed and clear about what kids of fees are legitimate and what are not.
- Regarding training employees to avoid fraud, MSC writes "The rewards and consequences of noncompliance must be defined and communicated to all agents in advance."
- Suggested elements of a fraud response strategy:
  - Flag the issue – notify the internal fraud monitoring team
  - Notify customer immediately
  - Freeze account
  - Ask the customer to come to a physical branch to verify credentials and reset pin
  - Inform law enforcement
  - Inform regulator
- Suggested elements for a strategy to avoid fraudulent fees charged by agents:
  - Improve monitoring and enforcement of fee structures;
  - Revise incentive and commission structures where they may lead to extra charges and fees.
  - Increase consumer awareness of official fees and encourage customers to resist paying extra charges
  - Change which agents you use
  - Note that proximity appears a strong driver of customers' choice of agents.
- Suggested practices to implement to help customers who were victims of fraud:
  - At minimum, this involves giving customers the information about how to contact the correct authorities to report the fraud.
  - Reschedule loans for customers who were victims of fraud.
  - On a case-by-case basis, the FSP can also consider helping the customer financially if s/he lost money.
  - One FSP suggested a principle of not refunding a customer if she engaged in behaviors you informed her not to do, like sharing her PIN, but thinks the FSP should help customers financially who have been a victim of fraud that was sophisticated, where it was unreasonable to expect the customer to avoid it.
    - Helping customers who were victims of fraud is aligned with the GSMA principles. Specifically, 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."

- Independent audits can be a useful tool to mitigate fraud risk.
- Consider having a board committee devoted to fraud oversight.

Outstanding questions:

- Fraud prevention measures can be costly. Is there a way for FSPs in a country or a region to pool resources to implement a collaborative strategy to reduce fraud risk and address fraud when it does occur?
- Fintechs are tending toward prioritizing have the minimum number of interactions with customers as possible. But this can inadvertently make fraud easier. For example, if the fintech uses only one way to verify customer identity instead of verifying it through multiple channels, it may be easier to commit fraud around customer identity. So what is the right balance in terms of economical data collection but also a system of checks and balances?
- In some countries, law enforcement does not have a strong understanding or capacity to respond to perpetrators of fraud. In these cases, should the FSP take the time to report to law enforcement anyway, and is there a way for FSPs to improve that situation in their country? Jean-Louis PERRIER advises, "From my experience regarding fraud, you would greatly benefit from coordination with your peers in the market and train together the law enforcement, as most of the time they don't understand well financial frauds."