

USENIX

THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Security and Privacy Considerations for Confirming Payments in Rwandan Mobile Money Systems

Oluwole A. Adewusi, Assane Gueye, Wallace S. Msagusa, Jema David Ndibwile, David Nkundineza, Okemawo Obadofin, and Wilson Rutaremara, *Carnegie Mellon University Africa;* Blase Ur, *University of Chicago*

https://www.usenix.org/conference/usenixsecurity26/presentation/adewusi

This paper is included in the Proceedings of the 35th USENIX Security Symposium.

August 12–14, 2026 • Baltimore, MD, USA

ISBN 978-1-939133-58-8

Open access to the Proceedings of the 35th USENIX Security Symposium is sponsored by



جامعة الملك عبدالله للعلوم والتقنية

King Abdullah University of Science and Technology

ARTIFACT EVALUATED
USENIX
AVAILABLE

Security and Privacy Considerations for Confirming Payments in Rwandan Mobile Money Systems

Oluwole A. Adewusi, Assane Gueye, Wallace S. Msagusa, Jema David Ndibwile, David Nkundineza, Okemawo Obadofin, Wilson Rutaremara, Blase Ur†
Carnegie Mellon University Africa and † University of Chicago

Abstract

Mobile money (MoMo) services let users pay individual merchants or businesses using either a smartphone or a basic phone. They are widely used for commerce in African countries, including Rwanda. To better understand the security and privacy aspects of how Rwandan businesses confirm MoMo payments in practice, we interviewed 30 Rwandan business owners and employees. While MoMo services send payment confirmations over SMS to both senders (customers) and recipients (merchants), we found that merchants often inspect confirmation messages on *customers'* phones, not their own. The reasons included confirmation messages being sent only to business owners' (not employees') phones, busy markets, phones being physically unavailable, and delayed SMS delivery. Trust also played a major role. As the customer controls their phone, this workaround can enable fraud via screenshots of past messages or spoofed confirmations. As these confirmation messages include customers' account balances, participants also reported privacy concerns. In response, we investigated the design space of alternative workflows, finding promise in redesigning customers' confirmation screens to remove private information and to add a secret known only to the merchant. We reflect on designing for security and privacy under the unique constraints of Sub-Saharan Africa.

1 Introduction

Rwanda, an East African country with a population of about 14 million, has undergone a significant digital transformation in recent years [11]. One contributor to this transformation has been the growth of mobile money, or **MoMo**, services. These services let any registered user transfer money to other individuals and businesses. Both of Rwanda's main telecommunications operators, MTN and Airtel, offer a MoMo service [11, 34]. Notably, over 70% of Rwandan adults have a registered MoMo account [27], with the national penetration rate for active MoMo wallets at 53.4% [34]. Furthermore, over 60% of active users live in rural areas [27], positioning MoMo as a key mechanism for financial inclusion in a country with limited access to traditional banking [27].

A key difference between MoMo and the mobile payment systems popular in Western countries is that MoMo does not require a smartphone or data plan [13]. Instead, transactions are primarily initiated via USSD short codes (see Section 2). Deposits and withdrawals are handled by a nationwide network of MoMo agents [38, 39], who often have a small kiosk or even just a chair on the side of the road. Even villagers with basic phones (and without bank accounts) can use MoMo.

In this paper, we investigate the process by which Rwandan merchants verify MoMo payments from customers, focusing on the security and privacy aspects. When a customer pays a merchant, the customer receives both USSD and SMS confirmations of their payment. The merchant also receives an SMS confirmation of the transaction [2, 22]. Our study was inspired by our own experiences as MoMo users. Specifically, we observed informally that merchants often seemed to verify that a customer has paid them by examining the *customer's* (untrusted) phone, rather than their own phone, setting the stage for fraud through replayed or fabricated confirmations.

To this end, we conducted semi-structured interviews of 30 Rwandan business owners, managers, and employees. Our participants ranged from motorcycle taxi drivers to the owners of roadside stalls to shopkeepers in both urban and rural areas. We focused on the following research questions (RQs):

- **RQ 1**: How do Rwandan merchants verify MoMo payments from customers in practice?

Reinforcing our own experiences, 17 of the 30 participants reported relying on customers' phones to verify payments in at least some situations, presenting a security vulnerability. This practice was driven by challenges like inaccessible devices, network latency, and high customer volume, as well as trust. Notably, since point-of-sale terminals are uncommon in Rwanda, only the business owner (and not any other employee) typically receives payment confirmation messages.

- **RQ 2**: What privacy concerns do users have when using current MoMo payment confirmation interfaces?

The payment confirmation messages customers receive, which were not designed to be shown to others, contain the customer's full account balance. The majority of participants preferred not to show this information to merchants due to the potential safety risks. At the same time, business owners did not want employees to see the business's account balance.

- **RQ 3**: What security vulnerabilities arise from current MoMo payment confirmation practices in Rwanda?

Most participants had experienced some MoMo-related fraud, though the prevalence of fraud was low. Participants discussed spoofed payment confirmations, fraudulent transaction reversals, and phishing, as well as customers simply not paying.

- **RQ 4**: How could MoMo payment confirmation workflows in Rwanda be redesigned for security and privacy?

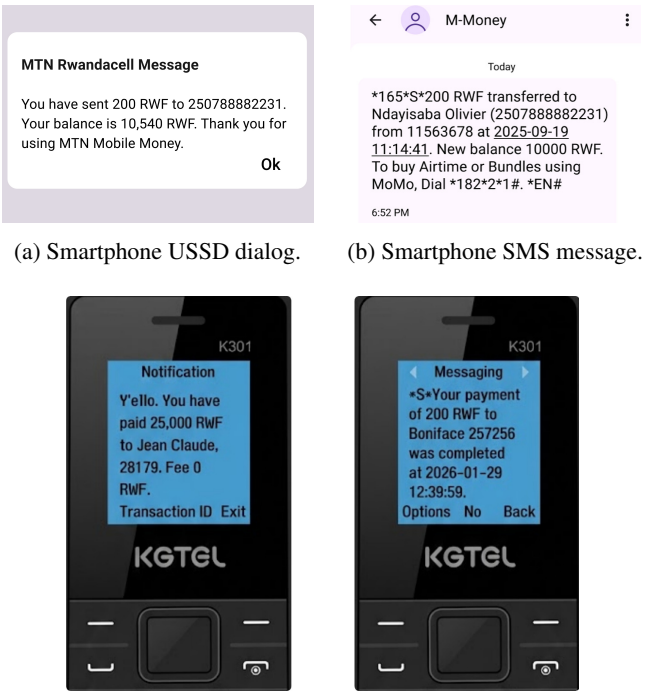
We brainstormed and prototyped various alternative payment confirmation workflows. We considered simple changes like moving the customer's account balance to a separate screen. We also explored adding merchant-defined secrets to customers' payment confirmations, potentially as part of an interactive protocol, as well as sending payment confirmations to multiple recipients. Participants favored these redesigns, except for those that had merchants touch customers' phones.

2 Background on MoMo in Rwanda

For low- and middle-income countries, MoMo is critical for accessing financial services. This is especially true in Sub-Saharan Africa, where formal banking infrastructure remains inaccessible to many [37]. Rwanda has two major telecommunications providers, MTN and Airtel, both of which provide MoMo services. That said, MTN MoMo is much more widely used than Airtel Money in Rwanda. As a result, in this paper, we adopt the umbrella term "MoMo" to encompass *all* mobile money services in Rwanda, reflecting colloquial usage in Rwanda. Notably, MoMo is widely used; 81% of Rwandan men and 72% of Rwandan women have a MoMo wallet [17]. In the MTN ecosystem, personal wallets are used for transfers between individuals, while MoMoPay wallets are used for businesses to receive payments from customers via distinct USSD codes [23]. As we detail in Section 5.3.3, many small businesses simply use personal wallets registered to the business owner, rather than a MoMoPay business wallet.

2.1 MoMo System Architecture

Rwandan MoMo transactions rely on interactive Unstructured Supplementary Service Data (**USSD**) sessions. USSD is an older protocol for mobile phones that creates a real-time connection between a user's phone and the mobile network operator. Rather than relying on global standards, USSD behavior is defined separately by each mobile network operator. Users typically access USSD via short codes defined by the mobile network operator. For instance, the short code "*182#" initiates an MTN MoMo session. At that point, USSD dialogs provide a text-based menu (Figure 6 in Appendix A). A typical MoMo transaction requires the user to enter a recipient's phone number and the amount of money to send. The user can cancel the transaction at any point during these steps. The user then authenticates using a personal identification number (PIN), at which point the transaction is processed on the mobile network provider's platform, which is integrated with the Rwanda National Digital Payment System [33, 35]. Transactions are often processed in seconds [3]. A key advantage of USSD is that short codes and text-based menus work on both smartphones and basic phones, increasing inclusion.



(a) Smartphone USSD dialog. (b) Smartphone SMS message.

(c) USSD (left) and SMS (right) confirmations on a basic phone.

Figure 1: Sample payment confirmation messages on a smartphone (top) and basic phone (bottom) in both the USSD and SMS variants. These messages have changed in minor ways over time; see Appendix A. *Note: We used generative AI for Figure 1c to transform photographs we took of our own basic phone into an abstract representation with more legible text.*

2.2 Payment Confirmation

Once a transaction is processed following successful PIN entry, the sender is shown a payment confirmation dialog via USSD (as in Figure 1a). In addition, a corresponding SMS message is sent to both the sender (as in Figure 1b) and the recipient. Each individual's SMS confirmation message includes their updated account balance following the respective deposit or withdrawal. Both the USSD and SMS messages are also displayed on basic (feature) phones, as in Figure 1c.



Figure 2: Reenactments of the MoMo payment confirmation workflow. In the intended workflow (top), both the sender and recipient inspect confirmation messages on their own devices. In practice, however, customers often simply show merchants the confirmation message they received on their phone (bottom). *Note: We used generative AI to obfuscate the models' identities and to highlight the phone for visibility.*

In an idealized workflow, payment confirmation will involve both the sender and recipient independently checking the payment confirmation message sent to their respective devices. However, in an alternative workflow we find to be prevalent in practice (see Section 5.3), the merchant never checks their own device. Instead, the customer (sender) shows the merchant (recipient) the payment confirmation on the customer's device. Figure 2 shows a reenactment of these two workflows. Customers may show the merchant either the USSD or SMS confirmation message on their (potentially untrusted) device. Conceptually, this workflow introduces security and privacy risks, including the potential for fraud.

3 Related Work

Despite its role in promoting financial inclusion in Africa, MoMo has introduced security and privacy challenges. The magnitude of these security risks was evident, for instance, in the temporary suspension of MoMo transactions in Uganda after a major system breach, resulting in massive financial losses [38]. In this section, we highlight prior work on the security, privacy, and usability of MoMo-like systems. Although prior work has extensively examined social engineering attacks and systems security vulnerabilities, as detailed below, our study is the first to investigate how African users confirm payments in real-world usage contexts. Our focus on Rwanda is particularly notable as non-Western contexts are often overlooked in security and privacy research [16, 41, 42].

