CDC Investment works

Social Performance TASK FORCE

CDC-SPTF FINTECH WEBINAR SERIES FOR INVESTORS

Brief 3. FinTech Investments: Evaluating Risks with Agent Network Management

Many investors want to better understand opportunities in the FinTech space but do not have a roadmap for how to evaluate such investments for their risks and benefits to clients. Industry-wide standards exist for evaluating the consumer protection and social performance management (SPM) practices of traditional financial service providers and can be a starting point for FinTech providers as standards and guidelines are being adapted. In the meantime, investors are seeking answers to the questions: *During due diligence and monitoring of FinTech investments, how do we evaluate client protection risks? How do we assess the value for the end consumer?*

SPTF and CDC Group have designed a webinar series for investors to help answer these critical questions. SPTF is coordinating with experts including the Smart Campaign, MicroSave, and others to develop content for the series.

This brief presents key lessons from the third webinar. During the webinar, Venkat Attaluri of MicroSave discussed the risks associated with agent network management, as well as the questions investors can ask about this risk during due diligence and monitoring of FinTech investments. Future webinars will delve into other topics, such as "pay as you go" models and data privacy, and what they mean for due diligence and ongoing monitoring.

Listen to the full recording here. Click here for additional details regarding agent network risk. To sign up for the webinar mailing list, contact Katie Hoffmann.

Venkat Attaluri started the call by outlining the importance of agents to digital financial services:

1. **Lower Costs** - Agents provide affordable transactions, and they reduce travel and opportunity costs for clients.
2. **Greater Access** - Agents supply local, convenient access to financial services to clients.
3. **Extended Reach** - Agents provide transactions far from traditional bank infrastructure.
4. **Proven Methodology** - Agents provide transactions through a proven and trusted process.

He outlined two common business models that digital financial service (DFS) providers use that rely on agents:

- **Model I**. DFS providers contract a master agent to build and manage an agent network. These master agents are usually distributors or wholesalers who have existing relationships with retailers in the immediate area. Master agents identify, train, monitor, and provide liquidity and management support for agents. This model often features a super-agent who provides rebalancing of an electronic float (e-float) or cash for the network. *This model allows DFS providers to rapidly expand their networks and limit their responsibilities, but it leaves the provider with less control over the agent network.*
- **Model II.** FinTechs, banks, or mobile money providers build and manage their agent networks themselves. There are no master agents, but super agents continue to provide liquidity support for the agent network. *This model permits providers to maintain better control over the agent network, but the process of constructing an agent network from scratch is more expensive.*

Part 1: What are the risks associated with Agent Networks?

Venkat noted that in recent years, the industry has seen considerable growth in the number of active agents and the average values processed by agents. While that growth brings new opportunities, it also introduces new risk to clients and financial service providers. "Agent networks have become the bedrock of successful mobile money and digital financial service enterprises," he said. "But risks remain." Such risks include:

- **Regulatory risks.**
    - **KYC penalties**. Providers can face stiff penalties if agents fail to adhere to Know Your Customer (KYC) regulations. For example, the Nigerian regulator has imposed a $1,000 per customer fine for not abiding by KYC laws, and regulation in Uganda has required MNOs to reregister all customers with proper KYC. Following such regulations can be particularly difficult in countries without a national identification system.
    - **Overcharging customers.** In most countries, regulation requires agents to display charges. Some agents overcharge customers by collecting additional charges in cash, which is illegal.
    - **Over-the-counter (OTC) transactions.** OTC transactions are those that an agent conducts on behalf of the sender or recipient from either the senders' or agents' mobile money account. Such transactions decrease providers' profitability and can lead to more unregistered transactions, which increases the risk of terrorism financing or money laundering.
    - **Anti-money laundering/Combating the Financing of Terrorism (AML/CFT).** If agents are not trained on the potential signs of money laundering or terrorism financing, it exposes the provider to violating laws related to these issues.

