The role of mobile money providers and their agents in protecting customers' data

December 2022

Photo credit: Arshi Aadil

MSC
MicroSave Consulting

CGAP

Disclaimer

This work was funded in whole or in part by CGAP. Unlike CGAP's official publications, it has not been peer reviewed or edited by CGAP, and any conclusions or viewpoints expressed are those of the authors, and they may or may not reflect the views of CGAP staff.

Authors

CGAP

Myra Valenzuela

Eric Duflos

David Medine

Majorie Chalwe-Mulenga

MSC

Akhand Jyoti Tiwari

Arshi Aadil

Surbhi Sood

Thomas Murayi Maina

Acknowledgments

The authors would like to thank Nitin Garg, Praveen Saldanha, and the entire team of FLOW Global for their help and support in conducting field research in Uganda. We also thank Grace Lukwago for her support in moderating the field discussions.

CGAP | MSC

Table of Contents

CGAP | MSC

Executive summary

Executive summary

According to recent CGAP research, consumer risks, particularly data misuse, are growing significantly. These risks erode consumer trust and undermine the delivery of financial services to underserved and low-income segments, especially women. This reading deck summarizes observations and learnings from qualitative research conducted with customers, agents, and mobile money providers in Uganda. It provides insights into mobile money providers and agents' practices to protect customers' data and privacy. The study also highlights the state of data protection in Uganda included in the provisions of the 2019 Data Protection and Privacy Law.

Key takeaways from the field study in Uganda

1. **Mobile money providers have strengthened data protection policies and agent practices since the launch of the Data Protection and Privacy Act of 2019.** However, providers must improve the training and monitoring of agents and agent supervision.

2. **By supporting their agents, providers can bolster their data protection approach.** Responsible practices include training agents on data protection, providing marketing collaterals on PIN management, and offering an agent support number to respond to agent queries with a 72-hours turnaround time. However, structured training on data protection and privacy aspects needs to be incorporated in agent training modules.

3. Most agents follow responsible practices to protect customers' data and play a significant role in increasing customer awareness. Responsible practices include agents advising customers to reset their PINs periodically, installing video cameras at agent locations to deter fraudsters, and communicating through WhatsApp groups to share information on emerging threats related to fraud and data protection breaches and how to safeguard themselves.

4. **Challenges remain for both agents and providers around data protection.** The requirement to enter transaction records in logbooks and frequent network downtime issues puts consumer data at risk. However, providers can better support their agents by offering them a communications toolbox on data protection and supervisory support via in-person visits, especially in rural areas.

CGAP | MSC

1. About this study

CGAP's project on "Protecting Vulnerable Customers"

The project promotes an approach where regulators, supervisors, providers, and market facilitators ensure positive outcomes for customers in their financial journey. With a focus on digital finance, women, and vulnerable groups, it includes three workstreams:

Market Monitoring Toolkit

Tools such as regulatory report analysis, complaint analysis, mystery shopping, and phone surveys enable supervisors, regulators, and other market actors to assess consumer risks. CGAP is testing the toolkit in a WAEMU regional pilot.

Elevating the Collective Consumer Voice

Empowering consumers to share their experience through consumer groups/ associations, regulatory consumer panels, and technology & social media. Pilots include India (social media) and South Africa (consumer panel).

Showcasing Responsible DFS Providers

Identifying and promoting customer-centric DFS providers that adopt business models and distribution channels (e.g., agents) that protect consumers from risks. **This qualitative research study fits within this workstream.**

Cross-cutting research on the evolution of DFS consumer risks feeds into the three work streams.