Security Vulnerabilities. Unlike smartphone-based banking apps that can take advantage of techniques like sandboxing, MoMo relies on USSD, arguably a legacy protocol. Lamoyero and Fajana highlighted that USSD lacks end-to-end encryption and relies on weak PIN authentication [20]. Furthermore, because messages are transmitted in plain text, they can be vulnerable to interception or spoofing [1]. SIM swap fraud is another threat. Attackers hijack a user's phone number to intercept one-time passwords and reset credentials [20, 28, 29]. Castle et al. noted the risks of SMS spoofing, weak authentication workflows, and MoMo agent fraud [8]. Reaves et al. showed that MoMo smartphone apps often suffer from insecure coding practices, including improper certificate validation and a lack of encryption [31]. Regulators must balance financial access with safeguards against fraud [6].

Privacy Risks. Odai and Daniel argued that the fundamental design of MoMo systems (with phone numbers doubling as user IDs) presents risks to personal information [30]. Furthermore, users' reliance on MoMo agents creates additional privacy risks. Nearly half of MoMo users in Uganda expressed discomfort with how agents collect and process their personal data, fearing that agents may share their information with third parties like politicians or fraudsters [38]. While MoMo users consistently regard their PIN as sensitive, opinions vary regarding the sensitivity of phone numbers and transaction histories. Large transaction amounts are often perceived as highly sensitive due to the fear of robbery. Sowon et al. identified four primary user concerns: fraud, unauthorized data reuse, reputational harm, and physical risk [39].

Social Engineering. Attacks like phishing that exploit human behavior are common in MoMo systems [10, 14]. Adongo taxonomized common attacks across Africa, ranging from impersonation to social manipulation [1]. Some attackers generate fake transaction alerts to trick users into believing a transfer has occurred or to solicit account credentials. In Uganda, voice phishing is especially prevalent. In those cases, fraudsters pose as customer support agents. Other attackers use pretexting schemes that impersonate respected community figures. Mihretu et al. reported that fraudulent phone calls account for over half of reported incidents in Tanzania [21]. Castle et al. also noted the risks of friends and family members whose physical access to devices enables fraud [8].

Confirming Payment Transactions. Unlike Western countries, where credit cards and digital wallets (e.g., Apple Pay,

Google Wallet) are widely used, in Rwanda MoMo and cash are the primary methods of payment. In this regard, Rwanda resembles other lower-resource countries, where payment systems rely on interpersonal relationships and trust [36]. To our knowledge, our study is the first to focus primarily on payment confirmation practices for a mobile money system in an African country. In the East African context, perhaps the closest work to ours is Sowon et al.'s proposal of a new protocol that better protects the privacy of MoMo users from the agents who facilitate deposits and withdrawals [39]. Specifically, they proposed redesigns of deposit and withdrawal procedures involving agents for a MoMo system in Kenya, evaluating their approach by interviewing 32 customers and 15 agents. They did not examine payment confirmation practices, however.

Outside the African context, He et al. investigated the challenges street vendors in China face [18]. The mobile payment systems used in China differ substantially from those used in East Africa. For instance, the Chinese systems place a large emphasis on QR codes, which are rarely used in East Africa. Furthermore, those systems' payment confirmation workflows differ substantially from Rwandan ones. Nevertheless, some themes from He et al.'s work overlap with some of ours. For instance, they also recorded vendors' concerns about customers fleeing before completing transactions, some vendors not having their own devices to receive payment confirmation messages, and the potential for fraud in the payment confirmation process. Their main findings related to avoiding fraud, such as street vendors' practice of waiting for an audible beep that indicates successful payment. Further differentiating our work from theirs, we also investigated potentially more secure approaches to displaying payment confirmation messages on customers' devices.

African Security and Privacy Practices. Other work has studied additional aspects of security and privacy in the African context beyond MoMo systems. For instance, Munyendo et al. uncovered numerous security and privacy pitfalls of the reliance on cybercafes for digital access in Kenya [25]. Researchers have also highlighted the security and privacy dangers of mobile loan apps in Kenya [24], WhatsApp mods popular in Africa [26], and shared infrastructure both in rural Ghana [40] and in Kenya [19]. MoMo did not feature prominently, or at all, in those prior studies.

4 Methods

In this section, we describe our process of recruiting participants, the structure of our interviews, and our approach for analyzing qualitative data. We also discuss key limitations. As detailed in our Ethical Considerations appendix, we took a number of steps to protect participants and treat them fairly. Our protocol was approved by both our university IRB and the Rwanda National Ethics Committee (RNEC), which must approve all human-subjects research in Rwanda.

4.1 Population and Recruitment

Our goal was to recruit a sample of Rwandan business owners, managers, and employees who were directly involved in confirming customers' MoMo payments. We exclusively targeted merchants for this study because they face a higher risk of encountering fraudulent customers than MoMo users who only transfer money to their friends and family. Merchants also engage in a higher volume of daily MoMo transactions. Our inclusion criteria required participants to be adults age 18 or older who had resided in Rwanda for at least five years, used MoMo as a merchant, and spoke either Kinyarwanda or English. Our choice of inclusion criteria was motivated by our experiences living in Rwanda and using MoMo. These criteria may have shaped the initial research questions and hypotheses on informal practices of MoMo use. To mitigate this influence, interviews were kept open-ended and participants were encouraged to describe their experiences in detail.

A key recruitment challenge was that human-subjects research, especially research related to technology, is much less common in Rwanda than in Western countries. Recruitment methods common in the USENIX Security community (e.g., online crowdsourcing platforms, flyers, participant pools, and classified ads) are either uncommon or completely nonexistent in Rwanda. In response, we adopted a direct approach procedure in which members of our research team directly approached prospective participants in public locations. This strategy enabled us to access a diverse range of users who might not be reachable through other means. In choosing whom to approach, we both attempted to balance our sample's demographics and to minimize the chance that we were interrupting a prospective participant. For instance, we did not approach anyone who appeared to be involved in a transaction or conversation. Our Zenodo open science repository includes our recruitment scripts in both Kinyarwanda and English.

Because we suspected MoMo usage would differ between urban and rural areas based on usage statistics [27], we recruited participants in a variety of environments. Table 1 lists each recruitment site and the number of participants recruited at each. Of our 30 interviews, 18 took place within Kigali City, Rwanda's capital and urban center, with a population of nearly 2 million people. Even within Kigali, we intentionally recruited in distinct neighborhoods, such as Kimironko (the home of Kigali's largest market), the Nyabugogo bus terminal, and Nyamirambo (the heart of Kigali's Muslim community). We recruited the remaining 12 participants in Rwanda's more rural Northern, Eastern, and Southern provinces. We targeted small businesses and sole proprietorships, where payment confirmation often relies on personal devices.

If a prospective participant expressed interest, we provided a consent form for review. Upon obtaining their consent, we let participants choose whether to complete the interview immediately or at a later time via a WhatsApp call or phone call so that the protocol would be as convenient as possible

Table 1: Recruitment sites and the number of participants.

Region	Specific Location	#
Kigali City	1. Gasabo - Kimironko	4
	2. Gasabo - Bumbogo	3
	3. Gasabo - Rusororo	2
	4. Nyarugenge - Downtown	4
	5. Nyarugenge - Nyabugogo Bus Park	2
	6. Nyarugenge - Nyamirambo	3
Northern Province	1. Rulindo - Base	2
	2. Rulindo - Tare (Mukinini)	1
	3. Gicumbi - Mutete (Gaseke Market)	2
Southern Province	1. Kamonyi - Bishenyi	3
	2. Muhanga - Nyamabuye	1
	3. Muhanga - Muhanga (Igihuma)	1
Eastern Province	1. Bugesera - Ruhuha	2

for them. Despite our offer of a call, all 30 participants opted to complete the interview in person at the time of recruitment. We continued recruiting new participants until we achieved thematic saturation, the point at which sessions had ceased to yield new insights regarding our research questions.

Interviews took place from October 2025 to December 2025. We compensated each participant 7,500 RWF ($5.14 USD, €4.36 EUR) via a MoMo payment. We deliberately chose this amount to strike a careful balance within the local economic context. Rwanda's minimum wage has not been revised since 1974 and remains 100 RWF per hour ($0.07 USD, €0.05 EUR) [43]. Thus, our research team decided to benchmark the compensation to the approximate cost of an entrée at a mid-range restaurant. Our research team felt this amount provides a meaningful incentive that respects participants' time without being coercive.

4.2 Study Design and Interview Structure

We designed the interview, which employed a semi-structured format, to take about one hour. Prior to the main study, we conducted five pilot interviews to refine the interview guide and seek a formative understanding of how participants might react to our design probes. We let participants choose whether to conduct the interview in Kinyarwanda or English; 28 of the 30 participants chose Kinyarwanda. Our Zenodo open science repository includes both the Kinyarwanda and English versions of our interview guide. To verify the accuracy of our translation, we used back translation. One member of the research team translated the interview guide from English to Kinyarwanda, while another (who had not seen the English version) translated it back from Kinyarwanda to English. This process was repeated until the two versions matched. We also hired an independent translator to certify our final translation. The interview proceeded as follows:

General Use of MoMo: The interview began with questions exploring MoMo usage. We asked about the participants' history with MoMo, usage in personal and work contexts, the type of device used (smartphone or basic phone), and how they performed transactions (e.g., via USSD or an app). This part of the interview established an understanding of participants' MoMo practices and helped frame later discussions.

Payment Confirmation Practices: We then examined MoMo payment confirmation practices. We particularly focused on the workflows participants employed when interacting with their customers. The questions first probed their experiences as merchants processing customer payments and subsequently as customers paying other merchants. Investigating the payment process from both perspectives provided a comprehensive understanding of how different entities verify MoMo payments and enabled us to identify points of uncertainty, delay, or misunderstanding during transactions. This approach was informed by our pilot interviews, which highlighted that merchants were primary targets of fraud.

Perceived Risks, Trust, and Privacy: We also assessed participants' general concerns related to privacy, security, fraud, and reliability when using MoMo. We asked specific questions about both direct and indirect experiences with fraud. We also inquired about participants' trust in others. These questions helped us to understand how users balance convenience, social trust, and privacy when using MoMo.

Prototype Interface Evaluation: To gauge the feasibility of potential alternative workflows for confirming payments, our final activity elicited participants' reactions to four alternative confirmation interfaces shown in randomized order. We chose which types of designs to explore based on group brainstorming informed by team's personal experiences as active MoMo users, formal discussions about the pilot data, and our knowledge of the usable security literature. Our designs included removing account balances (Figure 14 in the appendix), adding either a static or interactive secret to the confirmation message (Figure 15 in the appendix), or enabling confirmation messages to be sent to multiple people. For two interfaces, our prototypes included additional variants differentiating between payments to individuals and to businesses. For each prototype, we solicited both overall reactions and specific feedback on the design. Our open science repository includes both our Kinyarwanda and English prototypes.

Demographics: Finally, we administered optional demographic questions to contextualize participants' reported experiences. We also gave participants the opportunity to share additional comments or ask questions.

4.3 Data Analysis

All interviews were audio-recorded, transcribed in their original language, translated to English (if applicable), and reviewed multiple times in team meetings. In total, five coders qualitatively analyzed interview transcripts using an iterative, inductive thematic analysis approach [7]. Our goal was to understand participants' practices, concerns, perceptions, and

experiences regarding MoMo, focusing on payment confirmation practices. Specifically, our thematic analysis established themes through the following process. First, we took notes on potential emerging ideas and recurring patterns when reviewing moderators' post-interview memos of each interview. This initial immersion helped us form a preliminary understanding of participants' experiences as we prepared the transcripts for more systematic coding. We employed process coding techniques [9], focusing on identifying actions expressed in participants' narratives. Rather than using predefined categories, we developed short descriptive labels that captured key practices related to MoMo. This approach helped us stay grounded in participants' articulations of their own experiences, helping us trace the relationship between participants' security and privacy concerns and their resultant behaviors.

