

Fraud in Mobile Financial Services: Protecting Consumers, Providers, and the System

The rapid growth of mobile financial services (MFS) is arguably the single most significant contributor to increased financial inclusion in emerging markets today. It has facilitated access to cheap and reliable financial services to an ever increasing formerly unbanked population segment. Innovative mobile money services like M-Pesa in Kenya and Tanzania have grown into major payments services that move billions of dollars annually. Unfortunately, MFS have also rapidly become a conduit for fraud and other criminal activity.

Various fraud types have been noted in key MFS markets, including consumer-facing fraud from agents and third parties, and fraud perpetrated against agents. Additionally, incidences of internal fraud have created significant economic loss for providers and affected a considerable number of mobile money users in these markets.

Consumer- and agent-reported fraud levels are relatively high in some of these markets—resulting in losses for consumers, agents, and financial services providers (FSPs)—and by contrast, fairly low in other markets. This indicates that although fraud can be a primary concern, it is also a risk that can be effectively mitigated.¹ The fear or actual experience of losses from fraud may play a role in limiting low-income consumers' MFS uptake and continued use. These concerns may also contribute to the limited demand for additional nonpayment products that consumers perceive as both more complex and risky.

Failure to rein in internal and external fraud can reduce perceived consumer benefit and financial inclusion gains in these markets, and impact FSPs' business case. Furthermore, regulators may be less inclined to allow the needed space for innovations to expand and diversify MFS, to the extent they view providers' internal controls as inadequate to detect and mitigate fraud. Providers, therefore, need to implement controls that strike an appropriate balance between risk management and other business objectives.²

In 2015, CGAP undertook a comprehensive research study on fraud in six leading MFS markets: Ghana, Kenya, Pakistan, Rwanda, Tanzania, and Uganda. This research included analyses of consumer-reported fraud issues from Intermedia Financial Inclusion Insight (FII) Survey interviews with industry fraud and risk management experts; engagement with policy makers on key risks and relevant policy responses; mapping of good practices for fraud detection and mitigation; and workshops and trainings with industry and government, some organized jointly with GSMA (the global mobile

industry association). This Brief describes key findings and recommendations from this research and identifies several key vulnerabilities and strategies for FSPs and policy makers to combat fraud risks and minimize harm to consumers, agents, and FSPs' businesses.

MFS Fraud Risk Factors and Vulnerabilities

Before effective solutions can be implemented, the risk factors that make mobile money vulnerable to fraud and money laundering activity, and the various accompanying fraud typologies, should be analyzed.³

Key mobile money risk factors and corresponding indicators include the following:

- **Product Risk.** While the speed, portability, and security of mobile money make it a preferred service in emerging markets, the same qualities make it a preferred channel for more and rapidly executed frauds and scams. The emergence of new MFS, including bulk payments, insurance, mobile savings and credit, prepaid cards, and cross-border and international money transfer services, can create opportunities for fraud.
- **Channel Risk.** This risk arises from the ubiquity of mobile phones and the extent to which new and less experienced consumers are entering the market through this channel.
- **Agent Risk.** Providers with large agent networks find it challenging to build adequate infrastructure and systems for effective agent oversight and monitoring of compliance violations, especially in remote areas.
- **Customer and Compliance Risk.** Countries with large numbers of unbanked, illiterate, and/or rural populations that lack national identification regimes find it difficult to ensure know your customer (KYC) due diligence and to track criminal activity, especially given that frontline KYC checks often rely on agents rather than branch staff.

¹ Intermedia Financial Inclusion Insight (FII) Surveys (<http://inclusion.org/>) ask several questions related to fraud perpetrated on consumers by agents, with levels of incidence varying across markets, demonstrating how fraud risks may play out differently in individual MFS markets. For example, 2014 survey respondents reported being overcharged by an agent or asked to pay for a deposit at high levels in Uganda (11%), low levels in neighboring Rwanda (1%) and Pakistan (0%), and moderate levels in Tanzania (5%). Additionally, data from FII surveys indicate a higher prevalence of agent-to-consumer fraud in Uganda and Tanzania at an average incidence of 5 percent, than in Kenya, where the average incidence for agent-to-consumer fraud was considerably lower at 2 percent. See also Figure 1.

