

Design and Evaluation of Privacy-Preserving Protocols for Agent-Facilitated Mobile Money Services in Kenya

Karen Sowon*, Collins W. Munyendo†, Lily Klucinec*, Eunice Maingi‡, Gerald Suleh‡,
Lorrie Faith Cranor*, Giulia Fanti*, Conrad Tucker§ and Assane Gueye§

* Carnegie Mellon University

† The George Washington University

‡ Strathmore University

§ Carnegie Mellon University-Africa

Abstract—Mobile Money (MoMo), a technology that allows users to complete digital financial transactions using a mobile phone without requiring a bank account, has become a common method for processing financial transactions in Africa and other developing regions. Operationally, users can deposit (exchange cash for mobile money tokens) and withdraw with the help of human agents who facilitate a near end-to-end process from customer onboarding to authentication and recourse. During deposit and withdraw operations, know-your-customer (KYC) processes require agents to access and verify customer information such as name and ID number, which can introduce privacy and security risks. In this work, we design alternative protocols for mobile money deposits/withdrawals that protect users’ privacy while enabling KYC checks. These workflows redirect the flow of sensitive information from the agent to the MoMo provider, thus allowing the agent to facilitate transactions without accessing a customer’s personal information. We evaluate the usability and efficiency of our proposed protocols in a role play and semi-structured interview study with 32 users and 15 agents in Kenya. We find that users and agents both generally appear to prefer the new protocols, due in part to convenient and efficient verification using biometrics, better data privacy and access control, as well as better security mechanisms for delegated transactions. Our results also highlight some challenges and limitations that suggest the need for more work to build deployable solutions.

1. Introduction

Mobile money (MoMo) is a technology that allows mobile phone users to exchange and store money using their phones and associated phone number, without the need for a traditional financial account [1], [2]. MoMo has re-imagined digital transactions in many emerging economies [3], e.g., sub-Saharan Africa where the majority of the unbanked reside [4]. MoMo transactions are executed via simple technologies, typically SMS, USSD, and a SIM-resident

application suitable to both basic phones¹ and smartphones.

To safeguard MoMo transactions, regulations in most jurisdictions mandate that financial institutions acquire proof of customer identity before transacting, a process known as “know your customer” or KYC [5], [6], [7]. The MoMo providers—usually, but not always, telecommunications companies (telcos)—are responsible for ensuring KYC processes are completed for their users. However, authorized third-party agents acting as last-mile service providers often assist in the KYC process, handling sensitive user data [8].

In addition to the inefficiency and inconvenience of KYC mechanisms, the involvement of agents brings heightened privacy concerns as agents access sensitive information that may disclose details about the volume and recipients of individual transactions, their habits, social connections, and personally-identifiable information (PII). Prior work shows that users are concerned about potentially malicious practices of agents, including illegal use of customer data to register additional SIM cards [8]. In pursuit of privacy, some users adopt practices such as using SIM cards registered in another person’s name [9], creating challenges for compliance with KYC policies. Further, recent data protection laws in several African countries including Kenya [10] mandate that individuals handling private user data protect PII via measures like data minimization and data retention limits [11]. Unfortunately, most agents are not equipped with the skills necessary to protect users’ data as mandated by these laws, putting them and their businesses at risk.

Privacy concerns have been widely discussed in digital ID communities; proposed solutions make use of techniques like verifiable credentials (VCs) [12], [13]. While VCs can achieve a privacy-preserving solution (see Section 3), they do not define a way to interface with MoMo. For example, even if the agent was able to verify the user’s VC, they would still have no way of knowing how much money to give/take from the user or whether they had any money in their wallet, as this requires the intervention of the telco. Similarly, the literature on digital payments has seen signif-

1. Basic phones, also known as feature phones, mainly have call and text features and cost as little as \$10. Some may allow basic internet and email access, but most cannot download apps from an online marketplace.

icant advances in privacy preservation techniques to address the challenges of safeguarding user data while ensuring the efficiency and usability of payment systems [14], [15], [16]. However, most of these solutions, including homomorphic encryption [17] and Zero-Knowledge Proofs (ZKPs) [18], [19], are impractical for less sophisticated devices such as basic phones that are widely used for MoMo.

The goal of this study is to design and test alternative privacy-preserving KYC protocols that are practical in the context of MoMo. To this end, we design a suite of protocols that allow MoMo users to deposit (cash-in) and withdraw (cash-out) while minimizing the exposure of users' personal data to the agents. This also removes the burden of protecting users' PII from the agents.

Our new protocols redirect sensitive data flows from agents—who conduct KYC checks today—to the MoMo provider; our findings (Section 5) suggest that users generally trust telcos with sensitive data more than agents. Users of the new protocol authenticate themselves to a digital ID service using biometrics, either on the user's own smartphone or using already-deployed voice authentication tools for basic phones [20]. Users then share the authentication certificate with the telco, which provides a one-time code to the agent and the user. This code is used to confirm identity, and allows the agent to transfer or collect cash from the user. We also extend our protocols to delegated withdrawal, which is a common use case (e.g., a user sends her friend to withdraw cash at an agent). The main design challenges were to make the protocols usable and compatible with resource-constrained devices (i.e., basic phones), and efficient (i.e., minimizing communication costs).

After designing these alternative KYC protocols, we investigate the following research questions (RQs):

- **RQ1:** What are users' privacy perceptions and what factors influence their data sharing attitudes in the context of agent-facing mobile money transactions?
- **RQ2:** What security, privacy, and usability factors influence user and agent preferences and concerns for our alternative, privacy-preserving protocols?
- **RQ3:** What other design considerations arise with the use of privacy-preserving protocols?

We present the results of a role play and semi-structured interview study conducted in March 2024 with 32 MoMo users and 15 agents in Kenya to test our privacy-preserving protocols. We summarize our findings below:

- Expanding upon prior research suggesting that users have privacy concerns when sharing their data with agents [8], we gain a deeper understanding of the specific types of concerns, including fraud and concerns for personal safety that they have.
- We observe that users and agents generally prefer our proposed protocols, in part because they address existing workflow inconveniences and provide increased security and privacy. Specifically, users prefer the use of biometrics to physical IDs and appreciate the privacy protections afforded by the new protocols and the security of authentication in delegated transactions.

- We highlight limitations of the proposed protocols from users' perspectives. Agents were concerned about the data minimization leaving them vulnerable to agent-targeted fraud, while users expressed concerns about the protocols being lengthy and complex, as well as limiting who they can send as a proxy.

We recommend that MoMo providers pilot and further refine these privacy-preserving protocols. We also recommend further research on agents' concerns about agent-targeted fraud, the design of secure and usable delegated transactions, and more generalizable approaches to privacy-preserving identity proofing and KYC.

2. Background and Related Work

2.1. Background

Mobile money (MoMo) is widely adopted and used by both banked and unbanked users, with more than 640 million users worldwide in 2023 [21]. Users include both smartphone and basic phone owners, with a significant portion of the population using basic phones. In Kenya for example, the basic phone market share exceeds 40% [22].

MoMo transactions include depositing money into the MoMo wallet, withdrawing money, and person-to-person transfers [8]. Withdrawals can be done in multiple ways, e.g., at an agent or via bank to MoMo transfers. For this study, we focus on the withdrawal and deposit processes involving an agent. In the current withdrawal process (Figure 1a), a user first goes to an agent and presents their Identity Card (ID) for identification, before initiating the transaction on their phone. Typically, they will open the MoMo app, select the transaction type e.g., withdrawal, enter the amount, followed by the agent's number, and finally confirm the transaction by entering their MoMo PIN. If successful, the transaction will generate two confirmation messages (see Figure 2), with one sent to the agent and one to the user. Once the agent confirms the transaction has occurred, they record user details including their ID number and names, and transaction details including amount, time, and transaction code before handing the user the money.