Following this initial free-form coding, we identified recurring themes and grouped related codes into thematic clusters. We reviewed these themes in group meetings to ensure alignment with our research questions. The full team then took these preliminary codes and used a process informed by affinity diagramming [15] to merge, separate, and refine themes. We performed affinity diagramming using online spreadsheets containing all participant quotes that had been tagged initially. We fully resolved all disagreements through discussion among members of the research team. All members of the research team had a formal education in computer security topics, as well as personal experience using MoMo in Rwanda.

4.4 Limitations

While we made a significant effort to recruit a diverse sample of Rwandans, ultimately we report on a convenience sample. We conducted recruitment entirely within Rwanda, focusing on high-traffic locations within Kigali City and in the Northern, Southern, and Eastern Provinces. Because user studies are so uncommon in Rwanda, we suspect that prospective participants may come from a smaller pool than user studies in Western contexts. Our inclusion criteria also mean that our findings do not try to capture the viewpoints of Rwanda's new residents or visitors, as well as non-users of MoMo.

Furthermore, our investigation focused on users of Rwanda's dominant MoMo service provider (MTN), rather than the entire MoMo ecosystem in Rwanda or even East Africa more generally. We crafted our study to accommodate participants using Rwandan MoMo services from either MTN or Airtel. Nonetheless, most participants only used MTN MoMo, reflecting MTN's 84.3% share of active MoMo-linked SIM cards in Rwanda [34]. While many other East African countries' MoMo services superficially resemble MTN's MoMo system, our findings may not fully generalize to users of platforms like Airtel Money (Rwanda) or M-PESA (Kenya and many other countries). Moreover, most participants primarily used the USSD interface to MoMo, rather than the smartphone app. While our own experiences suggest that this finding reflects real-world usage patterns, it limits our insight into MoMo smartphone apps. As smartphone adoption grows, this distinction could become more important.

Additionally, some quantitative figures reported in Section 5 (e.g., P-7's "95%" and P-23's "80%") reflect participants' own estimates rather than values elicited on a scale. They should be read as directional rather than precise responses. Furthermore, the prototype interfaces evaluated by participants are best characterized as design probes. Our design ideas tried to address core challenges for users, but are limited, exploratory, and not validated solutions. However, they did successfully establish a necessary foundation for further empirical evaluations and future design iterations.

Finally, our methods centered on self-reported data from semi-structured interviews. Participants' descriptions may differ from their actual practices and reflect biases like satisficing. Participants might also underreport behaviors they know are insecure. We mitigated this concern by conducting recruitment and consent in person to establish rapport before the interview itself. Furthermore, device sharing is relatively common in Africa [19], yet our protocol did not fully explore this topic. Despite these limitations, our study provides a formative understanding of the security and privacy challenges in how Rwandans confirm MoMo payments in practice.

5 Results

We first summarize participants' demographics and MoMo usage. We then report our key findings on payment confirmation practices, as well as privacy and security concerns. Section 6 subsequently details participants' reactions to our prototypes of alternative payment confirmation workflows.

5.1 Participants

Table 2 details our 30 participants' demographics. Among participants, 17 identified as male and 13 as female. We covered a diverse age range, with six participants aged 18–24, eight aged 25-34, nine aged 35-44, three aged 45-54, and four aged 55-64. Regarding participants' level of education, 13 had completed primary education, 10 had completed high school, and six held a university degree. While our study interrogates participants' roles as both merchants and customers, all 30 participants were recruited in their capacity as merchants.

Our sample included eighteen business owners (most frequently of sole proprietorships), four managers, and eight employees. Their occupations covered a broad spectrum of the local economy. Notably, our sample included four motorcycle taxi drivers (operators of the country's primary mode of transport), seven owners of small kiosks (tiny shops in rural regions that sell fruits, vegetables, and toiletries), two MTN agents (facilitators of MoMo cash-in and cash-out services), an Irembo Agent (providing access to digital government services), and workers at various other types of shops and

Table 2: Participants' demographics, including occupation, gender (M/F), age range, education, recruitment location, and language. The location abbreviations are defined in Table 1.

P-X	Occupation	M/F	Age	Education	Recruited	Language
P-1	Moto taxi driver	F	25–34	Primary	Kigali-4	Kinyarwanda
P-2	Kitchen shop manager	M	25–34	Secondary	Kigali-4	Kinyarwanda
P-3	Moto taxi driver	M	35–44	Primary	Kigali-4	Kinyarwanda
P-4	Fuel station attendant	F	35–44	Secondary	Kigali-5	Kinyarwanda
P-5	Wholesale shop owner	F	35–44	Primary	Kigali-5	Kinyarwanda
P-6	Irembo agent	M	25–34	University	Kigali-1	Kinyarwanda
P-7	Moto taxi driver	M	18–24	Secondary	Kigali-1	Kinyarwanda
P-8	Coffee shop barista	F	18–24	University	Kigali-2	English
P-9	Restaurant waiter	M	25–34	University	Kigali-6	Kinyarwanda
P-10	MTN agent	F	18–24	Undisclosed	Kigali-6	Kinyarwanda
P-11	Bakery cashier	F	35–44	Secondary	Kigali-6	Kinyarwanda
P-12	MTN agent	M	25-34	Primary	Kigali-4	Kinyarwanda
P-13	Food stall manager	M	25-34	University	Kigali-2	English
P-14	Bar manager	M	25-34	Secondary	Kigali-1	Kinyarwanda
P-15	Moto taxi driver	M	45-54	Secondary	Kigali-1	Kinyarwanda
P-16	Bar attendant	M	18-24	Primary	Northern-3	Kinyarwanda
P-17	Shop attendant	F	18-24	University	Northern-3	Kinyarwanda
P-18	Restaurant owner	F	18-24	Secondary	Southern-1	Kinyarwanda
P-19	Hardware shop owner	F	25-34	University	Southern-1	Kinyarwanda
P-20	Greengrocer	F	35-44	Primary	Southern-1	Kinyarwanda
P-21	Retail shop owner	M	45-54	Primary	Southern-3	Kinyarwanda
P-22	Restaurant owner	F	35-44	Secondary	Southern-2	Kinyarwanda
P-23	Small kiosk owner	M	35-44	Primary	Northern-2	Kinyarwanda
P-24	Small kiosk owner	F	45-54	Secondary	Eastern-1	Kinyarwanda
P-25	Small kiosk owner	M	35-44	Primary	Eastern-1	Kinyarwanda
P-26	Small kiosk owner	M	35-44	Primary	Northern-1	Kinyarwanda
P-27	Stallholder	M	55-64	Primary	Northern-1	Kinyarwanda
P-28	Small kiosk owner	M	55-64	Primary	Kigali-3	Kinyarwanda
P-29	Small kiosk owner	M	55-64	Secondary	Kigali-3	Kinyarwanda
P-30	Small kiosk owner	F	55-64	Primary	Kigali-2	Kinyarwanda

restaurants. Of the interviews, 18 took place in Kigali, while 12 took place in more rural areas. Furthermore, 28 interviews were conducted in Kinyarwanda and only two in English.

5.2 Use of MoMo

Prevalence and Usage Habits. The majority of participants reported heavy reliance on MoMo, prioritizing it for both personal and business needs. P-13 noted a clear dominance of MoMo payments, stating *"70% of [customers] use MoMo, and 30% use other methods."* Similarly, P-15 shared that *"out of 10 clients, about 7 or 8 pay via MoMo, and only a few pay in cash."* Cash was the primary alternative payment method: *"I would say around 60% is through MoMo and 40% is cash"* (P-11). While urban merchants reported particular prevalance of MoMo among customers, most rural participants (outside of Kigali City) described significantly lower MoMo usage among customers. P-21 explained, *"Looking at my daily report, most [customers] pay in cash rather than using MoMo. For example, yesterday I made 60,000 [RWF] in sales, and only 17,000 [RWF] came through MoMo."* Some of the rural merchants attributed this gap to village residents either lacking phones or typically receiving their wages in cash.

Access Modalities. While MoMo mobile apps are available for both Android and iOS, all 30 participants reported using USSD short codes as their primary MoMo interface. In fact, 27 participants reported using USSD exclusively, while three participants reported occasionally using the smartphone app. No one relied exclusively on the app. Participants preferred USSD due to its familiarity, offline capability, and compatibility with both smartphones and basic phones. The three participants who used the smartphone app did so for extra features like transaction history at a glance or alternative payment interfaces (P-6: *"I have the MoMo app, which I can use to make payments... by scanning [a QR] code"*).

Account Ownership. The use of multiple accounts was widespread; 24 participants reported having more than one MoMo account. Approximately 50% of participants leveraged this strategy to separate business revenue from personal funds, often using multiple SIM cards all registered in their own name. For example, P-18 explained, *"There's one I use here at work and there are others I use in regular life."* Further, 16 participants maintained accounts for both key MoMo providers (MTN and Airtel) for the benefit of network redundancy. P-15 explained, *"Sometimes MTN's network is down in some areas, while in others Airtel's is down."* That said, twelve participants mentioned regularly interacting with accounts registered to other people for social or business reasons. As P-13 reported, *"For one [account], I use my own phone, and then for the second one, it's for my boss's company."*

5.3 Payment Confirmation in Practice

As highlighted in Section 2.2, successful transactions on MoMo are followed by SMS notifications delivered to both the merchant and the customer. Best practices would dictate that both parties inspect their confirmation messages independently. However, we found that merchants commonly relied on the *customer's* phone to confirm a successful payment. In our interviews, we focused on participants' experiences as merchants confirming payments from customers. However, to minimize the chance they would underreport practices they knew to be insecure, we subsequently asked about their experiences as customers of other businesses.

5.3.1 Whose Device is Used for Confirmations?

Customers' Phones. In their capacity as merchants attending to customers, the majority of participants (17 of 30) used the customer's device as their primary method when confirming payments. Six of those 17 participants reported relying exclusively on the customer's device. For instance, P-7 reported that they relied solely on the customer's device for *"6 out of 10"* transactions. When asked how often he asks customers to show him their phone as proof of payment, P-9 said, *"Often, especially when messages are delayed."* When further asked what percentage of customers show him the confirmation message on their phone, he stated, *"Almost all of them, like 95%."* P-13 explained, *"A lot of [customers] come and show me their payment confirmation screens... I can't confirm [on my own device] because I have many customers at that particular time."* P-14 echoed this experience, saying, *"When someone pays for things like food, they already know the price and are often in a hurry, so they can't wait for me to check the*

payment." Beyond high customer volume, other motivations participants mentioned include the phone that receives the confirmation messages being inaccessible or delays in the cellular network. Section 5.5 explores these aspects in depth.

In their capacity as customers of other businesses, participants reported that this practice was similarly prevalent. For instance, eight participants reported that their own phones (as customers) were usually the sole source for payment confirmation at other businesses. P-11 observed that in many shops, *"the merchant doesn't even know where their phone is,"* forcing a reliance on proof displayed by the customer. This approach presents risks to both the customer and the merchant. For example, the customer's confirmation screen contains their full balance remaining after payment, a frequent source of concern that we detail further in Section 5.6.1. The merchant also faces the risk of fraud, which we detail further in Section 5.7. For instance, screenshots of past confirmations could be shown. Similarly, a fraudulent SMS notification could be created to resemble a payment confirmation.