CGAP | MSC

Research objectives and study approach

Research objectives

- Identify good practices of responsible agents and providers in protecting customer data, focusing on female agents and female customers.
- Identify the factors that enable agents to manage customers' data responsibly.
- Study and compare the alignment of consumer protection standards **(**Data Protection and Privacy Act of 2019 **and** mobile money guidelines **by Bank of Uganda)** adopted by MNO providers and agents in Uganda with **GSMA's mobile money data protection guidelines.**

Study approach

Secondary research

+

Demand-side interviews with customers and agents

+

Supply-side interviews with MNO providers and agent management company

CGAP | MSC

Sampling details

	Qualitative study with customers and agents	Demand-side stakeholders interviewed
Sampling methods adopted	• Snowballing* and purposive sampling** approach to locate our customers and agents for the survey • Conducted supply-side interviews with mobile network providers and representatives of the agent management company	MNO agents: 12 Customers: 70

Districts covered as part of the sample

Districts covered:

- Kampala central region, Mukono district, and Buikwe district

Locations covered:

- Urban: Naguru, Owini Market, Bukoto, Nakasero market area, Jinja, Nakifuma-Mukono, Mbale main market
- Rural: Cheend, Kamwookya, Dangurumeera, Jinja

*Snowball sampling is where research participants recruit other participants for a test or study. It is used where potential participants are hard to find.
**Purposive sampling (also known as judgment, selective or subjective sampling) is a technique in which the researcher relies on their judgment when choosing respondents to participate in the study.

CGAP | MSC

Profile of agents interviewed

Qualitative research (n=12)		
Type of agent outlets	Dedicated: 1	Non-dedicated: 11
Location of agents	Rural: 5	Urban: 7
Gender of agents	Female: 8	Male: 4

Photo credit: Arshi Aadil

Profile of customers interviewed

70
Respondents
Rural: 35, Urban: 25,
Semi-urban: 10

30
The median age of the respondents

40

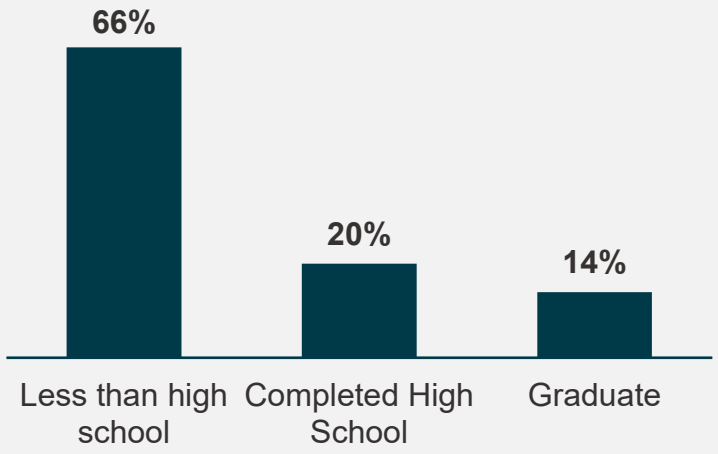
30

31%

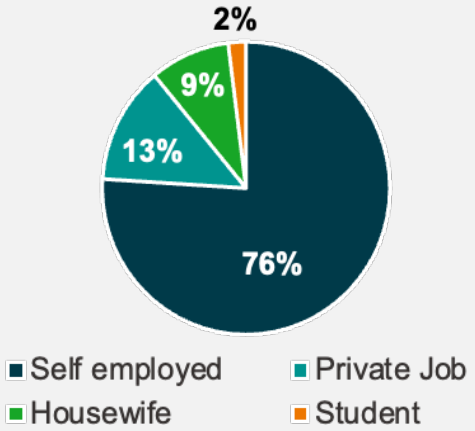
65%

4%

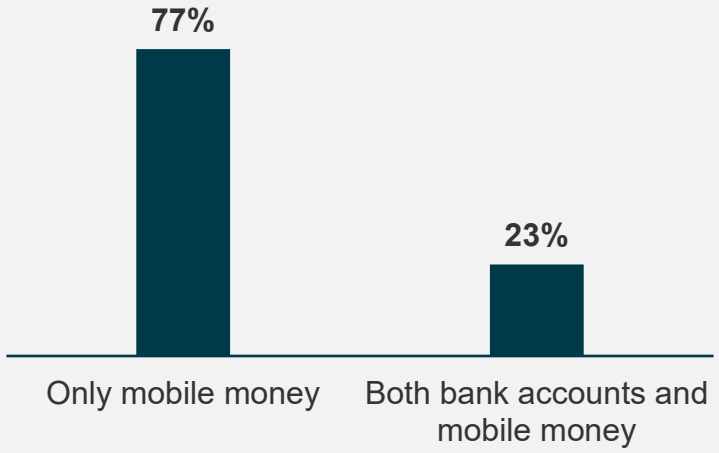
Education of the respondents



Occupation



Financial profile



Qualitative interviews were conducted with men and women belonging to different socio-economic backgrounds.