Privacy challenges with current process: Previous work [8] and our study show that many users worry that their personal information recorded by agents can be misused under the current processes. We highlight some of the steps in the current process (Figure 1a) that leak privacy, and what the risks are. (1) In the KYC step, users submit their ID for identification by the agents. Agents are also required to keep a record of all transactions that they facilitate in a physical book, including the ID number and name of each user. In addition to the ID card exposing many other pieces of data like place of birth that are not required for KYC, cases have been reported of agents using users' IDs for illegal activities such as registering additional SIM cards—also detailed by users in this study (see Section 5.1.1). (2) Once the transaction is authorized, the agent receives a notification (Figure 2) that contains more information such as the name and phone

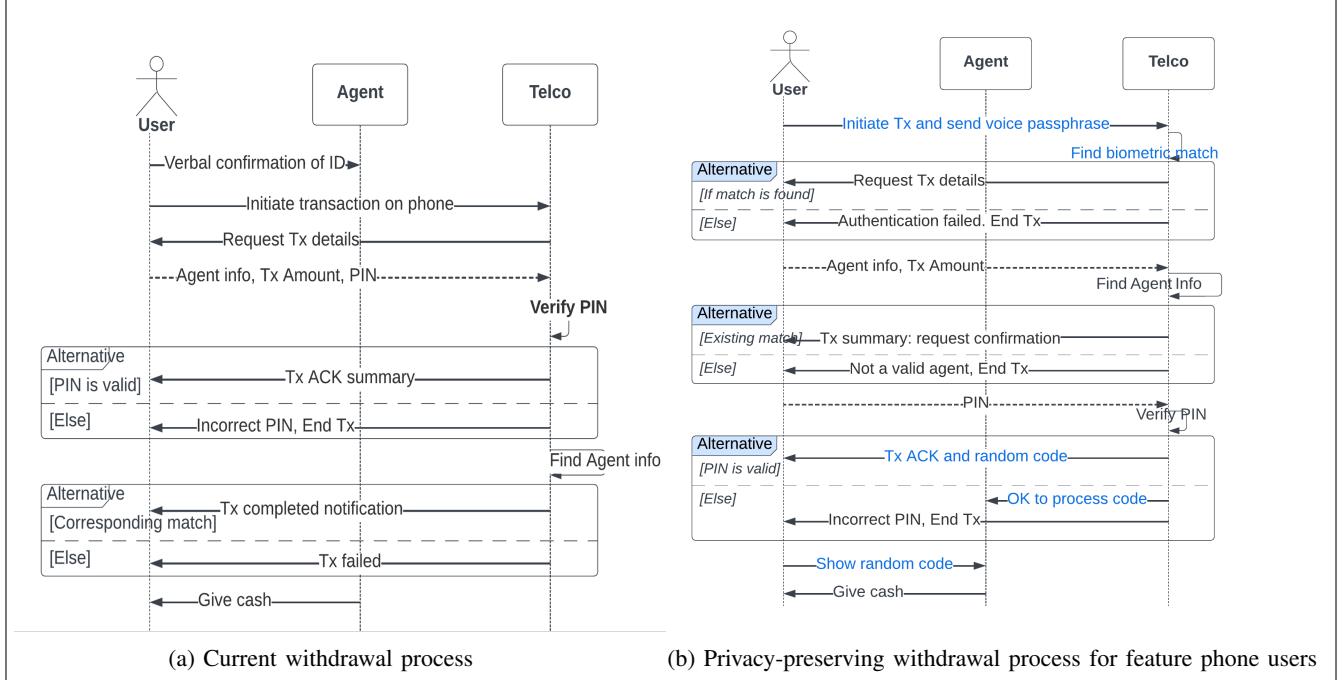


Figure 1: Withdrawal under the current protocol (left) and the proposed privacy-preserving protocol (right)

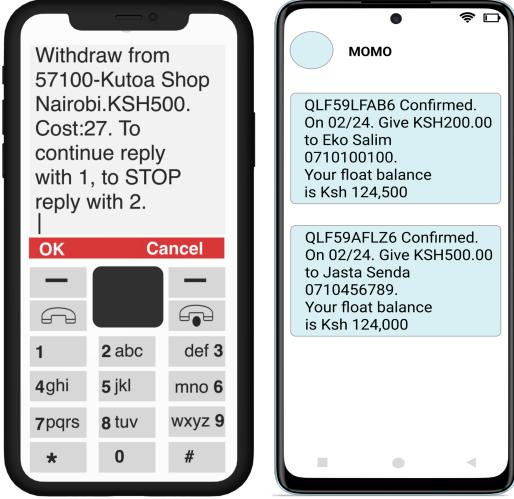


Figure 2: Sample MoMo UIs: Withdrawal acknowledgment on a basic phone (left) and messages for agents (right)

number of their user. These details can be misused by agents for unsolicited phone calls, or unauthorized data-sharing with third parties. Ultimately, privacy loopholes present risks for agents who cannot securely store users’ information in accordance with data protection laws.

Our solution: To protect users’ personal information when withdrawing money, we designed an alternative, privacy-preserving process (see Figure 1b). For this process, users do not need to hand their IDs to the agents nor share their personal information e.g., phone numbers with the agents. Instead, they authenticate using biometrics on their phones (fingerprint or facial for smartphones, and voice

identification for basic phones). Afterward, users can initiate the withdrawal on their phones, generating a confirmation message with a unique code sent to both the user and the agent. Once the agent confirms the user received a similar code, they can hand the money to the user. See Section 3 for more details about the processes.

2.2. Related Work

2.2.1. Security and Privacy of Mobile Money. While mobile money services fill a crucial gap by offering financial services to otherwise many unbanked users in the developing world [1], [2], there is limited work exploring the security and privacy of these services. In one of the earliest technical analysis of mobile money apps, Reaves et al. [23] uncovered a wide range of vulnerabilities in 46 Android MoMo apps used in 28 countries, with many of the apps containing botched certification validation and other forms of information leakage that left users vulnerable to impersonation and financial fraud. A related study of MoMo apps on Android similarly found that most of these apps were not following security best practices [24]. Through a systematic analysis of 197 digital financial services in Africa and South America followed by interviews with stakeholders e.g., developers, Castle et al. [25] found that although these apps were susceptible to various attack vectors, service providers were intentionally making efforts to secure them.

Bowers et al. [26] investigated 54 mobile money services in 32 countries in 2017, finding that almost half of these services did not have any form of privacy policy. For those that had privacy policies, these policies were hard to read, and often not in the language of their target users. This makes it difficult for users to understand what data is collected from them, how it is used, and how it is secured.

One unique aspect of MoMo services is that there are often human agents rather than banks to facilitate transactions such as cash withdrawals and deposits. However, the interaction between users and mobile money agents introduces unanticipated security and privacy challenges [27]. Through 72 semi-structured interviews in Kenya and Tanzania, Sowon et al. [8] found that both users and agents design workarounds to the challenges posed by MoMo systems, including relying on their relationships for informal authentication. The study recommends the need to rethink the privacy and security of this ecosystem to improve both security and usability. Accordingly, we design new privacy-preserving workflows for MoMo, and then evaluate their efficacy and feasibility via role play and semi-structured interviews with users (both agents and users) in Kenya.