² Also see Mudiri (n.d.).

³ Since fraud is a predicate offense for money laundering, a discussion of fraud risks and controls goes hand in hand with the prevention of money laundering and related criminal activity.

- **System and Delivery Risk.** System down times delay service delivery and can create opportunities for fraud. Inadequate system and access controls may also facilitate abuse of access rights and give rise to fraud. Lack of automated fraud management systems impede comprehensive transaction monitoring and sanctions screening to detect fraud and terrorist activity.
- **Regulatory, Supervision, and Enforcement Risk.** Some markets also have inadequate regulatory regimes for mobile money, which can lead to the proliferation of unlicensed money transfer agencies or unregulated money transfer products, which in turn can facilitate fraud, money laundering, and other criminal activity.

Emerging Fraud Trends and Typologies

The specific characteristics and risk factors highlighted above make fraud typologies prevalent in MFS distinct from those in traditional face-to-face banking. Broadly, the categories comprise fraud types that impact consumers, agents, and providers.

Consumer-Affecting Fraud

Consumer-affecting fraud types vary from one market to the next. For example, MFS providers in Rwanda and Uganda indicated that the top consumer-facing fraud concerns were as follows:

- Identity theft arising from fraudulent/offline SIM swaps that transfer the mobile wallet account from the customer's SIM to the fraudster's SIM, enabling the fraudster to gain access to the consumer's mobile wallet and bank account.
- False promotions, phishing, or social engineering scams, such as fraudsters impersonating providers and advising customers they won a prize in a promotion and to send money to the fraudster's number to claim the prize.
- Network down time, which can create opportunities for fraud, mainly through offline SIM swaps and over-the-counter (OTC) transactions that can be verified and reconciled only later when the network connection is restored.⁴
- Agents who ask for the customer's personal identification number (PIN). (Even where this may not necessarily have been done to defraud customers, it makes consumers more vulnerable to fraud risks.)
- Agents who defraud customers primarily through OTC transactions, e.g., overcharging for transactions, such as direct deposits or charging for normal deposits, which are typically free.⁵
- Provider impersonation by fraudsters who call consumers purporting to represent the provider and may then induce them to reveal their PIN or other personal information about their mobile money accounts, which can be used to defraud the customer.
- Loss from erroneous transfers to unintended recipients who refuse to refund the money.

FII Surveys indicate that the most common fraud concern is agents asking for PINs (though this may not necessarily have been done to defraud the customer), followed by cases of agents overcharging for transactions, such as direct deposits (direct deposits are illegal in a number of countries), or charging for normal deposits, which are typically free.⁶ Interestingly, the network being down was the most prevalent concern and had an average incidence level of 50 percent of customers sampled.

Despite the relatively high prevalence of consumer-impacting fraud or other problems, on average only 11 percent of MFS customers who experienced difficulties with mobile money reported them via formal complaints channels, such as customer care centers.⁷ This was mainly because of ineffective provider recourse channels or lack of information about where to file complaints. In some cases, OTC customers may be less likely to use formal complaint channels than wallet-based customers (Mazer and Garg 2015). This creates a significant challenge for FSPs to ensure they have full visibility on fraud levels within their network and take action to punish and prevent those who perpetrate fraud on customers.

Agent-Affecting Fraud

Agents and MFS providers are also vulnerable to fraud. Helix Institute of Digital Finance's Agent Network Accelerator Surveys found that 53 percent and 42 percent of mobile money agents in Uganda and Tanzania, respectively, had experienced fraud in the past year (Khan and Bersudskaya 2016). Fraud and crime rates recorded by Ugandan mobile money agents were the highest in the region (Bersudskaya and Kuijpers 2016). Common frauds affecting agents mainly involve float loss in the agent's account arising from unauthorized use, compromising of PINs, and scams involving impersonation of MNO staff by fraudsters who gain unauthorized access to the agent's float account. Customers can also commit fraud against agents—for example, withdrawal reversal fraud or fake currency deposits.⁸ The Helix Institute's 2015 surveys indicate that fraud is a primary concern for many agents. This is particularly true in East African markets, as noted in Figure 1.