- **Technology risks.**
    - **Server downtime.** When servers are down, agents can't perform transactions, which adversely affects client retention and contributes to reputational risk. Server

  downtime can also lead to agent fraud. For example, during a technical glitch at a mobile money provider, an agent withdrew $100,000 over a period of 45 days. By the time the provider discovered it, the agent had already spent about $20,000.
  - **Device failure**. If providers take a long time to repair or replace agents' devices, they may lose business.
  - **Transaction errors.** Such errors and slow processing times are common, and stem from poor connectivity. This can cause providers to lose both customers and agents.

- <u>Agent support risks</u>
  - **Lack of training and support.** MicroSave has found that many providers do not conduct trainings of their agents, even if the policy says they're mandatory. Poorly trained agents are unable to carry out basic services, and lack of proper agent training exposes the provider to fraud. Some have call centers to field agents' questions, but many of the call centers have such long wait times that agents have stopped calling.
  - **Lack of monitoring**. If providers do not routinely monitor their agents, it can also lead to fraud or a decline in the quality of services. Monitoring enhances quality of services and reduces churn of agents and customers.
  - **Lack of branding.** If an agent does not have proper branding materials from the provider, it can be challenging for them to convince customers that they are an authorized agent of a DFS provider.

- <u>Fraud risks</u>
  - **Theft.** Agents are often managing significant amounts of cash, exposing them to theft. In Bangladesh, thieves stole $16,000 and shot agents.
  - **Fraud by agents or customers.** This includes agents' providing unauthorized access to customers' PINs, illegal charges on customers' accounts, offering illegal services, or registering non-existent customers. For example:
    - In Kenya, an agent had 800 debit cards of his customers; he provided loans to them, and he would withdraw his installment from the debit cards monthly.
    - In other cases, agents would charge clients an extra fee if their transaction would deplete their physical or e-float. Clients are willing to pay because they're not aware that fee is illegal.
  - **Counterfeit money.** In several instances, clients have given agents counterfeit money. As a result, agents could lose money or pass along counterfeit money to other clients.

- <u>Liquidity risks</u>
  - **Costs of rebalancing.** Agents often must travel far to rebalance their floats. This can cause agent churn, or lack of sufficient cash.
  - **Lack of sufficient cash.** And, if they don't have sufficient e-float or physical cash, they can't service all customers. This leads to a negative customer experience.

- **Financial risks**
    - **Lack of customer base**. When agents kickstart operations, they often don't have an initial customer base, and there is a high rate of agent dropout in the beginning. It can be costly to build a customer following.
    - **Split transactions.** These transactions take place when agents split cash deposits by customers to make additional revenue in a tiered commission or revenue shared model. Customers end up paying more to withdraw cash, and the provider loses money if they're depositing cash.
    - **Manipulation of account activations**. Agents can fake mobile money accounts or wallets to earn more commissions.

- **Privacy risks**
    - **Data protection/confidentiality.** Agents have access to customers' account information, and they can disclose this to people who could use it for personal gain. In some places, the agent owns the PIN. This is particularly prevalent in nascent markets, as customers do not know the importance of the PIN.

Part II: How can investors mitigate the risks associated with agent networks?

If these agent-related risks are not managed, it can negatively affect the uptake of services, the pricing of services, the customer experience, and the providers' reputation. Venkat outlined several strategies that investors can take to help their FinTech investees better mitigate the risks related to agents. Investors should make sure their investees:

- **Enforce KYC polices.** Providers should have a policy in place for all agents to verify identification of customers. They should use biometric devices, when possible.
- **Provide regular, mandatory training to agents**. Such training should:
    - Define what it means to have good agent behavior. This definition should draw from examples of other successful agents in the region.
    - Ensure agents know how to identify valid KYC ID and verify it with government database, when available.
    - Train agents on suspicious behavior related to money laundering/anti-terrorism. Such behavior includes clients who operate multiple accounts directly or through proxies; frequent withdrawals with no apparent business source; multiple accounts with many deposits to avoid currency transaction report; high volume of activity and low balances; and unexplained increases in account activity.
    - Train agents to recognize counterfeit money.
- **Provide support to agents.** Providers should:
    - Measure satisfaction among agents.
    - Have a call center for agents' grievance redressal or service questions. The call center should be adequately staffed to ensure minimum wait times and to respond to agents' inquiries in a timely manner.
    - Provide agents with proper branding materials.