2.2.2. Emerging Digital Lending Apps. Besides mobile money, digital lending apps have emerged as a quick and easy way to obtain loans in the developing world, further enhancing financial inclusion [28], [29], [30]. This has been partly facilitated by increasing smartphone usage, as well as MoMo services that allow users to get these loans directly disbursed to their mobile phones. However, these apps have also raised privacy concerns. By identifying 51 representative digital credit lenders, analyzing their privacy policies, and then comparing them to the data gathered by the apps, Bowers et al. [31] found numerous security and privacy issues with these apps, including the collection of previously undisclosed data types. Munyendo et al. [32] interviewed users of mobile loan apps in Kenya and learned about issues such as social shaming when users default in repayment. Similar concerns have been noted in India, sometimes driving loan app users to suicide [33], [34], [35], [36]. Akgul et al. [37] analyzed reviews on the Google Play Store and found that these privacy concerns are widespread across many other countries beyond India and Kenya.

2.2.3. Our study. While previous studies [8], [26], [31], [32], [37] highlight security and privacy issues with digital financial apps in the developing world, none of them study the privacy attributes of “know your customer” (KYC) practices. We design privacy-preserving KYC processes for mobile money and evaluate their usability through a user study in Kenya with both mobile money agents and users.

3. Protocol Design

The objective of this paper is to design a privacy-preserving KYC protocol for MoMo. The key design considerations were: 1) *Correctness*: the protocol should correctly implement KYC for MoMo. 2) *Privacy*: it should provide better privacy for users relative to the current process. We define privacy in terms of *data minimization*: that is, minimizing the transfer of sensitive information to the agent. 3) *Cost*: the protocol should minimize costs for users, including communication round trips to/from MoMo and transaction fees.



Figure 3: Users interacting with the paper prototypes

Our design makes assumptions about trust in MoMo providers and availability of identity infrastructure.

Trust in MoMo providers: We assume that users trust the MoMo provider *more* than individual agents, an assumption validated by some users in our study (see Section 5.1.1).

Availability of identity infrastructure: In line with prominent identity frameworks [38], we assume there exists infrastructure for identity-proofing individuals by providing required evidence such as an ID card or other accepted documents for initial validation. At the point of executing transactions, we assume this infrastructure also enables digital authentication of users, e.g., using biometrics especially given the increased efforts to pilot digital ID systems in Africa [39]. Given the wide use of feature phones by MoMo users, we assume authentication infrastructure for both smartphone and basic phone users. For smartphone users, existing options include fingerprint or facial image recognition, while feature phone users can use voice biometrics. While photo ID authentication is still in its early days worldwide (e.g., [40]), Kenya (specifically, Safaricom) has already implemented a voice biometric system called *Jitambulisse*, which allows users to identify themselves when they need to reset their PINs [20]. The identity infrastructure could either be managed by the telco provider (as in the case of Jitambulisse), a national digital ID service, or an approved third party. Our protocols are therefore robust enough to be used with solutions such as VCs without any additional overhead or workflow changes.

The protocols for smartphone users and basic phone users are exactly the same, with the only difference being the type of biometric used. In the following sub-sections, we illustrate only two privacy-preserving protocols for withdrawing: 1) withdrawing for basic phone users and 2) delegated withdrawing. The current (see Figure 5a) and corresponding privacy-preserving deposit (see Figure 5b) protocols are included on Figure 5 in the Appendix.

3.1. Privacy-preserving withdrawal

Our privacy-preserving withdraw protocol for basic phone users is illustrated in Figure 1b. The parts of the protocol that *differ* from the current withdraw protocol (shown in Figure 1a) are indicated in blue. In our new protocol, a user initiates a MoMo transaction by first supplying their biometric (e.g., a voice passphrase). Basic phone users will initialize a transaction normally, but will receive a phone call requesting voice authentication.

Once authentication is successful, the user proceeds with the transaction by entering the transaction details including the amount, and the agent number of the agent store they are withdrawing from. The telco will verify that the agent number is valid, before providing a transaction summary for the user to confirm the transaction on their phone by entering their PIN. Both the agent and user receive a confirmation SMS of the authorized transaction. Unlike the process at the time of the study where the agent SMS contains the name and phone number of the customer, the privacy-preserving protocols provide a unique code to both the customer and agent. The agent also receives an amount associated with the code. After verifying that the two codes match, the agent gives the specified amount of cash to the person with the code.

Evaluation of Design Objectives: (1) *Correctness*: The new protocol may have similar or better KYC correctness compared to the current protocol, as users are authenticated automatically by the MoMo provider, rather than by a human agent. This can prevent fraudulent KYC practices, as discovered in [8]. While automated biometric verification can lead to errors (particularly in non-white populations) [41], we note that Jitambulisse has already been used successfully for seven years in Kenya. (2) *Privacy*: The new protocol has better privacy protections against agents, who never see the user's name or phone number. However, they do see the transaction amount; we view this as insurmountable, as the client must receive (or give) cash to the agent. (3) *Cost*: The protocol incurs 1.5 extra round-trips of communication from the client to the MoMo provider.

3.2. Privacy-preserving delegated withdrawal

Prior work on user-agent interactions in Kenya and Tanzania [8] revealed that MoMo users often involve other people when withdrawing money. In these *delegated transactions*, a *sender* (the user who wants to withdraw money) sends a *collector* (typically a friend or relative, also called a *proxy*) to withdraw cash. There are different ways of executing delegated transactions using existing MoMo systems. In one variant, users send a peer-to-peer transaction to the collector, who withdraws cash on the sender's behalf. In another variant, the sender may share their ID, physical phone, and PIN with the collector (typically a trusted party, like a child). The sender may also withdraw remotely using the agent details that they have saved, and send the proxy to receive the cash. In the latter scenario, agents often operate

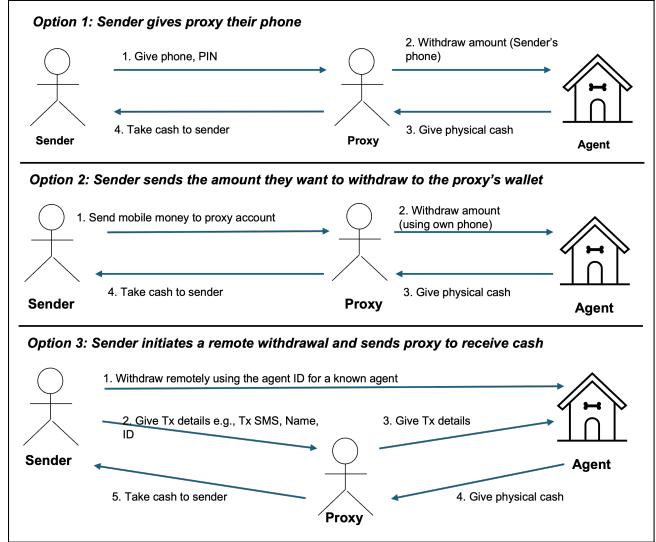


Figure 4: Current workarounds for proxy withdrawal

on trust: they release cash to the collector without verifying that the sender authorized the collector to withdraw on the sender's behalf. This process is illustrated in Figure 4.

Our proposed delegated privacy-preserving withdrawal protocol (Figure 6) formalizes the delegated cash withdrawal process by allowing a user to initiate a transaction and assign it to a collector who will travel to an agent store to complete the process. Unlike the current withdrawal practice, our proposed protocol ensures that both the sender and collector are authenticated to MoMo, thus facilitating proper KYC.

Like the base privacy-preserving withdrawal protocol (Figure 1b), the first step upon transaction initiation entails user verification through biometrics (see Figure 6a). The sender then assigns the transaction to a proxy by providing their phone number. When the proxy (collector) arrives at an agent store (see Figure 6b), they initiate collection by providing the agent number from whom they will collect the money. The collector selects the transaction that they want to collect. After confirming the transaction by entering their own PIN, the unique codes are sent to both the collector and the agent. The agent ensures that they are giving money to the right person if both codes match. At this point, the sender receives a notification about the completed transaction; only the sender incurs transaction charges.