CGAP | MSC

Tools used

Agents

In-depth Interviews with agents of Airtel, MTN, and Wave Money

Customers:

Focused-discussion groups and in-depth interviews with users of mobile money

Providers

In-depth interviews with MTN, Airtel, and Agent Banking Company (as a key informant)

Areas of inquiry for agents
Transaction experience and training support
Awareness of data protection and mobile money guidelines
Customer data handling practices
Risk management and grievance resolution
Experience with women customers
Audit and monitoring

Areas of inquiry for customers
Experience in digital financial services
Awareness and attitude around aspects of data protection
Preference for agents (gender, trust, and service)
Responsible data protection practices employed by agents
Sharing information with agents

Areas of inquiry for providers
Agent onboarding and training
Customer service
Preference for agents (gender, trust, and service)
Responsible data protection practices employed by agents
Sharing information with agents

CGAP | MSC

Limitations of the study

Deliberate sample selection

We took support from our partner institutions to recruit respondents, which facilitated detailed discussions with them. However, we limited the impact of this selection on the research outcomes by maintaining a reasonable variation in the sample – men, women, rural, urban, literate, and semi-literate.

Limited generalization

The study's findings are indicative, with generalization limited to the sample areas or locations.

High sensitivity among respondents

We acknowledge that this research covers a highly sensitive topic – data protection. We ensured that we used best practices in moderation and interviews and a mix of participatory and group discussion tools to make participants comfortable with the topic.

2. What are some **responsible agent practices** to protect customer data?

Many agents report taking several steps to safeguard customer's data while conducting transactions (1)

No access to the customer's PIN

Agents do not access the customers' PIN unless customers specifically seek their help in conducting transactions at the agent point. The agents ensure the customers enter their PINs after initiating the transactions.

Maintenance of logbooks

Most MNO agents maintain a logbook of daily transactions. These agents record the customer transaction details and the identification number of the customers. Some agents ensure that the logbooks are securely stored to avoid exposure to client data.

Remote transactions

Agents follow all guidelines regarding conducting live transactions and ensure that the transaction status is shared with customers and proper records are maintained.

" I will lose customers if I do not agree to their requests. Sometimes, I go out of my way to help my customers." – A female agent

CGAP | MSC

Many agents report taking several steps to safeguard customer's data while conducting transactions (2)

A few agents have **installed cameras** that deter fraudsters since they know their faces will be seen and risk exposure to the police.

Agents have created a **WhatsApp group** to share emerging fraud threats, data protection breaches, and how to safeguard themselves.

Agents serve **one customer at a time** and ensure there is a distance to reduce the chances of one customer viewing another customer's PIN.

Agents **do not keep the logbook at the counter** and ensure the customer details are kept confidential.

Agents **do not make calls on the number** they use for official business. They do so to avoid any fraud.

Agents **advise customers to change their PINs** every few months to minimize cybersecurity and fraud risks.

CGAP | MSC

Case studies on agent best practices – Hasfa

Agent profile

Hasfa is a mobile money agent in Kampala, an urban area. She has been an agent for over twelve years. She is 33 years old and is married with children in primary school. She is a college graduate.

Quote

"I know the mobile money guidelines around safeguarding customer information and keeping PIN safe. I was informed of the guidelines and other rules when registering as an agent."

Current practices

- She operates the agency business for MTN and Airtel.
- She runs a separate business selling utensils.
- She admits to facing risks of fraud and theft.
- She has installed cameras to deter fraudsters.

How does she support customers?

- She educates clients on safeguarding PINs.
- She only helps elderly people to conduct transactions.
- Part of a group where they discuss data protection and fraud.
- Serves one customer at a time to ensure customer details are safe.

CGAP | MSC

Photo Credit: Arshi Aadil

Case studies on agent best practices – Jenie

Persona profile

Jenie is a bank and mobile money agent in Jinja, an urban area. She has been an agent for six months. She is 26 years old. She has post-graduate education.