  - Recognize high-performing agents with monetary and non-monetary (such as "agent of the month") rewards.
  - Provide police protection to agents on days when they are expected to have an influx of cash, such as paydays.
  - Work to minimize rebalancing costs or liquidity risks for agents. For example,
    - One provider has started agency banking, in which a mobile man visits different trading centers, so agents can rebalance float.
    - Providers can partner with other banks to increase access points for agents.
    - Providers can offer loans or overdrafts to agents to assist with liquidity.
    - In the Philippines, a provider offers an advance to agents during peak periods. When the period is over, the money is pulled from their wallets.
  - Provide regular feedback from clients to the agents. If complaints need resolution, work with the agent to address them.
- **Monitor agents.** Providers should:
  - Conduct quarterly "mystery shopping" with agents to make sure they are compliant with all policies.
  - Talk to a sample of agents' clients, including those who are active, those who are not active, and those who have recently left the provider.
  - Partner with the government or other providers to monitor agents. For example, the Bank of Ghana is hosting a centralized database to curb fraud. All agents get a unique ID, and the list is accessible by all providers whenever they need it. If an agent commits fraud, the provider reports it to the Bank.
- **Educate consumers.** Such education should help clients better understand:
  - The importance of privacy related to PINs.
  - Illegal charges or services
  - To check tariff sheets and agent IDs.
  - To identify proper branding of the providers' agents.
- **Use data analytics.** Data analytics can help providers combat many of these risks.
  - Providers in different countries are using data to track suspicious behavior related to money laundering or terrorism financing. Regulators in Malawi, Uganda, and Zambia collect a monthly report from providers on these types of transactions and instruct providers on course of action.
  - Data analytics also can help providers more precisely e-float. Analytics can help make sure agents have enough e-float on days they need it, while also making sure they do not have so much cash that it exposes agents to theft.
- **Have a strong maintenance contract with technology provider**. Providers should have a strong service agreement with technology provider, including penalties for delays.

For a longer list of due diligence questions related to agent networks and other topics, see Annex I.

ANNEX I: Due diligence questions for DFS Provider Agent Networks

Business model

1. Is the business model clearly defined? Are stakeholders (agents, super agents and master agents) roles and responsibilities clearly defined as part of channel strategy?

Regulatory

1. How is the institution monitoring agents for KYC and AML/CFT?
2. What is the strategy to combat OTC/Agent Assisted Transactions?

Technology

1. What is the average server downtime (frequency and severity)?
2. What is the service level agreement for network uptime and device maintenance?

Agent Support

1. What is the frequency and the agenda for trainings - onboarding, refresher, new product/ service, etc.?
2. How many transactions failed in the last 12 months? What were the reasons for the failures?
3. What is the frequency of monitoring visits and focus areas? Is there a report submitted after the monitoring visit with action points? How does the monitoring visit report move within the institution?
4. Is there any mystery shopping activity undertaken to understand agents' knowledge and agents/ customers challenges?

Fraud

1. What are the trends in fraud by agents/ customers? Is there an education program for agents about customer fraud, and a program for customers regarding agent fraud?
2. What are the proactive and reactive controls for fraud?
3. How is fraud liability managed between the provider, agent and customers?

Liquidity Management

1. How is the liquidity management monitored from headquarters? Is there an automatic alert for agents who approach the minimum threshold for liquidity?
2. What is the average float maintained by agents? Divide by urban and rural areas.
3. What are the different options available for rebalancing?
4. Is it only as banks who are acting as super agents or other actors?

Reputational

1. Are the roles and responsibilities among the provider and other partners clearly defined?

Financial

1. What is the average commission earned by agents in urban, semi-urban, and rural areas?

Privacy

1. Has the DFS provider taken steps to ensure the protection of customers' personal data?

ANNEX II: Related reading

Helix Institute, Fitting the Pieces of the Liquidity Management Puzzle.

Helix Institute, Benchmarking Training and Support: By Agent Network Management Model.

International Telecommunications Union, ITU Focus Group Digital Financial Services: Main Recommendations.

MicroSave, Measuring Risk in Agent Networks: What risks are inherent in agency business and how to track them.