Evaluation of Design Objectives: (1) *Correctness*: The formalized delegated protocol removes guesswork and inconvenience involved in authenticating users who transact remotely. With both the sender and collector authenticated to MoMo, the agent has better assurance about the identities of all parties. (2) *Privacy*: The protocol offers additional privacy guarantees to the sender, because they do not have to share any personal information with the collector or the agent. (3) *Cost*: As no formal process for delegated transactions exists, we cannot compare the communication round trips. However, the new protocol may reduce surcharges. In the informal proxy transaction process, users often incur

TABLE 1: Participant demographics for users and agents

	Users		Agents
	Smartphone	Feature phone	
Gender			
Male	10	7	8
Female	9	6	7
Age			
18-24	5	2	3
25-34	10	7	6
35-44	4	3	2
45+	0	1	3
Education			
Below high-school	0	2	0
High-school	6	6	8
Post high-school	3	5	7

double charges to withdraw if they send money to the collector's wallet so that they can withdraw it.

4. Methods

To evaluate our proposed privacy-preserving protocols, we conducted a user study with MoMo users and agents in Kenya. We conducted an in-person within subjects usability study with 32 MoMo users where we adopted a wizard-of-oz approach, with a dedicated researcher simulating the responses of the phone based on the user's interaction with our low-fidelity paper prototypes. We also conducted an interview study with 15 MoMo agents. Rather than requiring agents to role-play, we adopted a process walk-through approach where we demonstrated the protocols to 15 agents. We did this because agents are typically small business owners and it is difficult to get them to dedicate more time to the study. Each demo was followed by interview questions to gather agents' perceptions of the processes. All interviews were conducted in a mix of English and Kiswahili, as is commonly spoken in Kenya. The interviews were conducted by a native researcher assisted by two native researchers.

4.1. Study Procedure and Data Collection

Prototypes: We created the privacy-preserving protocols as low-fidelity prototypes, using Figma for design. We printed the finalized prototypes on paper for the user experiments. To control for learnability, we designed our prototypes to maintain the look and feel of Safaricom's M-Pesa [2], the most popular and widely used MoMo product in Kenya.

We designed two interface variants: one for smartphones, and another for feature phones. For each variant, we created interfaces in both English and Kiswahili to reflect the current language choices that MoMo offers. We showed each user the variant and language that corresponded to the phone they used. We used the same wording and messaging of notifications and prompts across variants. Due to limitations of paper prototypes and character count limitations on basic

phone displays, we intentionally excluded message elements like the date and time. This ensured that notifications could fit on one screen, and that we could use the same prototypes for the whole study regardless of time. In addition to the new protocols, we also had paper prototypes of the current process. We also had additional study material that users would have seen, or interacted with if the MoMo provider were implementing the new protocols. These included an ad highlighting the biometric authentication features and a video demo of the biometric enrollment process.

Participant Recruitment: To recruit MoMo users, we posted flyers at agent shops in five diverse neighborhoods in Nairobi. We also visited agent shops in these locations to recruit directly by engaging the individuals visiting these shops. We asked participants and other people in our networks to share with others information about our study. We advertised the study as an interview about alternative mobile money processes (without stating anything related to privacy) to minimize social desirability bias and avoid priming.

We also asked the agents who owned the shops that we visited if they were interested in participating in the agent part of our study. We aimed for a good balance between male and female agents as past research has shown that gender influences how people use MoMo services [42]. In the end, we had eight male agents and seven female agents. Table 1 provides a summary of the demographics of the participants. The final sample sizes were adequate to reach saturation.

We provided information about study participation and scheduled appointments over the phone or in person. Those who agreed to participate received reminders before the scheduled interviews. We emphasized that participation was voluntary and that participants could opt out without any consequences. We compensated all participants for their time and transportation costs at rates that were approved by the Kenyan ethics board (approximately \$5.40).

Interviews and Tasks: We introduced the study as a product test that we were completing for a fictitious company to avoid participant bias. Before starting, we briefed participants on what to expect and demonstrated the concept of thinking aloud. We also tested each participant's ability to read by asking them to complete tasks unrelated to the study. These included pointing out from a list of menu items on the screen what they would select if they wanted an option to 1) save for their business, 2) identify themselves' and 3) make a phone call to a number not saved on their phone. The menu items that we included in this literacy test section aren't included in the current MoMo interfaces. The test ensured that we did not proceed to the core part of the study with those who could not read but were familiar with the current MoMo interface and placement of menus out of habitual use, and could therefore navigate it even without knowing how to read. We assumed literacy if the participant could accurately select the correct option based on the task. One participant was excluded this way.

Thereafter, participants were required to complete three tasks: 1) withdraw using the standard protocol 2) withdraw

using the privacy-preserving protocol, and 3) complete a delegated withdrawal using the privacy-preserving protocol (both as a sender and as a collector). All tasks were completed in the same order by all participants. Each of these tasks was followed by a set of interview questions to elicit participant feelings and perceptions of the protocol.

We asked participants to think aloud as they completed the tasks. We recorded their audio as well as videos of their screen interactions with the paper prototypes, capturing their hands only for confidentiality purposes (Figure 3). After completing each task, participants were interviewed about their experiences and perceptions of the proposed protocols. The experiments, together with the accompanying post-task interviews, were approximately 60 minutes long.

The interviews with agents followed a similar flow with questions focusing on their roles as agents. These lasted 30 minutes on average. Both agent and customer interview scripts are in Appendices A and B, respectively.

Pilot Testing: Before data collection, we conducted two walkthroughs with members of the team and six pilots to test the setup, understanding of tasks, and flow of questions. We used the insights to modify when we showed participants the additional study material to reduce priming and improve clarity of interview questions. We do not report on pilot data.

4.2. Data Analysis

The audio-files were translated to English and transcribed before being uploaded to Nvivo v14 for coding. The coding was carried out by three researchers, two of whom are Kenyan natives. We used inductive analysis to develop an understanding starting from the data rather than from a predetermined set of codes. We had three major stages of coding. The first stage entailed development of the initial codebook where three researchers independently coded an agreed upon sample of the transcripts. They then met to discuss emerging codes, come to a shared understanding of their meanings, and develop the initial codebook. This was done iteratively until agreement was reached.

In the second stage, the coders used the initial codebook to inductively code the remaining transcripts. This was completed cross-sectionally, by splitting the transcript to three sections based on the user tasks, and assigning each coder a section across all the transcripts. We did this to allow better consistency in coding the data. The coding team met weekly to discuss the suitability of existing codes, add new codes to the codebook, and resolve any differences. This ongoing process also ensured that the entire team developed a shared understanding of the emerging codebook.

The final stage was a peer review process which allowed us to double code the data and ensure integrity of the process. Each coder was assigned a section that they were not the original coder for to peer-review. Secondary coding helped identify any inconsistencies, which were discussed and resolved between the primary and secondary coders. Since all conflicts were discussed and resolved, there was no need to compute inter-rater reliability [43].

After all coding was completed, the primary coder reviewed the codes to combine, group, and categorize similar ideas into code categories first, before abstracting them further to create themes and sub-themes based on the research questions. The resulting themes were discussed with the wider research group and refined further.

4.3. Ethics and Positionality

Ethical Considerations: This study was approved by three Institutional Review Boards (IRBs), including the [ANONYMIZED] IRB in Kenya, [ANONYMIZED], and [ANONYMIZED]. We also received a research permit from the National Council of Science and Technology (NACOSTI) in Kenya. We took several steps to protect participants. First, we assigned the participants a fictitious profile with a name, a phone number, and an ID to use throughout the study to avoid sharing their own PII. Second, we sought consent to audio and video record with the latter capturing just the hands of the participants. We planned to use the video recordings to offer additional insights to participant interaction with the protocols. In the end, the think-aloud data sufficed. Although we collected participant phone numbers for follow-up and compensation, this information was stored separately and not linked with study data. Access to the audio files was limited to researchers and a transcriptionist. Participant responses are reported using pseudonyms e.g., A01 for agents, and U01 for users.