Quote

"To safeguard the customers' data, I follow all the banking guidelines regarding conducting only live transactions and confirming transaction status with the customers."

Current practices

- She operates a bank agency business and a mobile money agency business.
- She runs a separate business selling cell phones and other electronics.
- She researched risks related to fraud and exposure of customers' data.
- She has installed cameras to deter fraudsters.

How does she support customers?

- She ensures she confirms the transaction status with the customer.
- She greets the customers to make them feel at home before transacting.
- She maintains proper records and ensures customers sign the logbook.
- She serves one customer at a time to ensure they don't see others' PIN.

CGAP | MSC

Photo Credit: Arshi Aadil

3. What are some challenges faced by agents to protect customer data?

Agents face several challenges as they serve customers and protect their data

01

Fraud

Many agents have fallen victim to fraudsters who pose as customer care agents of the provider when they intend to obtain customer data with the intent of defrauding customers.

02

Space constraints at agent locations

Due to a lack of space at some agent locations, like small kiosks, it can be difficult for an agent to ensure transaction details are protected every time they serve a customer.

03

High illiteracy levels among customers

Agents often face the challenge of customers revealing their PINs since they are illiterate and, therefore, cannot undertake the transactions independently. This may compromise the agent's ability to safeguard the customers' PINs.

04

The logbook structure does not foster confidentiality

The design of the transaction logbook is that several customers sign sequentially on the same page. This does not foster confidentiality since one customer can access the information of another customer on the same page of the transaction logbook.

05

Policy vs. practice

Due to excessive competition, agents often agree to customer requests to conduct remote and direct transactions. Agents charge UGX 1,000 (USD 0.26) to conduct a direct transaction. However, this is not allowed per the mobile money guidelines by the Bank of Uganda.

Direct transactions: Customers are not supposed to make direct deposits to someone else using the agent channel.
Remote transactions: Transactions conducted on someone else's behalf.

CGAP | MSC

Female agents perceive additional challenges

Although both male and female agents follow similar practices to protect customers' data, female agents perceive additional challenges in dealing with customers.

Vulnerable to fraud

Many female agents feel that fraudsters find them easier targets compared to male agents.

Female agents also believe they are more likely to be robbed at their location than male agents.

More men act as fraudsters

Female agents believe that men are more active as fraudsters than women.

They mention that although women customers are less patient with them, they are less likely to indulge in fraudulent activities. They need to be extra careful dealing with unknown male customers.

Male agents are more respected

Female agents believe that male agents command more respect than female agents.

Most female agents have a perception that people find male agents to be more competent, fast, and equipped to solve their issues. (MSC found similar perceptions in India).

CGAP | MSC

Based on anecdotal evidence collected from field interactions with the female agents.
Data collected from the eight female agents.

4. What are some responsible provider practices to protect customer data?

MNO providers adhere to the Data Protection and Privacy Act to ensure that the processes and systems are in place to collect, store, share, and delete customer data

	Collect	Store	Share	Delete
Provider practices	Providers train their agents to collect only specific information relevant to the transaction. No sensitive data (religious or philosophical beliefs, political opinions, sexual orientation, financial information, medical records) is collected to open mobile money accounts.	Providers require their agents to keep a record of the transaction in a logbook. While agents must update the logbook if they want to file a complaint, customers are unwilling to sign the logbooks.	While sharing data with banks and partners, providers ensure that the data is anonymized. MTN has a tool similar to 'Safeguard' (used by banks) to protect customer data.	Providers follow the due process laid out by the regulator regarding data processing and deletion.

MNO providers also support their agents to help them follow responsible practices around data protection

Providers cover some aspects of data protection through 'fraud management' topics during **agent training**.

Providers have made available a **dedicated agent phone line to support agent queries** with a 72-hour turnaround time.

Providers give their agents **collaterals** on marketing material, agent fees and commissions, and **PIN management**.

Providers **conduct mass media campaigns** around protection from fraudsters and safeguarding PINs.

Providers monitor transaction data regularly and **identify any data discrepancies in transactions** regularly.