Internal Fraud in Mobile Money Providers

Fraud within providers is also a concern. Several high-profile instances of internal fraud have resulted in significant losses for MFS providers, while putting users' accounts at risk and raising financial integrity concerns for the system. For example, MTN, the largest mobile money provider in Uganda, lost an estimated US\$3.4 million through internal fraud perpetrated by staff in 2011 (Morawczynski 2015), while a similar incident cost Tigo in Rwanda an estimated US\$700,000 in 2014 (Mugisha 2014). Inadequate internal controls (facilitating internal data hacking), inadequate audit processes, poor corporate governance structures, lack of employee fraud education, and lack of whistle blowing mechanisms are among the key contributors to internal fraud.

⁴ OTC transactions involve agents taking cash from a customer and transacting directly instead of loading the cash onto the customer's mobile wallet.

⁵ Direct deposits are OTC transactions where the agent deposits directly into a third-party wallet, normally on the customer's instructions.

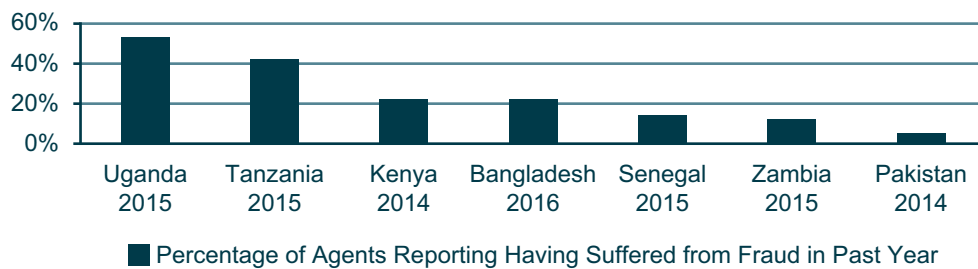
Direct deposits are illegal in several countries because they violate customer verification guidelines and can facilitate money laundering.

⁶ FII Surveys (2014) Uganda, Kenya, Tanzania, Rwanda, and Ghana (<http://finclusion.org/>).

⁷ CGAP qualitative consumer research conducted in Bangladesh, Colombia, and Uganda, as discussed in McKee, Kaffenberger, and Zimmerman (2015).

⁸ Withdrawal reversal frauds occur when the customer asks the provider to execute an immediate reversal of a completed withdrawal on grounds that the customer did not receive the funds from the agent.

Figure 1. Agents Reporting Having Suffered from Fraud in Past Year



Source: Bersudskaya and Kuijpers 2016.

Mitigatory Controls for MFS Fraud⁹

Provider Action

Providers can take specific steps to minimize the likelihood and monitor the occurrence of some of the more common types of fraud and to deal with their consequences.¹⁰ These include the following:

- Comprehensive fraud management programs, including cost-effective automated transaction monitoring and sanctions screening systems to facilitate early detection and prevention of fraud and other suspicious activity, including terrorist activity.
- Compliance monitoring and agent recruitment, training, and management programs may need to be strengthened to ensure top-to-bottom compliance with established procedures and to reduce internal and external fraud risk.
- Product risk assessments that are incorporated into every MFS risk management program to ensure all risks are identified and adequately mitigated with appropriate controls (e.g., KYC requirements, consumer sensitization, systemic safeguards) before the launch of new MFS products that can create new risks. Risks typically involve identity theft and phishing scams that facilitate loan impersonation and similar fraud.
- Comprehensive fraud awareness and prevention programs that providers offer to sensitize consumers, staff, and agents on fraud trends and prevention measures. These can include training, media campaigns, and periodic bulletins sent as email or text, systemic safeguards to prevent the compromising of PINs, and liaison with law enforcement agencies in the investigation and prosecution of frauds.
- Continuous sensitization of consumers on the new types of fraud and scams appearing in the market. Emphasis should be on ways consumers can protect themselves, such as keeping their PINs secure and checking their balances before sending back money purportedly sent to them in error.
- Comprehensive agent fraud prevention measures that include training, compliance monitoring, sensitization programs, and systemic safeguards restricting the use of the till.
- Provision of effective complaints recourse channels with trained staff conversant in handling fraud and

other complaints and dedicated recourse channels for agents. Effective recourse helps to reassure users of new financial services that their money is protected, and that they will be able to resolve the issue if they encounter a problem (Mazer and Garg 2016).