Author Positionality: Four of the researchers, including the lead researcher, identify as Kenyan natives and have extensively interacted with MoMo. This informed the design of the study and helped ensure correct interpretation of the data without losing contextual nuances. The non-Kenyan members of our team brought fresh perspectives that further enriched our protocol design and the analysis of the results.

4.4. Study Limitations

Our study has some limitations. First, due to the qualitative nature of the study and the small sample size, we cannot make any statistical generalizations. Second, the study may be subject to biases such as participant self-censorship and recall bias. Third, our paper prototypes are likely more cumbersome to use than a digital interface, which may have impacted participant perceptions. Finally, we found that some participants were confused when role-playing both the sender and collector in the delegated protocol.

5. Findings

In this section, we present our results for each of the three research questions stated in the introduction. Aligned with qualitative methods, our analysis aimed to surface general themes about privacy in the context of MoMo transactions as well as participants' experiences with the privacy-preserving protocols. To avoid implying generalizability, we report our findings using the following terminology: a few

(less than 25%), some (25-45%), about half (45-55%), most (55-75%), and almost all (75-100%).

5.1. Perceptions and Attitudes About Data Sharing

As in Sowon et al. [8], we found that users were concerned about their privacy in their interactions with agents. Our findings provide richer insights regarding factors that contribute to users' data sharing attitudes with agents.

5.1.1. Privacy perceptions. We present the privacy perceptions that emerged from the study as a four-dimensional typology that captures user perceptions about what is private, private from whom, risks, and risk mitigation techniques.

What is private and why: When asked what data was private and what was not, most users felt that their account balances and ID information were private, while almost all mentioned that their PIN is private. About half felt that their phone number was personal and very few considered their name private. In terms of the reasoning for information being private, some cited the personal identifiability of the data, while others discussed realities such as their ID being a gateway to many other identities and information: "if someone has my ID number, they can track my NSSF,² NHIF,³ [and] my ID number links me to my bank and my family details" (U18).

A few users said they would consider their data as private under some conditions e.g., large transaction amount.

"[The amount is] personal depending on the money transacted. For instance, if I have withdrawn a million and someone has that knowledge they might plan to attack and rob me" (U22).

Privacy from whom: Participants frequently expressed concerns about who had access to their information during transactions, with almost all users uncomfortable with agents having access to their data. In addition to sharing specific concerns (Table 2), a few explained that too much data was shared, and others expressed concerns about the recording of data, such as in a physical book for evidence of transactions. Only a few users were concerned about the MoMo providers having access to their information. The most common reason for concern by this group was a mistrust of MoMo employees who could access account balance data, potentially identifying those with large balances.

When asked about sharing data with proxies in the current proxy engagement techniques, some users were worried about sharing personal details e.g., ID or PIN even though most people send proxies that they trust.

What risks are users concerned about: Almost all users discussed the negative outcomes that could arise from data sharing during the MoMo transaction process. While there were a number of unspecified concerns, we find four main

2. The National Social Security Fund allows employers and citizens to contribute to save for retirement similar to the 401K in the US.

3. The National Health Insurance Fund is a contribution-based fund to provide accessible and affordable health insurance for Kenyan citizens.

types of specific concerns: 1) fraud and theft, 2) unauthorized use of data for non-MoMo purposes, 3) physical harm, and 4) economic judgments (See Table 2). The most frequently mentioned harms were fraud and theft, followed by unauthorized use. While most of the concerns cited the agent as the main threat actor, a few users feared that the MoMo provider employees were part of the MoMo fraud incidences and people losing their money. Users mentioned unauthorized uses of data by agents such as registering new SIM cards and using people's IDs to register voters. "I came to learn that my ID number had registered another sim card and I didn't know" (U18). Those who mentioned the risk of physical harm, tied it to the agent knowing user account balances and potentially acting as accomplices to defraud them, while some mentioned stalking and harassment. "[The agent] might try calling me and stalking me, and so I wouldn't want them to have a name and phone number to avoid that" (U19). Finally, a few users shared that there might be a risk of socio-economic judgments due to knowing how much money one transacts or has in their account balance.

What risk mitigation techniques do MoMo users use?:

To combat the concerns discussed previously, some users described potential privacy protections to balance the sharing of information with the ability to complete MoMo transactions. For example, some suggested blurring or removal of parts of sensitive information. This could include redacting portions of one's ID number or phone number, which is similar to a common practice of redacting all but the last four digits of the Social Security number in the United States. Users provided these suggestions to balance their desire for privacy with their desire to provide the data they perceived as necessary to complete transactions.

Some of those who shared data with proxies mentioned techniques such as redacting the account balance for the shared notification message, changing one's PIN when the delegated transaction was complete, and auditing their account to ensure the proxy did not withdraw a larger amount. "She went to the shop and came back with the money and after that I changed my PIN" (U30).

5.1.2. Factors influencing data-sharing. We explored participant beliefs about the various pieces of data exchanged in MoMo transactions to understand their feelings about what was collected and shared. We find that perceived utility of shared data, perceptions of data sensitivity, trust, and obligatory compliance contribute to why participants find data-sharing acceptable.

Perceived utility of shared data: Almost all users and agents mentioned the practical utility of sharing various pieces of information e.g., authentication and verifying users, monitoring transactions, and recourse. "I verify [who the customer is] by asking for his or her ID" (A1).

Most agents and users pointed out scenarios where sharing data could help both parties follow up with each other or contact the provider in case of issues with a transaction. Agents specifically relied on the data collected during the transaction process for recourse.

Party	Fraud and Theft (n=26)	Unauthorized Use (n=16)	Physical Harms (n=10)	Economic Judgments (n=6)
Agent	PIN, ID No., Account Balance, Phone Number, Amount Withdrawn	ID No., Phone No., Name, Amount Withdrawn	Amount Withdrawn, Account Balance, Phone No., PIN	Account Balance, Amount Withdrawn
Proxy	PIN, Phone	-	-	Account Balance, Amount Withdrawn
Provider	PIN, ID No., Phone No., Name, Account Balance	-	-	Account Balance, Amount Withdrawn

(n): number of respondents who mentioned

TABLE 2: A summary of some common data concerns and the related threat actor from the perspective of users

“[When] a person has withdrawn he can go and reverse the money—he can call Safaricom, and claim he had withdrawn from a wrong agent and so you see when Safaricom calls me as an agent and they ask me “did you get the ID?”, if you didn’t get the ID Safaricom will automatically send the money back to the person” (A14).

Perceptions about data sensitivity: Many users discussed being comfortable sharing data they felt was “less sensitive” for various reasons. The most common reason was that certain data, mostly the name and amount were “common knowledge” to other people or to the agent. “everyone calls you by your name, so it is not a secret” (U18). A few participants were open about sharing their information because they “had nothing to hide” or because they believed they were anonymous to MoMo: “I am not doing an illegal transaction like I have stolen anyone’s money, it’s very legal so I don’t have anything to hide” (U28).

Data sharing based on trust: A common theme throughout the study was the requirement of trust when completing transactions. About half of users mentioned trusting agents and providers, with the MoMo providers being trusted slightly more often than the agents. For instance, U22 said: “They are the service providers offering the service. I trust them to keep my information secret.”

In the case of delegated transactions, trust also played a central role in how users decided who to send, and to which agent. Even after going through the privacy-preserving delegated process where participants acknowledge the benefits of not having to share data with proxies, about half of users still cited trust as a requirement for sending someone else. Ultimately “once the [proxy] has the money I [still] need them to actually give it to me” (U3).