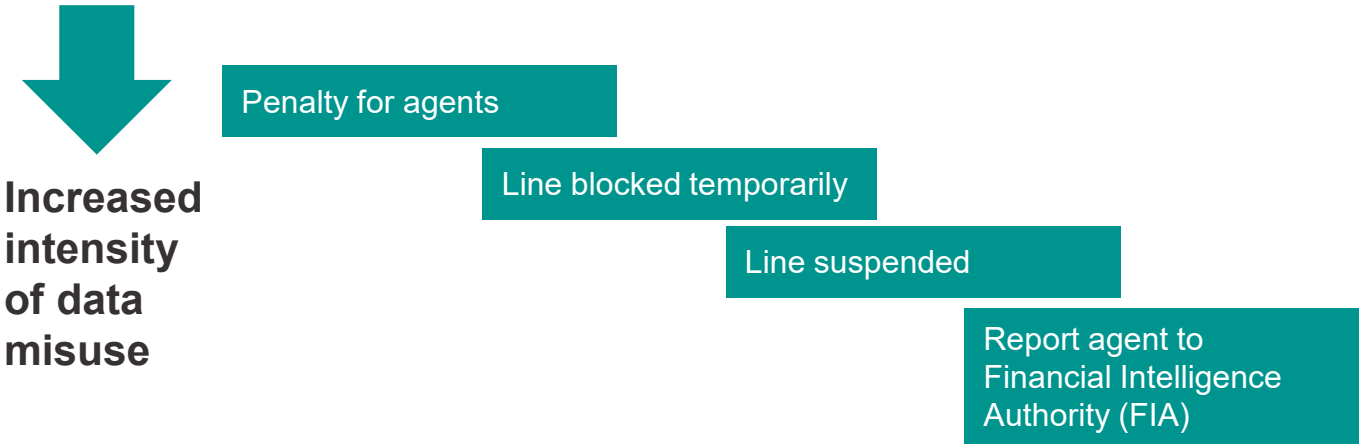
Providers monitor network systems and **inform agents in advance** if any network issues are expected.

CGAP | MSC

After the implementation of the Data Protection and Privacy Act, providers have strengthened their risk management practices

- The Ministry of ICT audits providers monthly to ensure their systems and services comply with the Data Protection and Privacy Act.
- As per the Data Protection and Privacy Act, providers have onboarded a dedicated Data Protection Officer who ensures that the data privacy act is adhered to.
- To monitor any discrepancies with the agent business, providers conduct a monthly audit of agents' data around the transactions, branding conformance, operating hours, and grievances.

Implications for agents – based on level of data misuse



> "Only the customer-facing function has access to customer data, and we have processes in place to safeguard it. Sensitive data exists at two levels: i) Governance level and ii) System-level."
>
> – Provider staff

5. Which areas can providers further strengthen, through their agents, to better protect customer data?

Providers can further strengthen data protection, working through their agents

01

Agent training

Agents do not get focused training on customer data protection. Post-COVID-19, providers have still not re-started refresher training in rural areas.

02

Supervisory support in rural areas

Agents in rural areas face more challenges in getting supervisory support. Supervisory visits are significantly less frequent in rural areas than in urban areas.

03

Lack of standardization around communication on data protection

No promotional material or training content on data protection was available with agents, which resulted in a lack of standardization around communication on data protection.

04

Lack of agent incentives

There are no rewards or incentives for agents who do not receive customer complaints. Providers used to run this incentive scheme, but it has been discontinued.

> “Agents used to be rewarded if they had zero complaints, but this has been discontinued. There is no specific provision to incentivize agents for safeguarding data.” – Provider staff.

CGAP | MSC

6. Are the data protection measures by mobile money providers in Uganda aligned with GSMA's guidelines on mobile money data protection?