Both Customers' and Merchants' Phones. Among the 17 participants who reported confirming payments primarily by looking at customers' devices, 11 reported practicing what we term "double confirmation": checking both the customer's phone and their own, perhaps at different times. As P-4 explained, *"They show us the message and then we confirm it on [our] phone."* P-8 echoed this practice: *"I check the customer's phone, then I check my phone."* However, qualitative nuances suggest that the second check often occurs after the fact. Merchants may inspect the customer's device to expedite the transaction, letting the customer leave before verifying on their own device. As P-16 explained, *"No, I don't usually wait because sometimes they really show me their phone and I see that they sent money. I let them go without problem. I wait for the SMS message to come after I let them go."* Unfortunately, merchants lack recourse once a customer has left.

Merchants' Phones. In total, 13 of the 30 participants reported relying on their own devices as their primary method of payment verification in their capacity as merchants. These participants typically emphasized that confirming payment using their own phone was the most secure approach. For instance, P-10 explained, *"Checking on my phone is the most reliable way."* P-14 reinforced this preference: *"The best way, in my view, is that the merchant should check their own phones on their own."* Adding more nuance, P-11 explained, *"Checking on my phone is the most reliable way for me because when the money comes in, you receive a message and immediately see that the balance has increased. Honestly, this is the only method I trust."* Indeed, changes in the merchant's account balance were commonly reported as a signaling mechanism. For instance, P-7 reported, *"Sometimes, [confirmation] messages take time to arrive, but since I know my balance, I check it. If the balance has increased, it means the money has come in."* In fact, the aforementioned P-10 uniquely reported a nearly complete reliance on balance checks: *"I don't trust that the customer has paid me just by looking at their phone; I first check the balance."*

While these participants perceived checking their own phone as the most secure approach, interviews with participants revealed frequent deviations from this practice. For example, P-14 seemed to partially contradict himself: *"Every time someone pays using MoMo, I confirm the payment by checking on my own phone... I only look at the client's phone when it's necessary."* Despite reporting following one practice "every time," he subsequently noted that he does not *always* do so. We cannot definitively attribute the cause of these contradictions; possibilities include genuine variation in practice, discomfort with the interview setting, or alignment with perceived researcher expectations. Similarly, P-25 first reported checking their own device *"every time I receive money,"* but later clarified that *"there are cases where I tell the customer that I trust them. Sometimes I read the message immediately; other times I read it later."*

No Confirmation. Among the 30 participants interviewed, six participants reported some cases where they did not seek any sort of confirmation. Reflecting on her experience as a merchant, P-11 reported, *"Usually, I just ask 'Have you paid?' rather than asking to see the message because I also feel that's a way of showing respect."* Speaking instead from the customer's perspective, P-7 similarly explained, *"Yes, that happens... you pay and just tell them the money has been sent, then you leave without showing them the message."* P-13 noted that because they are a regular at certain stores, *"they can even let me go without checking my phone."* This approach is often reserved for frequent customers, though it can extend to strangers at high-volume times. P-11 estimated this occurs *"maybe about 2% of the time"* when making payments to other merchants as a customer. Notably, three participants described situations where they attempted to show their phone to a merchant as a customer, but the merchant refused. In addition, P-23 highlighted a practice among wholesale merchants who verify payments simply by asking for the customer's name.

5.3.2 Key Features of Confirmation Messages

To inform the design of payment confirmation messages, we asked participants which aspects of messages they examine.

Common Artifacts. Six participants reported distinguishing authentic confirmation messages from fakes by looking for specific keywords, such as *"y'ello"* or *"you have received,"* both of which appear in MTN's payment confirmation messages. P-2 shared that he will *"check the SMS for 'you have paid... On a smartphone, you can see 'you have received' in the message."* P-3 also mentioned, *"I immediately check if it shows 'sent'... there is usually the word 'y'ello' in the message, written in English. Once I see it, I know they have paid."* Unfortunately, these artifacts do not prove a message's authen-

ticity. As discussed further in Section 5.7, both screenshots of previous transactions and spoofed confirmation messages could easily contain these artifacts.

Other participants reported looking for the date/time, the amount sent, and the identity of the sender in addition to the artifacts described above. As P-11 summarized, *"Depending on which message the customer shows me. On the first one, there's a 'y'ello' mark. When I see it, I immediately know the payment went through. I also look at the second message to confirm the amount, date, and time, making sure the names and amount match what was paid."*

SMS Source ID. Four participants reported inspecting the sender listed for the SMS notification on customers' phones to confirm the message's authenticity. By default, SIM cards label this number "M-Money." P-19 reported, *"I check the message... I check that it is M-Money."* P-2 similarly shared that he will *"first check if it's truly via Mobile Money, not a regular number."* Notably, however, an attacker could simply save some other number in their phone under the contact name "M-Money," so this signal does not actually authenticate messages on customers' phones.

5.3.3 The Unique Role of Names

One unique aspect of the MoMo transaction process is that when a customer enters the merchant's number to initiate a transaction, they are shown the full, legal name of the individual to whom the account is registered for all personal (i.e., non-business) MoMo accounts. Figure 10 in the appendix shows an example of this screen. While large businesses often have MoMoPay business accounts, sole proprietors and small business owners typically reported using only personal accounts, not formal business accounts. In other words, the MoMo account was simply registered to the business owner as an individual for most moto taxis, kiosks, and small shops.

Participants often reported that saying the recipient's name during a transaction was important for ensuring the correct number was entered. Specifically, after inputting the MoMo number (e.g., of a moto taxi driver), it was common practice for customers to state the recipient's first name. As P-22 reported, *"You tell [the customer] your number and they say your name to ensure they send it to the right person."* However, these interactions also served as signals that the customer was initiating a real MoMo transaction. That said, the customer could simply cancel the transaction partway through after learning the recipient's name. Further, the disclosure of the business owner's full legal name creates a privacy risk.

5.4 Role of Trust in Payment Confirmation

Although many participants verified payments on customers' (untrusted) phones, the system did not collapse due to high levels of trust among Rwandans, especially acquaintances.

Established Trust. Trust was rarely extended to strangers. For instance, P-9 noted they would not hand their phone to anyone unless they *"fully trust the person."* Instead, participants described a *"neighborhood trust"* where geographic proximity and repeated interaction served as proxies for proof. P-12 explained that requests from known customers are processed *"without a second thought."* Similarly, P-14 noted that in local neighborhoods, merchants often accept a verbal confirmation. P-23 quantified this aspect, stating they trust familiar people *"about 80%,"* often allowing known bulk buyers to leave before confirmation arrives because the existing relationship guarantees future recourse.

Situational Trust. Seven participants reported bypassing standard confirmation protocols during high-pressure scenarios where external conditions made checking impossible or unsafe. P-3 described how the physical environment dictates this behavior, saying, *"It happens like when it's raining or when you're somewhere you're not allowed to park. In that case, the customer pays while leaving, but there's a higher chance they might cheat you."* P-13 observed that for many merchants, the decision to skip confirmation is a calculated trade-off, explaining that *"sometimes it's not about trusting the customer, it's about saving time or the amount that is being paid. For example, if it's like a small amount or they have a lot of customers in their shop."* Fatigue was sometimes also a factor; P-15 admitted that rigorous checking is difficult to sustain, saying, *"Sometimes you're just tired or stressed and don't bother checking every time."*

Impact of Appearance. Absent established relationships, some participants admitted to relying on visual appearance to assess trustworthiness, a practice that could expose them to fraud. P-22 explicitly acknowledged judging customers based on physical presentation, stating that their decision to hand over a phone or trust a payment *"depends on how you see that person, if the person looks like others or a fraudster."* P-10 further noted that *"normally we think that a good-looking person wouldn't betray you."* P-15 recounted a specific incident of deceit facilitated by a customer's appearance: *"I once had a very respectable lady... she said her phone was dying... and said she'd paid. I continued, but later, when I checked, she hadn't paid."* In other words, fraudsters can sometimes exploit social biases regarding appearance.

Zero-Trust Policy. Twelve participants reported strict zero-trust policies due to the prevalence of scams. P-5 described adopting this stance following a previous theft, stating, *"No, we don't allow that anymore... Someone once came, bought items, and said 'look, I've paid'... but when I checked the balance, I realized no money had been received."* This sentiment was echoed by P-9, who bluntly stated, *"I can't risk it. If something goes wrong, I'm the one who pays."* Ultimately, P-20 concluded that due to an increase in deceit, *"there is no reason to trust anyone now that involves money."*

5.5 Challenges When Confirming Payments

Participants reported a diverse set of logistical challenges as key reasons merchants use customers' phones, rather than their own phones, to confirm payments.

Device Inaccessibility. Merchants often lack physical access to the phone that receives payment confirmation messages for two distinct reasons. The first is that the owner of the business, whose phone typically receives these messages, is not always present for a transaction. For instance, P-24 reported sometimes leaving her child to tend her kiosk alone. When asked how customers pay, she explained that after she receives a payment confirmation message, *"I call my child and tell them someone paid me."* However, foreshadowing one of our prototype alternative designs, she continued, *"But if we both got the messages at the same time, it would be good."* Current Rwandan MoMo systems do not support such an approach.

Network Latency. SMS delays create significant uncertainty about transaction completion. P-6 identified a critical gap: *"Sometimes after entering the PIN, you realize the transaction hasn't completed. They don't give immediate feedback... they just say the application is down."* This absence of feedback causes anxiety. P-7 described this anxiety as follows: *"If someone pays and immediately leaves without showing the SMS, you remain anxious and unsure."* Unfortunately, delayed messages were common. P-15 reported that *"out of six customers who pay me through MoMo, only three messages come in immediately."* P-9 added that instability often sows confusion as *"sometimes messages come out of order."* When the network lags, P-14 admitted they are forced to abandon their preferred checks: *"If they're rushing, I check on their phone."*

Customer Volume and Logistics. The busy nature of markets and stores further impedes verification. P-13, who runs a food stall, noted that during lunch hours, *"I have many customers waiting, and I have to give attention to the customers and not the phone."* As a result, during these busy hours he sometimes relies exclusively on hearing his phone beep upon message arrival without reading the message. P-11 highlighted that *"it's usually the customers who want to leave quickly, so they're the ones who show you that they've paid."*

In other cases, the logistical challenges of running a business kept a customer away from their phone. P-6 explained that when they are completing a transaction with a merchant whose phone is charging away from the counter, *"they ask me to show them [my confirmation message], so I show them the message and then move on."* In fact, P-11 quipped that in many shops, *"the merchant doesn't even know where their phone is,"* rendering verification impossible.

In contrast, some merchants felt that any signal that they received a message was sufficient, even if they did not inspect the confirmation message itself. For instance, P-7 said he would *"hear my phone beep"* and consider that auditory signal sufficient verification. Other moto taxi drivers reported that feeling the vibration while their phone was in their pocket was enough. Notably, moto taxi drivers often wear heavy gloves and carry their phone in a pocket, making it onerous to look for a visual confirmation message.

5.6 Key Concerns as Customers

In this section, we highlight the privacy, security, and safety concerns participants reported in their role as customers, alongside some of their workarounds. The current MTN MoMo interface displays the sender's full account balance on both the USSD and SMS payment confirmation screens they receive. As highlighted in Section 5.3, common workflows involve customers showing these screens to merchants when they make a payment, leading to their key privacy concern.

5.6.1 Key Privacy Concerns

Participants' privacy concerns in their role as a customer centered on a single piece of information: their account balance.