Sharing out of obligatory compliance: Most users and agents expressed the need to share their data for compliance when completing MoMo transactions, or just as a necessary trade-off to use MoMo services: “there are details they might need and even if they are personal the company says it’s okay to give them, I am going to give” (U26).

Users seem to accept the requirement of sharing their information as part of the mobile money transaction process, but when shown alternative options, they understand the potential risks associated with those actions.

5.2. Existing Process Inconveniences

When asked if there was anything they would change about the current MoMo transaction processes, many users expressed general satisfaction, describing the process as

simple. However, upon being asked further questions about their current practices, both groups of participants shared a number of existing process inconveniences, which at this point they considered normal. The following four inconveniences were prevalent: 1) inconveniences related to the use of IDs, 2) inconveniences of balancing data-sharing and security, 3) contextual complexity in security and privacy decision-making, and 4) usability challenges.

ID-related challenges: Many of the agents and users expressed dissatisfaction with the use of IDs in MoMo. Users generally felt the challenges of using IDs were mostly linked to their usability, whereas agents felt that the use of ID was inefficient. The reasons given ranged from being cumbersome for both them and their clients, jeopardizing users’ privacy, and not being fully secure.

“Actually, [the use of IDs] is a bit challenging and there should be a simpler way of [verification] to speed up the process ... [Because] if you have four, five people that are there on the queue waiting, you know the process of checking, and writing is time consuming and maybe that person urgently needs the money” (A10).

One agent pointed out the inadequacy of IDs for security:

“We are in Kenya where people can go to [duplicate IDs] and have the same ID as someone else. These people that do fraud on M-Pesa nowadays have these fake IDs” (A12).

We note that agents’ concerns are largely not fully addressed by our protocols, which still rely on the ID infrastructure.

Inconvenience of balancing data-sharing and security: When sending others to complete transactions i.e., delegated transactions, most users found themselves having to share a lot of their personal information with the proxy. Most people indicated giving the proxy either their phone together with their MoMo PIN, or sharing other transaction details such as the details of the notification message, or the notification message itself, as well other personal information such as the physical ID card. “I gave him my ID card and phone and gave him my PIN.” (U14). U23 said: “I will forward the message for them to show the agent the message,” while U18 explained that they did not like that they shared their data, but was forced to as it was their only option when they needed to send someone to collect money.

Contextual complexity in decision making: Both the agents and users experienced contextual complexity from the current processes. For users, this mostly had to do with balancing factors such as the choice of agent, their location, and the transaction amount with privacy needs. On the agent’s

side, the complexity occurred in how they balanced the requirement for KYC with usability for their clients. Agents adopted more relaxed ID and transaction practices with known users or small transactions, while requiring stricter verification for unknown users, higher value transactions, or highly risky transactions like delegated withdrawals. “[I require the ID] for new users [because] that is where there is a lot of fraud” (A12).

Other challenges manifested as process inefficiencies. For instance, when asked about how they currently manage delegated transactions, both groups shared various techniques e.g., ensuring that the collector bears the transaction and sender information, and offline communication between the agent and customer to hash out various aspects of this informal transaction process.

“When that person who has been sent comes I don’t give them cash first, I call that customer first and verify like ‘whom have you sent—in terms of their names and their number, and ID number’. After talking to him or her, then I can confirm that they have indeed sent that person” (A12).

Some agents even stored their client details to facilitate efficiency in future remote and proxy transactions: “Before you come to trust users that way, at least you have their details. All those users I have their ID’s” (A14). Such modifications introduce risks and inconsistencies, as agents constantly balance security with convenience.

5.3. Impressions of Privacy-Preserving Protocols

When asked about the new protocol, we find that the participant preferences for the new protocols reflected perceived affordances beyond what the existing processes offer. In this section, we first highlight the specific security, privacy, and usability features that our participants identified as being advantageous in the new protocols. Next, we present usability and security issues associated with the new protocols that concerned our participants.

5.3.1. Better privacy and security affordances with the new protocols. Both groups of participants expressed preferences for privacy-preserving protocols. Both users and agents mentioned three categories of preferences—those related to 1) security, 2) privacy, and 3) usability.

Privacy-preserving process offers better security: Users and agents mentioned features that they felt contributed to better security. For example, in the delegated withdrawal process, the two groups felt that the verification of both parties, the transparency of the process, and the formalized way to engage someone enhanced security.

“It is secure and procedural and then everyone is comfortable with it—the agents themselves have a way to trust it, and myself and the other [person I am sending] can trust it. Everything is documented and just in case we encounter issues it can be traced on whatever happened” (U10).

In addition to these features in the delegated withdrawal, almost all users and some agents felt that the code in the privacy-preserving process offered additional security. “The code is another added layer of security. [The agent] and I are the only ones getting the code, and she asks me for the code and I tell her the same thing she has” (U13).

The final feature that contributed to perceived security was the use of biometrics for authentication over IDs. “I like it because I feel it is secure and someone will not be able to remove your money because they will not have your fingerprints” (U12). Many agents shared similar feelings about biometrics. “People steal [other people’s] ID’s. [With] this one, [the agent is] sure [because] there is no way your fingerprint will match my fingerprint” (A13).

Privacy-preserving process offers better privacy: When asked what they liked or if they would use the privacy-preserving process, almost all users cited the benefit that their personal information was not shared with the agent. Most also felt that the privacy-preserving protocols gave them better control over their data.

“[What I like is] that I just withdraw and [the collector] goes to collect for me so there is no personal information shared. I remain with my phone and my details and he uses his phone and his own details . . . there is also no way [the agent] can use my details in the [new process], but the first one [the agent] can even get my phone number and start calling me and harassing me” (U9).

Agents also liked the privacy offered by the new process. A10, referring to the physical book agents maintain for transactions they complete, said: “We have manual books and every time they are insisting we put down the [customer and transaction] details in case of anything—but this one is fully digital, and protects the privacy for the clients.”

Privacy-preserving process is more usable: About half of users and some agents specifically mentioned how the delegated withdrawal process offers a more convenient way to complete delegated transactions. Most users found the protocols relatively “straightforward” and “easy” to use and indicated that they would choose the new privacy-preserving processes over the existing ones. One recurring aspect that participants frequently discussed was the convenience offered by the process not requiring them to carry their IDs to transact. “It is good because there is no need for an ID, you just use your fingerprint to transact [and] your phone [which] I always have it with me, so there is no burden. We keep forgetting to carry our ID’s so this would really help.”(U14). Two users also thought that the new authentication process would be more convenient for agents.

Almost all agents felt the new process was more convenient for their users to authenticate. Two agents pointed out how better and efficient KYC impacted their own business success as agents. The process addresses “the challenge of users coming to transact and they don’t have their identification cards and so you cannot allow them to transact but with this, it will be good for our business as well” (U3).

5.3.2. Usability and privacy concerns. Only a few users and agents expressed usability and privacy concerns, which fall in four main categories: a) process inconveniences, b) process complexity, c) access and accessibility and d) privacy concerns related to voice biometrics.

Inconvenient process: Agents and users mentioned potential inconveniences of authenticating each time with the new processes. A6 preferred the flexibility offered by IDs in some cases: “You realize there are those users who frequently come here and you don’t need to keep authenticating their identity.” This may suggest some preference for authentication that is adaptable.

Both groups also expressed concerns about the authentication process having many steps. These were more pronounced with voice biometrics where they had to dial a short code, listen to the prompt, and repeat a passphrase: “it would be better if we had an option where you press and speak in without listening to that [prompt] before you speak — that would shorten the process.” (U31).