Key observations on data protection practices employed by the mobile money providers mapped to the GSMA guidelines on mobile money data protection (1)

Principles around data protection	Adherence on ground
Principle 1: Data governance: Use of an overarching framework to shape how data is managed. A clear governance structure and the codification of internal policies and processes are crucial elements of this.	**Strong** Providers have formulated internal policies to govern data within the organization. Providers mention that they have onboarded an officer dedicated to data protection and privacy.
Principle 2: User choice and control: Users should be provided with information about their personal data. Mobile money providers, therefore, take steps to provide users with meaningful choices and control over their personal data.	**Moderate** There is very limited awareness among the customers about their rights and their enforcement as guaranteed in the DPPA Act, 2019. Mobile money agents do not explain the service agreement conditions to the customers on opening mobile money accounts. They hand over the agreement copy to the customers in English.
Principle 3: Data minimization -A central aspect of best practice by mobile money providers is the minimization of data. Only the minimum personal information for the minimum period is necessary to be kept for business purposes.	**Strong** Although the providers are collecting minimum data for opening a mobile money account, many customers share physical copies of NID and photographs while opening a new account. Since the documents are being submitted physically to the agent, the customer details can likely be shared illegally even before they reach the provider. No sensitive data is collected for the opening of mobile money accounts.
Principle 4: Openness, transparency, and notice: Openness, transparency, and notice are crucial to ensuring that users clearly understand how their data is used, enabling them to make informed decisions about whether to use a service.	**Weak** The customers have very limited awareness about how their data is stored, used, and processed by the providers. The provisions in the DPPA act allow customers to request the deletion of their data, but none of the respondents knew about it.

Key observations on data protection practices employed by the mobile money providers mapped to the GSMA guidelines on mobile money data protection (2)

Principles around data protection	Adherence on ground
Principle 5: Data and information security: The security of personal data is critical to data privacy.	**Moderate** Mobile money providers typically implement several mechanisms to ensure data security, e.g., protecting mobile money data from loss, or unauthorized access, destruction, use, modification, or disclosure. Providers maintain that they have systems that monitor and regularly review the security of customer data, including risk assessments. However, there have been instances of data leaks.
Principle 6: Data sharing: The transfer of personal data between third parties is critical, as is the sharing of data within organizations, and this may occur across different national or regional legal jurisdictions	**Weak** Customers are not informed about how their data can be shared with third parties. Although providers capture customer consent during the opening of mobile money account, the agents do not explain in plain terms the conditions for which consent is being taken. Providers mention that only the customer-facing vertical with the providers has access to customer data, and processes are in place to safeguard it.
Principle 7: Accountability: Accountability applies to the measures implemented by mobile money providers, demonstrating adherence to the principles of data protection and compliance with other applicable laws and regulations.	**Moderate** Providers monitor the transaction and grievance data to resolve issues and observe discrepancies. The Ministry of ICT (Information and Communications Technology) has mandated monthly audits to be conducted by all mobile money providers.

7. What are a few takeaways for providers who want to improve their data protection practices?

What can providers do to improve their data protection practices further?

01

Emphasize data protection topics in agent training

The providers must emphasize data protection policies and practices in agent onboarding training and any subsequent refresher training. Further, providers should emphasize data protection challenges and mitigation strategies during agent trainings. This is especially important given the high rates of fraud and data misuse.

02

Provide more agent supervisory support

While a focused customer care number for agents provides some support, rural agents receive supervisory visits at a much less frequent rate than urban agents.

03

Raise customer awareness on consent management and how their data is stored, used, and shared

Working through agents, e.g., through agent training and relevant collaterals, and through mass marketing campaigns, providers should better inform end-customers on how their personal data is being stored, used, and shared with third parties.

04

Provide a communication toolbox on data protection

To enhance awareness on data protection among customers and agents, providers can build a communication toolbox including marketing collaterals and comics. The collaterals can be used by the agents as display material and also as a guide to answer customer queries related to data protection.

05

Remove the practice of maintaining logbooks at agent points

Providers can consider doing away with agent logbooks as it is a redundant practice (with agents receiving SMS confirmations of transactions) and logbooks can be a source of possible data exposure.

CGAP | MSC

8. Appendix

Appendix 1: Customers' perspective

What is the extent of consumer risks in using mobile money in Uganda? What are the key observations?

- Mobile money users are exposed to multiple data risks.
- Customers are concerned about their data and privacy due to ever-evolving risks and fraud, such as phishing via SMS/calls.
- Customers are unwilling to share information with anyone as they understand the risks involved but are less careful about maintaining transaction privacy at the agent point due to space constraints at agent kiosks.
- Data protection to most customers is synonymous with protecting their PIN. However, customers do not prioritize resetting their PINs for enhanced protection.
- Customers are less aware of the provisions of the mobile money guidelines by BoU and agent fees and taxes.
- Most customers do not report their issues/complaints on the toll-free numbers shared by the providers due to a lack of trust in the grievance redressal systems.