- Effective staff recruitment processes that include vetting of staff.
- Inculcation of a compliance culture, continuous staff training, and implementation of disciplinary measures.
- Implementation of technical controls that restrict user access rights and implement dual controls.

In addition to managing fraud within their own networks, MFS providers need to engage in coordinated industry action aimed at curbing fraud. Fraudsters often employ similar tactics across mobile money networks, and consumers similarly exhibit common vulnerabilities irrespective of the provider they choose (and in many markets consumers commonly use multiple mobile money providers). Market-level industry associations, for example, could monitor trends and promote the mutual sharing of information on fraud trends and prudent fraud management best practices.¹¹ This has worked well in most African countries where there are strong bankers associations and in countries like Uganda and Zimbabwe that have mobile money agent associations. However, not all countries have mobile money agent associations, and where MFS are offered through banks, the banks may not prioritize MFS issues.

Regulatory Oversight

The absence of appropriate regulatory regimes and supervisory oversight can create opportunities for fraud. The lack of enabling regulation can also stifle innovation, meaning providers will not be in a position to roll out new products without appropriate regulatory frameworks. These regulatory gaps are further exacerbated by poorly trained and equipped law enforcement agencies, leading to delays in investigating and resolving fraud cases.

Regulators in these markets should implement appropriate regulatory reforms, including the following:

- Appropriate legislation that make mitigatory controls mandatory and ensure due implementation of the same by providers. The recent introduction of mobile money

⁹ Providers in the countries surveyed have implemented these controls with good results. For example, in Kenya, the Hakikisha (Verification) Functionality on M-Pesa has significantly reduced incidences of erroneous transfers. In Tanzania, quarantine periods for accessing a mobile money account after a SIM swap have reduced the number of incidences of SIM swap fraud. Agent-impacting frauds have been controlled in East African markets by putting restrictions on agent tills, such as barring nonprovider incoming calls and SMS texts. Agent training on fraud has enabled the detection and prevention of social engineering scams in Cambodia.

¹⁰ Also see Buku (2012).

¹¹ Findings from CGAP research in Ghana, Kenya, Rwanda, Tanzania, and Uganda.

and electronic money regulations in several leading mobile money markets, such as East and West Africa and South Asia, has helped to formalize the sector and provide regulators with tools to implement and oversee stronger fraud monitoring and risk mitigation measures.¹²

- Continued engagement with regulators by consumer interest groups and financial inclusion agencies, to provide appropriate support toward achieving legislative reforms, where appropriate. This is particularly important in countries where enabling sector-specific regulations are yet to be implemented.
- Regulations that provide a legislative framework for authorizing and overseeing all MFS providers; provide for implementing mandatory consumer protection measures to curb fraud; and minimize other challenges experienced by consumers using MFS, such as inadequate communication and consumer recourse channels and unfair provider practices. A case in point is Ghana, where the Electronic Payments regulations launched in 2015 have clear provisions in this regard (Bank of Ghana 2015, Section 26–28).
- Cross-border coordination on fraud mitigation in regions that have multiple markets with extensive use of mobile money. One example is the East African community's efforts to develop a common SIM card registration framework for the explicit purpose of limiting mobile money fraud (Business Daily 2015).

Conclusion

The mobile money space is constantly evolving. As more players enter the MFS arena and new products are offered, providers will need to work together, and appropriate regulation may need to be introduced. Continued efforts to document and standardize effective fraud and risk management approaches can accelerate development of consistent and effective approaches across all MFS globally.

This Brief has documented how fraud is impacting mobile money providers, agents, and consumers, as well as efforts to reduce risks and vulnerabilities to fraud in mobile money and related services. While it is not possible to remove fraud entirely from any service—mobile money included—the examples addressed here show that fraud is a major issue in several key markets for consumers and agents, and that there are simple steps providers can take to reduce their vulnerability to common fraud types.