Involuntary Balance Exposure. Eleven participants expressed privacy concerns related to their account balance appearing on the payment confirmation messages they frequently showed merchants. As P-11 reported, *"Showing the message itself doesn't worry me, but I don't feel comfortable when the message also displays my account balance. I don't think merchants should see that."* P-6 reinforced the visibility problem, noting that SMS notifications reveal *"your new balance is this,"* recommending instead that messages should show balances *"only to authorized people without it always being visible so anyone could see how much money you have."* He also emphasized the effect of system delays: *"Sometimes SMS notifications delay, and you don't know if the payment really went through."* In these cases, customers needed to show their confirmation messages, which is *"not safe because others might see your balance."* P-13 echoed this concern, noting that confirmation messages revealing *"your MoMo balance"* cause discomfort.

Participants sometimes reported refusing to show merchants their confirmation messages to protect their privacy. P-3, a moto driver, described customers with high balances who *"won't show you his phone. Or he shows you his phone very quickly, like someone trying to hide something."* Even when SMS confirmation messages were delayed, P-2 avoided showing his phone unless pressed by insistent employees. In such situations, P-5 simply *"would just tell him that I paid."*

Some participants shared that they had few privacy concerns in their role as a customer. Instead, their main concerns related to security, as detailed in the next section. P-10 explained, *"I have no worries at all... Unless someone else happens to know my PIN... if you don't know it, I can leave you with my phone, no problem."* P-14 echoed this aspect: *"I wouldn't mind showing you my transaction history as long as you don't ask for my PIN. That's the most important thing."*

5.6.2 Key Security Concerns

Participants expressed two main concerns about security and safety in their role as customers of other merchants.

Shoulder Surfing. The act of shoulder surfing is when an adversary surreptitiously looks when a user is entering their PIN. Participants described shoulder surfing as a common threat during PIN entry, which is part of the MoMo transaction process. P-5 described a typical scenario: *"I stand there to pay but he watches all the numbers I press. When I show him the phone he could immediately memorize all the details... then he might hack and take the money or steal my phone."* P-13 echoed that *"typing the password and then someone tries to look... or they can even take your phone and then run with it"* were both concerns. Explaining how she hid her PIN during entry before sharing the payment confirmation message, P-5 said she would *"show him my phone, but not let him see too much information, only that I paid."*

Participants described PIN security as critical. As P-8 explained, *"I hide my password."* P-9 emphasized personal responsibility: *"The main issue is with the PIN. It's up to the person to keep it private. If no one knows your PIN, then there's no problem."* However, P-11 reported frequent attempts at shoulder surfing: *"Yes, it happens a lot. And if someone gets your secret number [your PIN] it's over because accessing your phone becomes very easy."* P-7 highlighted the extra risk *"when sending money or making a payment at a boutique... sometimes you worry that the merchant might have seen your secret PIN or that someone behind you might have seen your remaining balance."*

Potential for Theft. The frequency with which participants exposed their own account balances when showing merchants their confirmation messages fueled anxiety about theft. Notably, high balances were a signal of wealth. P-2 noted the risk: *"If you show someone [your phone's confirmation message], they might see the balance and think it's theirs."* P-5 called for a redesign of the MoMo payment confirmation workflow, explaining, *"It would be better if they improved the system so that when someone pays, the balance of your account would not show... only the payment message should appear without exposing my remaining balance."* P-6 elaborated, *"If I put [my phone] down, someone could look at it, see my messages, instantly know my balance, and try to take advantage of me or steal from me."* Interestingly, some participants reported higher anxiety with friends knowing their balance compared to strangers. P-14 explained, *"When you're in the neighborhood... someone I know, I definitely don't want them to know my MoMo information."* That said, strangers were also a worry. For instance, P-6 continued, *"Imagine showing [your full MoMo account balance] to someone untrustworthy who could harm you, thinking, 'That person has a lot of money; we'll get them later.' "*

5.7 Key Concerns as Merchants

In this section, we present concerns participants articulated in the primary role as merchants. Notably, participants did not report any major privacy concerns regarding their daily interactions with customers. While the MoMo interface does expose the merchant's full legal name to customers (as detailed in Section 5.3.3) and most business owners hope to keep their total balance private from their employees (a design constraint explored later in Section 6.4), participants' primary concerns were centered around transaction fraud.

Among our 30 participants, 24 reported having experienced fraud. For instance, P-9 reported that attempted fraud happens *"many times"* or even *"almost every day."* In qualitative analysis, we categorized these reports into five clusters: (i) spoofed confirmation messages; (ii) stopping the payment workflow before entering the PIN; (iii) abusing mechanisms for reversing transactions; (iv) social engineering like phishing; and (v) physical device compromise. P-5 acknowledged, *"We face [fraud] concerns quite often... we even know people who shared their testimonies with us, telling us how someone claimed they had paid when in fact they hadn't."* Fraud typically took one of the following five forms.

Spoofed Confirmations. Some fraudsters manipulate their SMS inbox to present fake proofs of payment. One approach involves editing or forwarding previous confirmation messages. P-11 described a case where a customer *"had a way of editing one message and sending it to another number that displayed 'Mobile Money completed'... so you see, the message someone sends to show they've paid can be edited by them."* P-7 similarly reported that *"when you forward a message, the merchant still sees the name and amount, so it looked real."* P-15 reported receiving a *"fake message that looked exactly like the real one... The message even had my name, but the balance shown didn't match mine."* Fraudsters also leverage static visual artifacts to trick merchants. P-20 reported instances where *"someone shows you a screenshot after buying items... and you think the money came."* P-12 shared that fraudsters *"take a screenshot showing that they are eligible to withdraw... cancel the transaction, take the screenshot from the other day, and show it to you again."*

Simulated Payment Actions. A common tactic involves customers starting a payment, yet intentionally canceling the transaction before completion. P-25 explained, *"Someone may show a message on their phone claiming they paid, but they never entered the PIN to complete the transaction... They just stop before confirming with the PIN and leave."* P-3, a moto taxi driver, described how a passenger *"would just press his phone as if he was sending money, then tell the driver the name registered on his SIM card... The driver would think the message is coming, then he would leave."* P-15 added that fraudsters often couple this strategy with urgency, such as claiming *"their phone is about to die."*

Fraudulent Reversals. Participants also reported some customers abusing the MoMo system's policies about reversing incorrect transactions. In these cases, the fraudster would pay legitimately, but then quickly contact MTN to reverse the transaction. P-2 described the fundamental risk: *"Someone may claim they sent money but didn't, or stop a payment claiming it was a mistake."* P-5 recounted one especially severe instance: *"He came like a normal customer... told me, 'Check, I have paid.' As he left, he managed to block the money transfer... After three days, I went to MTN to report the problem."* Unfortunately, P-14 described barriers to remediation, noting that *"If you look into the recovery process, you'll find the cost and that it takes a long time, so effectively the money is gone."*

Social Engineering. Participants reported fraudsters impersonating MTN staff or fabricating emergencies to trick victims into transferring funds. P-4 said, *"The fraudster lied to me and told me I had won 400,000 francs... He said, 'Press the star on your phone, then write the numbers I'll tell you'... I immediately realized he wanted me to dial those numbers so the money would go to him."* P-8 reported an impersonation attack: *"There's someone who calls me, and he told me that he's a guy calling from MTN Mobile Money and that he sent me 30,000, and I have to send it back to him."*

Physical Device Compromise. Some participants also reported strategies in which the fraudster would gain access to the victim's phone under false pretenses. For example, P-7, a moto taxi driver, explained, *"A passenger may borrow your phone pretending to make a call but instead goes into the MoMo menu. Since they don't know your PIN, they try several times, and your account gets locked."* P-3 shared how a businessman lent his phone to a fraudster who, *"instead of paying, they transferred 4 million to themselves."*

5.8 Experiences With Transaction Errors

Participants also raised concerns about transaction errors. These errors fell into two main categories: (i) sending money to an unintended recipient or (ii) transferring an incorrect amount. Around 70% of participants reported having made one or both of these errors in the past. Most incidents (95%) involved sending funds to the wrong recipient. For instance, P-6 *"entered one wrong digit, and the money went to someone else... I was supposed to enter 4 somewhere but I entered 7."*

Transferring incorrect amounts was similarly disruptive. P-13 described shock when realizing his mistake *"after receiving the message and seeing that 12,000 has been debited instead of 1,200."* The number of zeroes in typical Rwandan transactions contributes to the frequency of these errors; $1 USD is currently around 1,450 Rwandan Francs. For instance, as P-3 explained, *"Sometimes when paying 1,000 RWF, you may fear that you'll type it wrong and send 10,000 or even 100,000."* Furthermore, USSD MoMo transactions do not insert commas in all interfaces, creating a key usability gap.

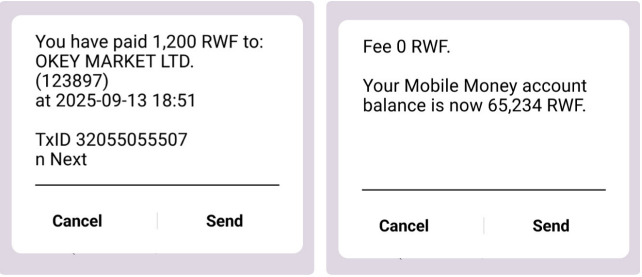


Figure 3: Prototype designs for a screen to show merchants (left) and the corresponding screen for customers (right).

6 Evaluating Alternate Interface Designs

Based on the team's experience, insights from the pilot study, and a literature review, we tested four alternative design concepts for MoMo payment confirmation workflows. We developed these alternatives through an iterative refinement process across multiple meetings. Our prototype designs aimed to address privacy, security, and usability concerns. In this section, we describe each concept we tested and detail participants' reactions during the interviews. We discarded some other designs we explored due to the additional cognitive effort and complex forms of human computation they would introduce. For example, we explored a concept design that required users to verify a derived value computed from the transaction information (such as the balance or timestamp). However, we concluded that this approach would likely be too burdensome.

6.1 Dedicated Screen to Show Merchants

Design Goals. To address the privacy and safety risks of exposing customers' account balances, we designed a confirmation dialog that separates transaction details from private account data. This design (Figure 3) splits the existing confirmation message for customers into a first screen with public data to show merchants and a second screen with private data (the account balance) for only the customer.

Participant Reactions. When presented with this alternative, 20 of the 30 participants strongly supported removing the balance from the initial verification screen. For instance, as P-11 explained, *"The message [for merchants] displays the amount paid, the names, and the time of payment. I find that to be enough."* This public screen supports merchant verification, while sensitive information is moved to a secondary private screen. While the overall response was positive, five participants raised doubts about whether the lack of a visible balance change might make it harder to trust the transaction since some participants used that information as a signaling mechanism. As P-15 questioned, *"As a merchant, I might wonder... if I don't see a decrease in their balance, how do I know they really paid?"*

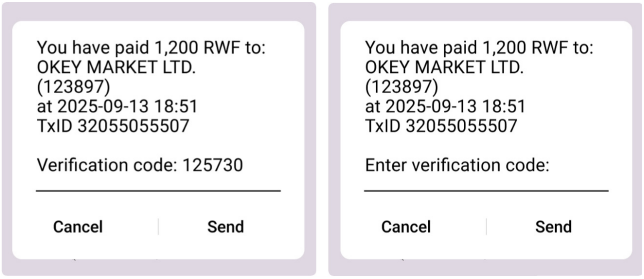


Figure 4: Prototype designs for non-interactive secret validation (left) and interactive secret validation (right).