Is the agent's gender a consideration for mobile money customers? Not if they get quick and good quality service

There are more agents present in urban areas as compared to rural areas. Since multiple agents are in urban areas, customers usually transact at multiple agent points based on the distance to the agent point, availability of float with the agent, agent's behavior, customer service, and crowd at the agent's location.

Factors that determine customer's choice of agents	Urban	Rural
The proximity of the agent point	1	2
Availability of float	2	3
Agent's behavior and customer service	3	1
Years in service	4	4

Ratings are based on the customer's responses on the attribute ranking and relative preference tools.

> **"Agents of the opposite gender tend to be more considerate sometimes"** – A female mobile money user in the rural area

> "**We do not care about the agent's gender if they provide good service. We go to the agent which is most close to our location"** – A male mobile money user in the urban market

> "**I can go to any agent, but I feel male agents are more patient and considerate with customers"** – A female mobile money user in the rural area

CGAP | MSC

To a certain extent, customers' location influences their preference for the agent's gender

01

Customers in urban areas need agents who can provide fast and reliable service. Their preference for an agent's gender is based on the gender of the agent they most frequently transact with.

02

Customers in rural areas mostly prefer agents of the opposite gender. This is because they need more assistance and information and feel agents of the opposite gender are relatively more considerate towards them.

03

Most customers in urban areas do not prefer the agent's gender. They switch agents as per the agent's availability in their vicinity. However, this is influenced by the fact that there are comparatively more female agents in the market.

04

Most women customers in rural areas are more comfortable conducting transactions at agent centers run by men. Women in rural areas trust agents more than their counterparts in urban areas.

Photo Credit: Arshi Aadil

*Insights based on responses received from customers who expressed a preference for the agent's gender

CGAP | MSC

Customer stories: Incidents

Most customers believe their data is being shared at the providers' end.

Sent money by mistake

Fatimah received a call from someone saying that they had sent some money to her account by mistake and requested to follow instructions. She agreed and lost UGX 20,000 (USD 5).

SIM cards being used to conduct fraud

Multiple SIM cards can be issued using the same NID card. The police caught many innocent customers as SIM cards issued in their names were used for fraudulent activities.

Follow instructions in exchange for gifts

Wesley, an MNO customer in an urban area, was told that the service provider was giving gifts during the festival and that he could claim it by following specific instructions.

Transfer money to arrange help

Doreen received a call that her husband needed to be rushed to a hospital after a bad accident, and UGX 150,000 (USD 39) was immediately required for his transport.

KYC or suspension of SIM

Many customers received calls from fraudsters pretending to be from the regulator. They were duped into losing their money on the pretext of conducting an immediate KYC to safeguard their connections from suspension.

PIN got stolen

Chris lost money while standing at the agent's location because someone had access to his PIN. Before the agent could authorize the transaction, fraudsters transferred money from Chris's account to a new number. The mobile number to which the money was transferred was switched off immediately.

Staff working with providers misuse data

Ana, a customer, mentioned that she was asked to follow instructions or her mobile money account would be blocked. She gauged that it was a fraud call and did not follow the directions. To her surprise, her number was blocked. This made her believe that either the present or the ex-employees of providers are involved in fraudulent activities.

Customer stories: Quotes

> “Since mobile money allows me to save regularly and easily, I am sure I will be able to support my family in times of financial crisis. However, I am afraid some fraudster might take my savings.”
>
> – Cynthia, 28, a single working mother, Uganda

> “The agents are from the village itself. They want our best and help and support us instead of exposing our data. Fraudsters get access to our data from the mobile network providers.”
>
> – Flavia, 35, women customer, Uganda

> “Fraud attempts are no big deal anymore since we are used to them. On average, we get one fraud phone call daily.”
>
> – Joseph, 40, male customer, Uganda

> Every time I get a message related to mobile money, I take it to my agent, who helps me verify the message’s authenticity.”
>
> – Lisa, 39, women customer, Uganda