Given a choice between the existing and the new processes, however, most of these participants who expressed dissatisfaction with the authentication process because of its length mentioned that they would still choose the privacy-preserving process despite this inconvenience.

Complex protocols: Many sentiments alluding to protocol complexity were linked to a misunderstanding about the code, it’s expiration, details (sender’s vs proxy’s) to enter, and perceived complexity about the two-step process completed by the sender and their proxy.

For code expiration, agents were concerned about the potential malicious use of an expired code by another user to get money from the agent. This is based on an incorrect understanding about how the code works. More importantly, both agents and users raised potential concerns with the code expiration window in light of potential network delays and long customer queues: “you have to make sure that these codes you share between me and the customer are shared very fast so that you don’t have to keep ten users waiting because you are waiting for the code”(A14).

Process confusion sentiments were mostly related to the delegated withdrawal process. Some agents described the process as “complicated” and “confusing.” For users, the confusion manifested mostly during the delegated withdrawal task process. Some participants got confused when they had to play both the role of the proxy and the collector and sometimes forgot which one they were at a particular time. In the follow-up interview, many confirmed that they were confused because the whole process was new to them and that it would not be after using it for some time.

“I was confused at this point but I remembered I am not the one collecting [and that] I was [supposed to be] withdrawing. [As] with anything new, things are a bit confusing, but with time we get used to it and it becomes easier” (U2).

Privacy concerns with voice biometrics: One participant perceived voice biometrics as inconvenient and less private because they would have “shout” every time they went to an

agent, making them prefer an ID: “I will use my ID, because you don’t have to shout around people about your password. It’s quieter than this one” (U25). Note that the Jitambulisse voice biometric does not require users to state sensitive information like a PIN—rather, they are asked to repeat a standard phrase, and their voice is used to authenticate.

Access and accessibility issues: Most agents were mostly concerned about the potential challenges with access to the privacy-preserving features as well as accessibility of the biometrics. The access issues they mentioned were mostly related to technology and demographics. These agents felt that issues such as malfunctioning phones and phone battery challenges would limit access and that older and illiterate people would struggle with the new protocols. With regard to accessibility, agents felt that people with physical deformities would be disadvantaged and potentially excluded, especially with reference to the use of fingerprints for verification. “Maybe [the person] is a construction worker and their fingerprints are not quite clear and so sometimes they might try to use the fingerprint and it fails” (A5).

5.3.3. Security concerns. Agents and users alike expressed concerns about potential security issues with the privacy-preserving processes. About half of the users believed that the information contained in the newly-proposed messages that would be sent to the agents following a transaction was insufficient. They suggested adding information e.g., name or phone number of the person transacting, to help with verification or potential recourse. About half of the agents shared similar concerns, e.g., wanting to see a customer’s details in case they needed to reach out. A few agents were worried that only relying on the code for the privacy-preserving processes was not adequate to authenticate users, preferring to see the customer name.

Another security challenge shared by both groups was the potential failure of biometric systems. For example, referring to voice biometrics U1 asked: “What if the voice changes when you get sick? Or when your voice is hoarse.” Similar points were raised by a few agents regarding changes in one’s voice. However, a few agents and participants also believed that this system could be exploited. A13 discussed a potential distrust of their users completing their own verification: “...for my security purposes, how do you really trust the customer to allow the customer to do self-service?”

5.4. Other Considerations: Benefits and Challenges

Users and agents discussed other considerations regarding the privacy-preserving processes. From the the users’ perspective, some mentioned that there was actually more flexibility in choosing a proxy, mainly because the sender does not have to give someone their physical device, while others mentioned more freedom from not having to rely on known agents only, as they previously did with the delegated transactions. A few also felt that the privacy-preserving proxy process would be more affordable, since there would be no additional charges for collecting money

for another person. Others appreciated the new proxy system for its increased geographic flexibility when compared to the current protocols where remote transactions are discouraged by the provider based on the distance between the customer and the agent.

A few agents and some users were concerned about the need for the proxy to have a phone or be registered. “I cannot send my kid. Maybe he or she is a teenager without a phone so the process is limited” (U12). Other users worried this process would be restricted to literate users, since prompts are given as text on a series of screens, while some desired a batch collection option so they could collect money for multiple people at once.

6. Discussion

Current MoMo platforms are fraught with privacy, security, and usability challenges. These are exacerbated in part by heavy reliance on agents as well as inconvenient and sometimes exclusionary KYC practices. Existing workflows expose users to significant risks of unauthorized data access, while the reliance on traditional ID-based KYC processes creates usability barriers for underserved and marginalized populations. The growing reliance on MoMo services in developing economies, necessitates the development of privacy-preserving protocols that consider both technical constraints and human factors. To our knowledge, our study is the first to design and test alternative privacy-preserving protocols for MoMo that account for both external and internal threats, including the risk posed by mobile money agents. Here, we discuss some takeaways.

6.1. Balancing privacy, usability and security

Privacy remains an essential question in many digital financial systems including cryptocurrencies and most recently central bank digital currencies (CBDCs). MoMo, perhaps one of the earliest forms of digital payment solutions with roots in emerging economies, is no exception with studies highlighting various privacy issues in MoMo apps [23], [26], [31], [32] as well as user privacy concerns in the context of MoMo [8]. From the corpus of privacy literature, we know that privacy perceptions often influence data sharing [44], [45], [46]. However, we also know that system design contributes to better or poorer privacy experiences for users. This leads us to our first takeaway:

Takeaway 1: MoMo users are uncomfortable sharing KYC data with agents, but do so out of necessity: We find that users’ privacy perceptions influence what they think is private and why. However, why they actually share their data is a factor of the protocol demands rather than their perceptions. Agents share the same sentiments on why data-sharing is necessary. The perceived utility of the data cuts across all the transaction stages from authentication and verification of transactions and users, to actual transaction completion and transaction recourse.

Given the centrality of mobile money in these economies, it is crucial that designers think about how

the MoMo protocols can work together with regulation to support the desired outcomes e.g., security and privacy in MoMo. By having a protocol that is not privacy-preserving by design and that requires too much personal data to be shared, privacy is put at risk. On the contrary, data minimization efforts with proper access controls do not have to sacrifice protocol requirements. In this work, we proposed and tested one such effort that minimizes process-driven data-sharing, supporting users’ preferences for not sharing more than is required while ensuring that transactions can still be completed with reasonable efficiency and transparency.

The need to comply with KYC regulations for the sake of security in financial systems is often the reason behind the systematized data collection of account holders through processes such as mandatory SIM registration in the context of MoMo. Although privacy has sometimes been viewed as a potential obstacle to KYC compliance, there is increasing evidence that the two goals do not have to be in opposition to each other. Our work demonstrates that it is perfectly possible to address both security needs and privacy concerns and this is elaborated in our second takeaway message:

Takeaway 2: Both users and agents prefer the privacy-preserving protocols not just for their privacy capabilities, but also for their increased transaction security: Our findings reveal that most user concerns about sharing their data have the agent as the main threat actor, ranging from the fear of physical harm to psychological harm. A few participants indicated that they would have preferred to have more personal information in the transaction notification because of its perceived utility, e.g., to provide assurance that the agent was transacting with the correct person. Even then, most of such participants felt that this information should be redacted. Overall, users preferred the privacy-preserving protocols because they do not share their personal information with the agent, and also provide a mechanism to engage the proxy without having to share too much personal information such as PINs and phone. Similarly, agents expressed a preference for the new processes because they protect users’ data and because they offer more security and transparency in delegated transactions, thus mitigating some of the associated risks.