6.2 Non-Interactive Secret Validation

Design Goals. To address the threat of fraudsters showing merchants a screenshot of a past—or fabricated—confirmation message (Section 5.7), we prototyped a design that embeds a merchant-defined secret directly into the USSD confirmation dialog. In this model, merchants set a short code that appears as part of the payment confirmation message on the customer's screen (Figure 4, left). In essence, this design introduces a freshness token [4]. If changed frequently, this token makes it harder for fraudsters to present a screenshot of an old message. If sufficiently unpredictable, this token also makes it harder to fabricate confirmation messages without having interacted with the merchant in the past.

Participant Reactions. A significant majority of participants (24 out of 30) supported this design as a practical way to stop fraud. P-11 expressed confidence that *"with this method, no one would be able to use an old screenshot."* P-13 emphasized that *"because the secret changes, a fraudster will not be able to use the screenshots from yesterday."* Notably, 18 participants specifically highlighted the freshness of the code as its most valuable security feature.

Beyond fraud prevention, 10 participants mentioned that a succinct secret would make checking payments faster by letting them look for a simple code instead of reading every detail on the screen. For instance, P-5 explained, *"You'd just check what you already know you set, without needing to look at too many details."* However, eight participants worried about the complexity of managing these secrets. P-15 cautioned *"it would be hard for an older woman in the village to understand."* While promising, these responses emphasize the need to balance security with usability in practical settings.

6.3 Interactive Secret Validation

Design Goals. Even more secure than a relatively static secret would be some sort of interactive workflow that requires a merchant to enter a verification code directly on the customer's device (Figure 4, right). The simplest design might involve a relatively static secret; the USSD workflow would be modified so that the payment confirmation is only shown when the correct secret is entered. For the purpose of our prototype, we left the precise implementation ambiguous, testing primarily how participants would feel about customers handing their phones to merchants. We discuss further security considerations (e.g., resisting keyloggers) and even more interactive human computation techniques in Section 7.

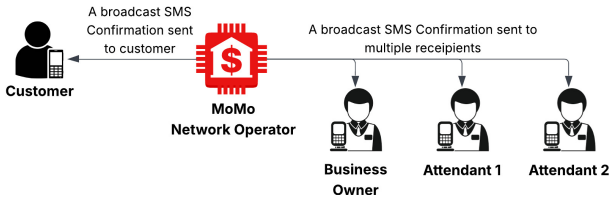


Figure 5: Prototype multi-recipient notification architecture.

Participant Reactions. Participants observed that this active input makes confirmation messages even harder to fake. P-12 said, *"It would solve the problem of people who just ask for the code, cancel the transaction, and then claim it went through."* P-13 added, *"Because it's only the merchant who knows the validation code, there's no way someone can say I sent money and they didn't receive the message."*

However, most participants felt the logistical and social costs would outweigh these security benefits. Specifically, 14 participants cited efficiency as a roadblock since handling devices would slow down work in busy markets. As P-6 articulated, *"If I had to handle the transaction for each customer, it would slow down operations."* P-13 simply characterized the approach as *"not feasible"* for a solo merchant. Furthermore, 12 participants flagged social risks of device handover. P-15 wondered, *"How many people would agree to give you their phone? Customers are often afraid... that could cause conflicts."* P-10 explicitly rejected the idea due to safety, explaining, *"Customers cannot trust to give you their phone... I wouldn't give it to anyone because in the past, there was theft when someone got your PIN."* Due to such points of friction, only six participants were willing to adopt this approach.

6.4 Multi-Recipient Notifications

Design Goals. While the previous three prototypes aimed to solve the various barriers to merchants confirming payments by redesigning the notifications customers receive, our fourth prototype took a different approach. To address the specific problem of payment confirmation messages going to the phone of the business owner, rather than the employee interacting with the customer, we explored a design that would enable real-time payment alerts to be sent to multiple people (Figure 5). This is a major issue in practice: 18 participants reported that business owners currently either have to leave their phone at their shop or rely on employees checking the customer's device to keep the business running while they are

away. We imagine a workflow in which a business owner can add the phone numbers of employees to their MoMo account for the sole purpose of receiving payment confirmation messages. We discuss logistical issues of doing so in Section 7.

Participant Reactions. Support for this feature was very high, with 26 participants identifying it as promising. As P-18 explained, employees *"would know they were paid without asking me if I was paid."* P-13 emphasized how *"it will help in tracking and controlling what goes in and out of the account."* Additionally, 10 participants believed this shared visibility would reduce mistakes and internal theft. P-8 said it would make her feel more *"safe"* because the employee is *"sure what she's getting."* Participants also anticipated some additional benefits. As P-24 noted, *"If the employee also sees the message while selling... we would be able to sell more."*

Despite the benefits, participants expressed concern about the line between work and home life. Specifically, they wanted to be able to turn these messages on and off as appropriate. Relatedly, 20 participants said they would never use this for personal transactions (e.g., to share messages with family members) because of the risk of social tension or unexpected scrutiny. As P-15 explained, *"For a company, that would be fine. For an individual, it wouldn't be good."*

The privacy of the business owner's financial information was an additional consideration. Seven participants explicitly noted that employees should be able to see the proof of payment, but never the business's total account balance. Finally, participants noted that the system must have strong management tools, with P-2 stating it is only acceptable *"as long as the business owner can control who receives it."*

7 Discussion

Our qualitative investigation demonstrated that Rwandan businesses' method of confirming MoMo payments from customers in practice differs from the system's intended usage, causing both security and privacy issues. From a traditional security perspective, a merchant should treat a customer's phone as fully untrusted, yet this is not what happened in practice. Furthermore, many merchants reported examining artifacts on customers' phones that are trivial to spoof (e.g., MTN's "y'ello" greeting for SMS confirmations, the SMS contact name being "M-Money"). In fact, it would be easy for an app developer to automatically generate fake—yet convincing—payment confirmation messages. Nevertheless, while many participants had experienced MoMo fraud, such fraud was relatively uncommon in part due to societal trust relationships.

Alternative Architectures. In many Western countries [13], as well as in many non-Western countries like India [12] and China [18, 36], mobile payment systems do not have the same potential for fraud since point-of-sale (POS) systems are widely used [8]. These POS systems give merchants a secure interface for confirming payment without needing to rely on their phones. Unfortunately, the cost of deploying a POS terminal is non-trivial for Rwandans. Further, Rwandan MoMo systems do not yet integrate with POS terminals. Instead, Rwandan business owners often rely on their personal phone as their sole portal to their business's MoMo transactions.

We speculatively investigated an alternative architecture in which business owners would register employees to receive payment confirmation messages on their own phones. While participants responded positively to this idea, the nuances are critical. Participants emphasized that messages sent to employees should not include a business's account balance. Further, employees must be able to easily turn these messages on (when they are at work) and off. Business owners also need to revoke former employees' access. The direct cost to business owners and employees would be minimal.

Alternative Interfaces. We also investigated how to redesign customers' payment confirmation pop-ups to support how they are used in practice. There was near consensus on splitting customers' confirmation message across two screens: one to show merchants and another to tell the customer their account balance. Some merchants expressed hesitation about removing the customer's account balance from the public-facing screen, most likely because the visible balance was a useful indicator of authenticity. However, we argue that the reliance on viewing a customer's balance provides a false sense of security. The merchant has no knowledge of the customer's previous balance to mathematically verify a true deduction, and a spoofed confirmation message could trivially include a fabricated balance. Therefore, removing the balance from the merchant-facing screen significantly improves buyer privacy without degrading the actual security of the transaction.

Overall, participants reacted positively to the idea of adding a merchant-defined secret to customers' payment confirmation messages, but negatively to having customers hand their phones to merchants. Again, the nuances are critical. Open questions include how often such a secret would need to change to maintain freshness, whether some sort of human computation [5, 44] could dynamically bind the specific transaction details to the secret, and whether an alternative interactive approach might be better received. In any case, our work uncovered opportunities for redesigning MoMo payment confirmation workflows to reflect the unique constraints of Rwanda, and Sub-Saharan Africa in general. Regardless, participants overall felt that adding a transaction timestamp (not included in the body of confirmation messages currently sent to customers) was an important enhancement that would make naive replay attacks (e.g., screenshots) more difficult.

Generalizability. We studied the MoMo ecosystem in Rwanda. However, the underlying insights likely apply to other MoMo providers across Africa (e.g., Safaricom's M-Pesa, Orange Money). Conceptually, these platforms share a common underlying system reliant on interactive USSD sessions [32]. As systems have distinct operational variations, further studies are needed to understand all risks and threats.

Ethical Considerations

We developed our research protocol in accordance with institutional ethical standards to ensure the protection of all participants. We obtained approval for the study from both Carnegie Mellon University's IRB and the Rwandan National Ethics Committee (RNEC) before starting recruitment. RNEC is the primary body responsible for reviewing human-subjects research in Rwanda. It audits study records and documentation to ensure compliance with national ethical mandates.

Key stakeholders in our research include MoMo users (merchants, customers, and agents), policymakers, telecom providers, and financial institutions. We discuss the measures we took to protect the welfare of each group in turn:

- `Participants`: We interviewed a diverse set of 30 participants, including business owners, managers, employees, and MoMo Agents across both urban and rural regions of Rwanda. The dominant harm from which we aimed to protect the participants was re-identification based on the information provided during the interview. As a result, we collected only the minimum information needed to conduct the study and process participants' compensation. To minimize harm, our research team ensured interviews were conducted at a convenient location free from distractions. We also offered the option (not taken by any participants) of a WhatsApp call instead. We also ensured that specific information about their place of employment was not recorded or revealed mistakenly. We recorded our data using pseudonyms (see Table 2). All audio recordings were deleted after transcription. Additionally, participants were compensated 7,500 RWF, which we carefully benchmarked to the approximate cost of an entrée at a mid-range restaurant to provide a meaningful incentive without being coercive.
- `Regulators or Policy Makers`: We aim to provide regulatory bodies, such as the National Bank of Rwanda (BNR) and the Rwanda Utilities Regulatory Authority (RURA), with data to refine the current frameworks to improve user safety. In our study, we also highlight how current practices facilitate social engineering and advocate for improvements that protect users.
- `Telecom Providers (MTN and Airtel)`: We have already begun meeting with Rwanda's main MoMo telecommunications provider (MTN) to responsibly disclose our findings. Our study aims to maximize the long-term benefit for MoMo service providers across the continent (e.g., M-PESA, Tigo PESA, and Orange Money) by identifying vulnerabilities within MoMo user interfaces. We are committed to a process of responsible disclosure, sharing our findings and proposed design improvements with MTN. Our analyses centered on understanding human workarounds to ensure the results can be used constructively to improve the MoMo platform. A potential secondary harm of our study was the potential to sow distrust in these companies' MoMo services among potential users in Rwanda. We aimed to strike a balance on this topic. We wanted to make participants aware of the potential for MoMo fraud, but not to cause them inappropriate or undue concern.
- `Financial Institutions`: Our research benefits the broader financial ecosystem by investigating issues within MoMo, which is tightly integrated with the banking systems in Rwanda. We propose alternate designs to reduce the incidence of fraud during payment confirmation. This will aim to minimize financial risk for financial institutions like the National Bank of Rwanda (NBR) and their customers.

Ultimately, the core objective of this research is ethically motivated: to identify and address security and privacy vulnerabilities in MoMo payment confirmation screens with the goal of improving safety for users in Rwanda.