> “Data can be exchanged only for loans or credit. I will not share my details with anyone if I don’t need a loan.”
>
> – Andrew, 35, male customer, Uganda

> “Before trusting an agent, I test them by giving them extra money for a deposit, checking their honesty. If they are honest, then they become my preferred agents.”
>
> – Sam, 33, male customer, Uganda

CGAP | MSC

Appendix 2: State of data protection in Uganda

Uganda's constitution protects the privacy and data of its citizens. Many other laws, acts, and guidelines have furthered the extent of data protection in Uganda

Article 27, Uganda Constitution, 1995: The Constitution of the Republic of Uganda provides for the right to freedom of expression and speech, privacy, and access to information under Article 27 of the constitution.

Mobile money guidelines, 2013: The Bank of Uganda launched mobile money guidelines to foster customer protection in mobile money services. The guidelines stipulate the specific roles of the Bank of Uganda, Uganda Communication Commission, Mobile money service providers, partnering financial institutions, mobile money agents, and customers.

Certain specific laws further incorporate data protection provisions applicable to regulated activities, including

- **The Access to Information Act, 2005**
- **The Regulation of Interception of Communications Act, 2010**
- **The Computer Misuse Act, 2011**
- **The Registration of Persons Act, 2015**

Data Protection and Privacy Act, 2019: Uganda enacted the Data Protection and Privacy Act, 2019, to supplement constitutional privacy protections under Article 27 of the constitution. This Act regulates personal data collection, processing, use, and disclosure and applies to every person, entity, or public body within or outside Uganda that collects, processes, or holds personal data. The Act takes a relatively comprehensive approach to data protection. It provides for a data protection and privacy register, notable powers for the NITA-U, and processes for investigating complaints relating to the infringement of data subject rights under the Act. In addition, the Act establishes consent as a central principle, specifies conditions for consent relating to minors and other special categories, and, notably, has an extraterritorial scope and may apply to entities outside Uganda.

CGAP | MSC

https://www.dataguidance.com/jurisdiction/uganda

Although the key mobile money guidelines by BoU state recourse for consumer protection, the ground level implementation of guidelines is not standard (2/2)

Guidelines on transactions:	Adherence on ground
1. A mobile money service provider, as well as its agents, shall uphold privacy and confidentiality of customer information and data.	Moderate (Although the providers and agents claim that they uphold privacy and confidentiality of customer data, customers complain that their data is susceptible to breach at agents and providers end)
2. The conditions under which customer information and data will be kept shall be disclosed before the customer enters into agreement with the mobile money service provider	Weak (Customers are not explained any provisions around their data protection but are made to sign the consent form on purchase of a new SIM)
3. Provisions of data protection including confidentiality shall be in tandem with all relevant laws	Strong (Providers mention that they comply to the DPPA Act, 2019)

*Based on field observations and interviews with agents, customers, and providers

Thank you

To learn more, please visit
www.cgap.org

CGAP | MSC

CGAP

www.cgap.org

BILL & MELINDA GATES foundation

British International Investment

UDENRIGSMINISTERIET
MINISTRY OF FOREIGN AFFAIRS OF DENMARK

European Investment Bank

Federal Ministry for Economic Cooperation and Development

giz

Global Affairs Canada

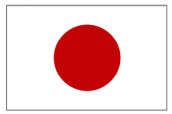
IDB | LAB

IFU INVESTMENT FUND FOR DEVELOPING COUNTRIES

IFC International Finance Corporation

IFAD
Investing in rural people

AGENZIA ITALIANA PER LA COOPERAZIONE ALLO SVILUPPO



JOA
JERSEY OVERSEAS AID

KFW

KOICA Korea International Cooperation Agency

THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG

Center for Inclusive Growth

mastercard foundation

MetLife Foundation

Ministry of Foreign Affairs and International Cooperation

Ministry of Foreign Affairs of the Netherlands

FMO
Entrepreneurial Development Bank

Sida

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Agency for Development and Cooperation SDC

Norad

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

UKaid
from the British people

UNCDF

UNDP

USAID
FROM THE AMERICAN PEOPLE