These steps include improving internal controls, building agent capacity to protect themselves and their customers, and revisiting procedures such as account access and SIM swaps, where necessary, to prevent common fraud schemes. With the introduction of new products and delivery channels, the types of fraud will continue to evolve, which means that monitoring mechanisms, such as compliance checks and customer feedback channels, will continue to be key elements to effective fraud and risk mitigation. Providers should share successful experiences with their peers, so that all providers can adopt good practices and

take collective action where necessary. There has already been communication among domestic bodies such as mobile money associations. This sharing of best practices and experiences will benefit the provider community.

Governments, donors, and development partners should continue to support FSPs and others, such as law enforcement agencies, with technical assistance (e.g., on infrastructure solutions) and capacity building. While the MFS industry has developed a range of responses to fraud, many policy makers lag behind without sufficient regulations or risk assessment tools for MFS. Going forward, there should be increased policy maker engagement with industry efforts to reduce fraud and, where possible, formalize good practices into standard requirements for MFS providers. Improved trust and use, product diversification, and reduced losses for consumers, agents, and providers are considerable benefits that support MFS, consumer welfare, and provider profitability.

References

- Bank of Ghana. 2015. "Guidelines for E-Money Issuers in Ghana." Bank of Ghana. <https://www.bog.gov.gh/privatecontent/Banking/E-MONEY%20GUIDELINES-29-06-2015-UPDATED5.pdf>
- Bersudskaya, Vera, and Dorieke Kuijpers. 2016. "Agent Network Accelerator Survey: Uganda Country Report 2015." Helix. <http://www.helix-institute.com/data-and-insights/agent-network-accelerator-survey-uganda-country-report-2015>
- Buku, Mercy W. 2012. "Mobile Money: Balancing Financial Integrity with Business Expediency." Blog post, 16 September. <http://www.acamstoday.org/mobile-money/>
- Business Daily. 2015. "EAC Members Move to Tame Mobile Money Fraud." Business Daily, 24 September. <http://www.businessdailyafrica.com/-/539546/2884060/-/12192dtz/-/index.html>
- Khan, Maha, and Vera Bersudskaya. 2016. "Working Together to Fight DFS Fraud." Blog post, 7 November. <http://www.helix-institute.com/blog/working-together-fight-dfs-fraud>
- Mazer, Rafe, and Nitin Garg. 2015. "Recourse in Digital Financial Services: Opportunities for Innovation." Brief. Washington, D.C.: CGAP.
- . 2016. "Improving Recourse Systems in Digital Financial Services." Blog post, 14 March. <http://www.cgap.org/blog/improving-recourse-systems-digital-financial-services>
- McKee, Katharine, Michelle Kaffenberger, and Jamie M. Zimmerman. 2015. "Doing Digital Finance Right: The Case for Stronger Mitigation on Customer Risks." Focus Note 103. Washington, D.C.: CGAP.
- Morawczynski, Olga. 2015. "Fraud in Uganda: How Millions Were Lost to Internal Collusion." Blog post, 11 March. <http://www.cgap.org/blog/fraud-uganda-how-millions-were-lost-internal-collusion>
- Mudiri, Joseck Luminzu. n.d. "Fraud in Mobile Financial Services." Hyderabad: MicroSave. http://www.microsave.net/files/pdf/RP151_Fraud_in_Mobile_Financial_Services_JMudiri.pdf
- Mugisha, Ivan R. 2014. "Two Men Arrested for Allegedly Defrauding Rwf495m from Tigo." Blog post, 20 November. <http://www.newtimes.co.rw/section/article/2014-11-20/183244/>

¹² Kenya, Tanzania, Ghana, Bangladesh, and India have electronic payment legislation in place.

AUTHORS:

Mercy W. Buku and Rafe Mazer

All CGAP publications are available on the CGAP Web site at www.cgap.org.

CGAP
1818 H Street, NW
MSN IS7-700
Washington, DC
20433 USA

Tel: 202-473-9594

Fax: 202-522-3744

Email:
cgap@worldbank.org

© CGAP, 2017