Use of Phone Numbers: To compensate participants via MoMo, it was necessary to use participants' phone numbers; there is no alternative way of specifying the recipient for Rwandan MoMo services. We used these phone numbers only for processing participants' compensation for the study. Our university required us to take screenshots of the payment confirmation messages as a proof of payment in order to process reimbursements. Once we took such screenshots, we deleted the SMS confirmation messages from our phones. Once these screenshots were processed by our university, we also deleted the screenshots.

Use of WhatsApp: As noted above, we offered participants the option to conduct the interview over WhatsApp at a later time if they preferred. None of the participants chose this option. In other words, all participants chose to conduct the interview in person.

As is common in Rwanda, the members of the research team coordinated meetings with each other over WhatsApp. We took care to ensure that no participant data was ever sent over WhatsApp. In other words, not even de-identified participant data was ever sent over WhatsApp.

Justification for Research: We determined that because vulnerable merchants actively suffer financial loss, it constitutes a greater ethical violation than the risk of publication. Furthermore, because the vulnerabilities identified are rooted primarily in usability flaws, rather than technical exploits, keeping them secret will not prevent further attacks, but only delay necessary interventions. By adhering to the rigorous protocol of responsible disclosure with MTN, we concluded that the research serves the public interest.

Respect for Peer Reviewers: The entire manuscript was originally written by human authors. However, the non-native English speakers used generative AI to correct their grammar in some areas. We also used generative AI to modify a few figures, as disclosed in the respective figures' captions.

Open Science

To promote replication, transparency, and enable evaluation of our contributions, we make the materials used in this study publicly available. All artifacts listed below are available permanently in the following Zenodo open science repository: https://zenodo.org/records/20314699

The repository contains the following separate folders, with content in English and Kinyarwanda where applicable:

- `Recruitment Script`: A guide to ask individuals to participate in the interview, explain the interview process and the outcomes, and assess their eligibility.
- `Interview Guide`: The full semi-structured interview guide used in the study, including all prompts.
- `Mockup Interfaces for Interviews`: Images of the prototype interfaces shown to study participants during interviews. These interfaces present key design approaches we tested during the interviews.
- `Interview Codebook`: The final codebook used for analysis, including code definitions and sample quotes.
- `Figma assets`: A .zip archive of the asset files we designed in Figma for our proposed interfaces and other design assets used in the study. The unzipped folder contains the Figma .fig file, along with the exported screens in a separate images folder.

Materials Not Shared: In compliance with our institutional policies, RNEC policies, and privacy obligations to safeguard participant information, raw interview transcripts are not publicly shared. Furthermore, audio recordings have been deleted. These materials contain potentially identifying information that cannot be fully de-identified without compromising participant confidentiality and risking re-identification.

Acknowledgments

We thank Jean Pierre Imanirumva for helping with initial interviews, the Upanzi Network and CMU-Africa communities for feedback on our protocol, and the UChicago Provost's Global Faculty Award: Sub-Saharan Africa for financial assistance. We are very grateful to our participants and pilot participants.

References

[1] Mendel Adongo. Mobile money social engineering attacks in African countries: A survey. *SSRN*, Apr. 2025. https://doi.org/10.2139/ssrn.5257020.

[2] Airtel Rwanda. Airtel Money frequently asked questions (FAQs). https://www.airtel.co.rw/airtelmoney/faq. Accessed: Jan. 6, 2026.

[3] Guma Ali, Mussa Ally Dida, and Anael Elikana Sam. Evaluation of key security issues associated with mobile money systems in Uganda. *Information*, 11(6), 2020. https://www.mdpi.com/2078-2489/11/6/309.

[4] Mihir Bellare and Björn Tackmann. Nonce-based cryptography: Retaining security when randomness fails. In *Proceedings of EUROCRYPT*, 2016. https://doi.org/10.1007/978-3-662-49890-3_28.

[5] Manuel Blum and Vempala Santosh. The complexity of human computation via a concrete model with an application to passwords. *Proc. Natl. Acad. Sci.*, 117(17):9208–9215, 2020. https://doi.org/10.1073/pnas.1801839117.

[6] Jasmine Bowers, Bradley Reaves, Imani N. Sherman, Patrick Traynor, and Kevin Butler. Regulators, mount up! Analysis of privacy policies for mobile money services. In *Proceedings of the Thirteenth Symposium on Usable Privacy and Security*, 2017. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/bowers.

[7] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, 2006. https://doi.org/10.1191/1478088706qp063oa.

[8] Sam Castle, Fahad Pervaiz, Galen Weld, Franziska Roesner, and Richard Anderson. Let's talk money: Evaluating the security challenges of mobile money in the developing world. In *Proceedings of the 7th Annual Symposium on Computing for Development*, 2016. https://dl.acm.org/doi/pdf/10.1145/3001913.3001919.

[9] Barry Chametzky. Coding in classic grounded theory: I've done an interview; now what? *Sociology Mind*, 6(4):163–172, Oct. 2016. https://doi.org/10.4236/sm.2016.64014.

[10] Kaouthar Chetioui, Birom Bah, Abderrahim Ouali Alami, and Ayoub Bahnasse. Overview of social engineering attacks on social networks. *Procedia Computer Science*, 198:656–661, 2022. https://doi.org/10.1016/j.procs.2021.12.302.

[11] Asli Demirgüç-Kunt, Leora Klapper, Dorothe Singer, and Saniya Ansar. The Global Findex Database 2021: Financial inclusion, digital payments, and resilience in the age of COVID-19, 2022. https://openknowledge.worldbank.org/handle/10986/37578.

[12] Derryl D'Silva, Zuzana Filková, Frank Packer, and Siddharth Tiwari. The design of digital financial infrastructure: Lessons from India. BIS Papers 106, Bank for International Settlements, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3505373.

[13] GSMA. The state of the industry report on mobile money 2024. Technical report, GSM Association, 2024. https://www.gsma.com/sotir/.

[14] Ali Guma, Mussa Dida, and Anael Sam. A secure and efficient multi-factor authentication algorithm for mobile money applications. *Future Internet*, 13:1–31, Nov. 2021. https://doi.org/10.3390/fi13120299.

[15] Gunnar Harboe and Elaine M. Huang. Real-world affinity diagramming practices: Bridging the paper-digital gap. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2015. https://doi.org/10.1145/2702123.2702561.

[16] Ayako A. Hasegawa, Daisuke Inoue, and Mitsuaki Akiyama. How WEIRD is usable privacy and security research? In *Proceedings of the 33rd USENIX Security Symposium*, 2024. https://www.usenix.org/conference/usenixsecurity24/presentation/hasegawa.

[17] Claire Hayworth and Moïse Bigirimana. The closing of the mobile money gender gap in Rwanda. FinDev Gateway Blog, July 2025. https://www.findevgateway.org/blog/2025/07/closing-of-mobile-money-gender-gap-in-rwanda.

[18] Changyang He, Lu He, Zhicong Lu, and Bo Li. "i have to use my son's QR code to run the business": Unpacking senior street vendors' challenges in mobile money collection in China. *Proc. ACM Hum.-Comput. Interact*, 7(CSCW1), Apr. 2023. https://doi.org/10.1145/3579493.

[19] Lindah Kotut and Hummd Alikhan. "Things on the ground are different": Utility, survival and ethics in multi-device ownership and smartphone sharing contexts. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, 2024. https://doi.org/10.1145/3613904.3642874.

[20] Zaynab Lamoyero and Oluwatobi Fajana. Exposed: Critical vulnerabilities in USSD banking authentication protocols. In *Prcoeedings of the 2023 IEEE International Conference on Cyber Security and Resilience*, 2023. https://doi.org/10.1109/CSR57506.2023.10224933.

[21] Arisema Mezgebe Mihretu, Joseph Mdumuka, Maxmillian Shetto, Ofentse Phuti Rice, Patrick Iradukunda, Tunga Tessema Chamisso, Victor Mwangi, and Yves Byiringiro. Effective mitigation strategies for social engineering attacks in mobile money services: A case study in Kenya. In *Proceedings of IEEE Africon*, 2023. https://doi.org/10.1109/AFRICON55910.2023.10293606.

[22] MTN Rwanda. MoMo terms & conditions. https://www.mtn.co.rw/terms-condtions/, 2025. Accessed: Jan. 6, 2026.

[23] MTN Rwandacell Plc. Annual integrated report 2025. https://www.mtn.co.rw/wp-content/uploads/2026/06/MTN-Rwandacell-Plc-2025-Integrated-Annual-Report.pdf, 2025.

[24] Collins W. Munyendo, Yasemin Acar, and Adam J. Aviv. "Desperate times call for desperate measures": User concerns with mobile loan apps in Kenya. In *Proceedings of the 43rd IEEE Symposium on Security and Privacy*, 2022. https://doi.org/10.1109/SP46214.2022.9833659.

[25] Collins W. Munyendo, Yasemin Acar, and Adam J. Aviv. "In eighty percent of the cases, I select the password for them": Security and privacy challenges, advice, and opportunities at cybercafes in Kenya. In *Proceedings of the 44th IEEE Symposium on Security and Privacy*, 2023. https://doi.org/10.1109/SP46215.2023.10179426.

[26] Collins W. Munyendo, Kentrell Owens, Faith Strong, Shaoqi Wang, Adam J. Aviv, Tadayoshi Kohno, and Franziska Roesner. "You have to ignore the dangers": User perceptions of the security and privacy benefits of WhatsApp mods. In *Proceedings of the 46th IEEE Symposium on Security and Privacy*, 2025. https://doi.org/10.1109/SP61157.2025.00087.

[27] National Institute of Statistics of Rwanda. FinScope Survey (2024) . https://www.statistics.gov.rw/statistical-publications/business-establishment-finance-trade/finscope-survey-2024, 2024.

[28] Catherine Njogu, Furaha Benedict, Susan Muthoni, Marie Noelle Kanyamuneza, Evalyne Lwoba, Everlyn Musembi, Yussuf Papy, and Edwin Kairu. Security gaps in the mobile money system in Rwanda: Challenges, risks and mitigation. In *Proceedings of the Science and Information Conference*, 2024. https://doi.org/10.1007/978-3-031-62277-9_42.

[29] Alima Nzeket Njoya, Franklin Tchakounté, Marcellin Atemkeng, Kapila P. Udagepola, and Didier Bassolé. Mobile money phishing cybercrimes: Vulnerabilities, taxonomies, characterization from an investigation in Cameroon. In *Proceedings of the 14th EAI International Conference on Towards New e-Infrastructure and e-Services for Developing Countries*, 2022. https://doi.org/10.1007/978-3-031-34896-9_26.

[30] Daniel Adjei Odai. The price of transparency: How exposing personal information in mobile money transactions fuels social engineering in Ghana. *Texila International Journal of Academic Research*, 12(1), 2025. https://www.academia.edu/127378336/The_Price_of_Transparency_How_Exposing_Personal_Information_in_Mobile_Money_Transactions_Fuels_Social_Engineering_in_Ghana.

[31] Bradley Reaves, Jasmine Bowers, Nolen Scaife, Adam Bates, Arnav Bhartiya, Patrick Traynor, and Kevin R. B. Butler. Mo(bile) money, mo(bile) problems: Analysis of branchless banking applications. *ACM Trans. Priv. Secur.*, Aug. 2017. https://doi.org/10.1145/3092368.

[32] Mats Renée, Firooz Badiee, Erwin van Rijssen, and Patrik Centellini. A converged approach to mobile financial services. Technical report, Ericsson, Nov. 2012. https://www.ericsson.com/4ac619/assets/local/reports-papers/ericsson-technology-review/docs/2012/er-ng-m-commerce.pdf.

[33] Rwanda Information Society Authority. Rwanda unveils three transformative innovations to advance digital finance and inclusion at IFF2025, 2025. https://www.risa.gov.rw/news-detail/rwanda-unveils-three-transformative-innovations-to-advance-digital-finance-and-inclusion-at-iff2025.

[34] Rwanda Utilities Regulatory Authority. ICT sector statistics report: Second quarter of the year 2025. https://www.rura.rw/fileadmin/user_upload/RURA/Documents/Sectors/ICT/Statistics/Quarterly_publication/ICT_Sector_Statistics_Report_as_of_second_Quarter_of_the_year_2025-R.pdf, 2025.

[35] Sectona. RSwitch uses sectona PAM for secure transaction processing, in line with the RNDPS, 2024. https://sectona.com/wp-content/uploads/2024/05/Sectona_Customer_Story-Finance-RSwitch.pdf.

[36] Hong Shen, Cori Faklaris, Haojian Jin, Laura Dabbish, and Jason I. Hong. 'I can't even buy apples if i don't use mobile pay?': When mobile payments become infrastructural in China. *Proc. ACM Hum.-Comput. Interact.*, 4(CSCW2), 2020. https://doi.org/10.1145/3415241.

[37] Dorothe Singer, Asli Demirgüç-Kunt, Peter Van Oudheusden, and Leora Klapper. The Global Findex Database 2014: Measuring financial inclusion around the world. Policy research working paper 7255, World Bank Group, 2015. https://doi.org/10.1596/1813-9450-7255.

[38] Karen Sowon, Edith Luhanga, Lorrie Faith Cranor, Giulia Fanti, Conrad Tucker, and Assane Gueye. The role of user-agent interactions on mobile money practices in Kenya and Tanzania. In *Proceedings of the 45th IEEE Symposium on Security and Privacy*, 2024. https://doi.org/10.1109/SP54263.2024.00184.

[39] Karen Sowon, Collins W. Munyendo, Lily Klucinec, Eunice Maingi, Gerald Suleh, Lorrie Faith Cranor, Giulia Fanti, Conrad Tucker, and Assane Gueye. Design and evaluation of privacy-preserving protocols for agent-facilitated mobile money services in Kenya. In *Proceedings of the Twenty-First Symposium on Usable Privacy and Security*, 2025. https://www.usenix.org/conference/soups2025/presentation/sowon.

[40] Emmanuel Tweneboah, Collins W. Munyendo, and Yixin Zou. "No, I can't be a security personnel on your phone": Security and privacy threats from sharing infrastructure in rural Ghana. In *Proceedings of the 34th USENIX Security Symposium*, 2025. https://www.usenix.org/conference/usenixsecurity25/presentation/tweneboah.

[41] Blase Ur, Manya Sleeper, and Lorrie Faith Cranor. {Privacy, Privacidad, Приватност} policies in social media: Providing translated privacy notice. In *Proceedings of the 1st Workshop on Privacy and Security in Online Social Media*, 2012. https://doi.org/10.1145/2185354.2185360.

[42] Blase Ur and Yang Wang. A cross-cultural framework for protecting user privacy in online social media. In *Proceedings of the 2nd Workshop on Privacy and Security in Online Social Media (WWW '13 Companion)*, 2013. https://doi.org/10.1145/2487788.2488037.

[43] WageIndicator. Minimum wage – Rwanda. https://wageindicator.org/en-rw/work-in-rwanda/minimum-wage. Accessed: June 11, 2026.

[44] Yang Xiao, Chung-Chih Li, Ming Lei, and Susan V. Vrbsky. Differentiated virtual passwords, secret little functions, and codebooks for protecting users from password theft. *IEEE Systems Journal*, 8(2):406–416, 2014. https://doi.org/10.1109/JSYST.2012.2183755.

Appendix

A Additional Figures

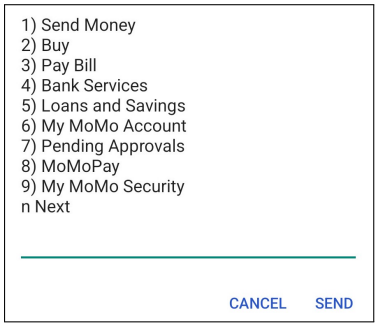


Figure 6: The MTN MoMo USSD menu, which appears after entering *182# on a phone with an MTN SIM card.



Figure 7: A user can simply enter the short code shown in this figure, inserting the individual recipient's phone number, to skip the menu shown in Figure 6. To pay a business using MoMoPay, the user would instead use a *182*8*1 prefix.



Figure 8: A user can also enter the amount directly in the dialer to avoid the step shown in Figure 9.

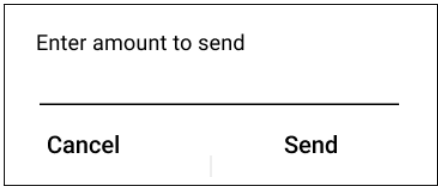


Figure 9: MoMo USSD dialog for amount.

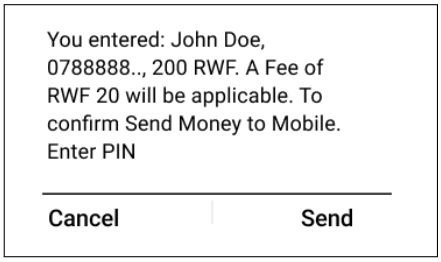


Figure 10: MoMo USSD dialog for PIN.



Figure 11: An uncropped version of Figure 1c from the body of the paper. *Note: We used generative AI to transform photographs we took of our own basic phone into an abstract representation with more legible text.*

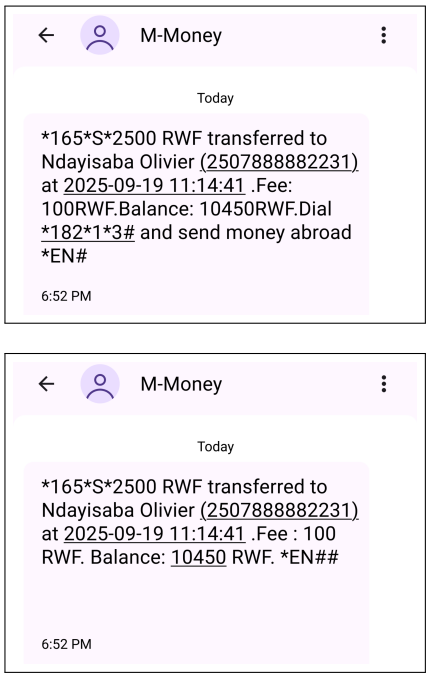


Figure 12: Figure 1b in the body of the paper presented a Figma mockup of a typical MTN MoMo payment confirmation SMS received by members of the research team. This figure shows two other versions observed during the research period. We hypothesize the changes in wording are due to MTN modifying the messages in the field. Typos and formatting peculiarities mirror the messages received in practice.

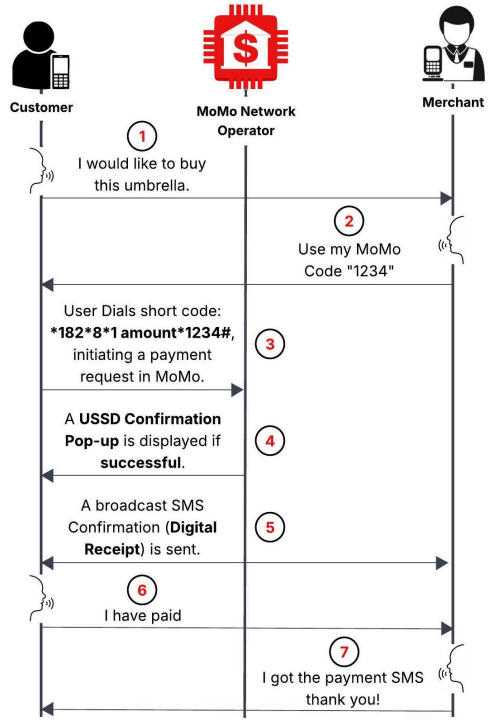


Figure 13: Standard payment workflow for MoMo.

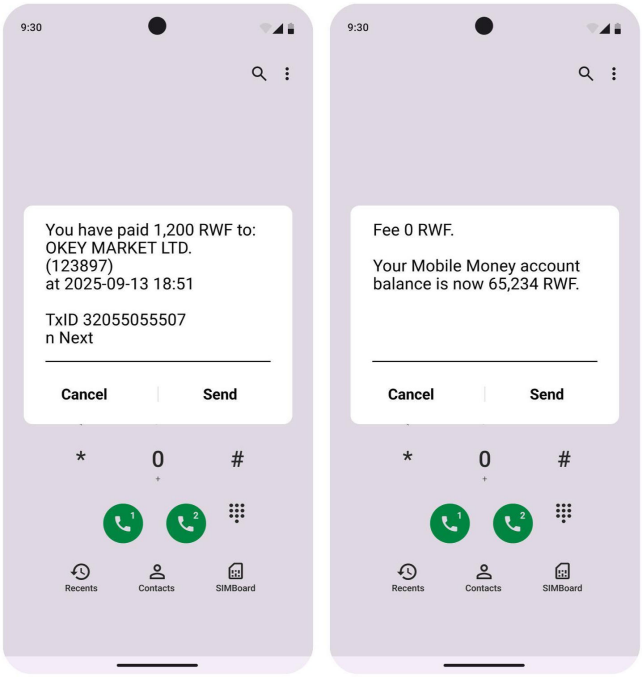


Figure 14: An uncropped version of Figure 3 from the body of the paper showing prototype designs for a screen to show merchants (left) and the corresponding screen for customers (right) containing their account balance.

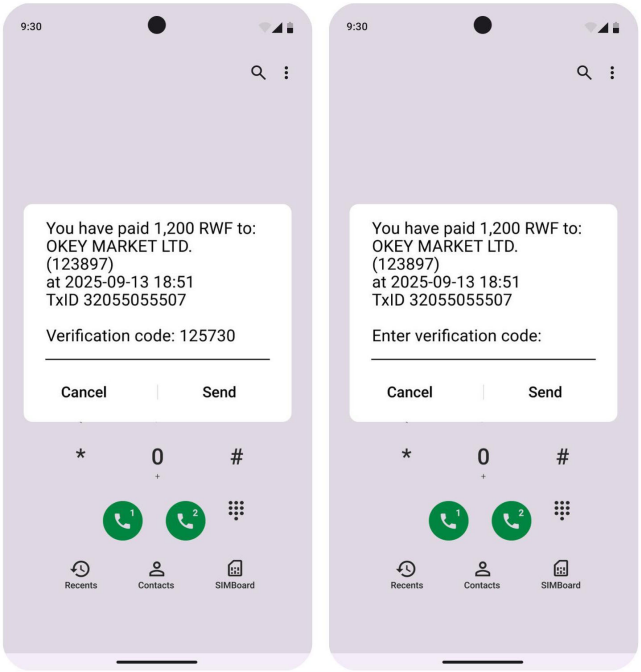


Figure 15: An uncropped version of Figure 4 from the body of the paper showing prototype designs for non-interactive secret validation (left) and interactive secret validation (right).