6.2. Digital identity verification and eKYC

Digital identity verification is seeing growing adoption [40]. In digital financial services, digital identity verification entails establishing “to some degree of certainty or assurance, a relationship between a subject accessing online services and a real-life person” to comply with KYC [38]. We find that MoMo users and agents are open to using biometrics for identity verification:

Takeaway 3: Authentication using biometrics is feasible and preferred to ID-based verification: The use of IDs for verification was a common process inconvenience cited by both agents and users. As a result, participants almost always indicated a higher preference for using biometrics over IDs. Previous work shows that the lack of legal identification

is one of the biggest barriers to financial inclusion [47], [48]. While such barriers affect MoMo users directly, they also indirectly impact agents who benefit from the economic opportunities that MoMo creates: “I prefer the new process [because] it addresses the challenge of customers coming to transact and they do not have their identification cards and so you cannot allow them to —but with this, it will also be good for our business.” The inconveniences of IDs that users face also inconvenience the agent and present additional risks when they have to adopt workarounds with privacy and security risks. As more service providers turn to eKYC to streamline the KYC process, our study provides a proof of concept with actual empirical results supporting the use of biometrics in a resource-constrained context.

6.3. Other Opportunities and Challenges

While our protocols show promise in improving MoMo privacy without sacrificing security and privacy, they have some limitations. This leads to our fourth takeaway:

Takeaway 4: New protocols are needed to accommodate delegated transactions in which the proxy does not have a MoMo account or phone: Our findings show that participants often send people in their social circles, e.g., their children, to collect money. With the formalized delegated withdrawal, the proxy would need to have their own phone and also be a registered MoMo user. This would therefore be problematic in situations where phones are shared among family members or when the proxy is a minor and therefore not a registered user. Although these may not be major issues in places like Kenya where phone penetration is high [49], we believe that the impact of such a limitation on financial inclusion needs to be further understood.

Takeaway 5: The data minimization in the new processes may present some vulnerabilities to agents: Some agents were also concerned that privacy-preserving workflows left them with inadequate information for critical processes, notably recourse. Agents indicated that they sometimes needed some of the users’ personal details such as name and phone number to reach out in case of a problem. These potential situations included dispensing the wrong amount, particularly excess cash. Those who preferred having the customer’s ID indicated that it served as legal evidence in case of fraud. We thus note that agents are also concerned about the fraud they face from potentially malicious clients.

7. Recommendations

While our protocols were largely acceptable to users and agents, there remain several areas of improvement. However, this was a qualitative study and the insights may not be generalizable to entire populations. To improve the proposed protocols, we present three recommendations:

Recommendation 1: Pilot the proposed protocols and test the placement of authentication in the workflow, to understand when, and why users may not consider authentication necessary then design alternative solutions

that would still balance the goals of privacy, security, and usability: An actual pilot of these protocols by MoMo providers (telcos) would help to confirm their feasibility. We also note that in practice, users may find the new authentication cumbersome if they have to complete it every time they use MoMo—even when completing transactions such as purchasing airtime. This experience appears to be consistent with their experience requiring the use of IDs whenever they transact. In investigating how authentication might be inconvenient, it would be beneficial to determine if this applies to all three types of biometric authentication or just to voice biometrics. Our study found more concerns with voice than with facial and fingerprint authentication.

Recommendation 2: Study the extent and nature of the fraud targeted at agents, and ensure that MoMo workflows are designed with appropriate and adequate security protections from malicious users: Security concerns and fraud targeting agents were a strong undercurrent among agents. It is evident that agents face some threats in the context of MoMo that would be useful to understand. To date, most security and privacy issues in the context of MoMo have been studied from the users’ point of view. Understanding what threats agents face will strengthen processes for all stakeholders. In thinking about agent protection, privacy-preserving protocols should have all the necessary protections to a) prevent fraud executed by ill-intentioned users, and b) ensure that if fraud happens, the agent has recourse via transparency offered by the protocols.

Recommendation 3: Study the impact of the limitation that requires that the proxies in delegated transactions are registered users or have own phones: It is important to continue pursuing inclusion in the context of MoMo. Previous research [9] has found that challenges with ID acquisition may negatively impact the registration of a SIM card in one’s name. Such barriers can negatively affect the successful implementation of the proposed protocols as users may find them more inconvenient if they cannot send the people they would naturally send in their day-to-day lives. Understanding the extent of such a limitation in the proposed protocols will help in making appropriate decisions about whether or how to resolve such a limitation.

Recommendation 4: Study how to make KYC systems both privacy-and-security-preserving by design: Regulators and central bankers have consistently argued that achieving a fully private payment system would be incompatible with AML and countering the financing of terrorism (CFT) requirements [50], [51]. This tension is especially evident in KYC where security is prioritized over privacy. This perspective potentially stifles innovations that could enhance user privacy while still meeting regulatory needs. A more nuanced approach would involve re-evaluating these assumptions to explore privacy solutions that minimize data exposure while still fulfilling identity proofing requirements.

References

- [1] K. Donovan, “Mobile money for financial inclusion,” *Information and Communications for development*, vol. 61, no. 1, pp. 61–73, 2012.

- [2] W. Jack and T. Suri, "Mobile money: The economics of M-PESA," National Bureau of Economic Research, Tech. Rep., 2011.
- [3] A. H. Ahmad, C. Green, and F. Jiang, "Mobile money, financial inclusion and development: A review with reference to african experience," *Journal of economic surveys*, vol. 34, no. 4, pp. 753–792, 2020.
- [4] A. Demirguc-Kunt, L. Klapper, D. Singer, and S. Ansar, *The Global Findex Database 2021: Financial inclusion, digital payments, and resilience in the age of COVID-19*. World Bank Publications, 2022.
- [5] H.-A. Nel, "Know-your-customer measures: mitigating money-laundering risks in mobile banking transactions," Ph.D. dissertation, North-West University (South Africa), Potchefstroom Campus, 2017.
- [6] P. C. Mondal, R. Deb, and M. N. Huda, "Transaction authorization from Know Your Customer (KYC) information in online banking," in *ICECE*. IEEE, 2016, pp. 523–526.
- [7] A. Gelb and D. Castrillon, "Identifying and Verifying Customers: When are KYC Requirements Likely to Become Constraints on Financial Inclusion?" Center for Global Development, Tech. Rep., 2019.
- [8] K. Sowon, E. Luhanga, L. F. Cranor, G. Fanti, C. Tucker, and A. Gueye, "The role of user-agent interactions on mobile money practices in kenya and tanzania," in *IEEE Security and Privacy*, 2023.
- [9] E. Luhanga, K. Sowon, L. F. Cranor, G. Fanti, C. Tucker, and A. Gueye, "User Experiences with Third-Party SIM Cards and ID Registration in Kenya and Tanzania," *arXiv:2311.00830*, 2023.
- [10] D. Nation, "African states tighten laws on data privacy and protection — nation," https://nation.africa/africa/news/african-states-tighten-laws-on-data-privacy-and-protection--4114310#google_vignette, 2023, (Accessed on 11/13/2024).
- [11] R. of Kenya, "The Data Protection Act," <https://www.kentrade.go.ke/wp-content/uploads/2022/09/Data-Protection-Act-1.pdf#page=4.78>, 2019, (Accessed on 11/13/2024).
- [12] M. C. Lacity and E. Carmel, "Verifiable credentials in the token economy," in *Blockchains and the Token Economy: Theory and Practice*. Springer, 2022, pp. 113–138.
- [13] C. Mazzocca, A. Acar, S. Uluagac, R. Montanari, P. Bellavista, and M. Conti, "A survey on decentralized identifiers and verifiable credentials," *arXiv preprint arXiv:2402.02455*, 2024.
- [14] J. Bernal Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. Torres Moreno, and A. Skarmeta, "Privacy-preserving solutions for blockchain: Review and challenges," *IEEE Access*, vol. 7, pp. 164 908–164 940, 2019.
- [15] G. Almashaqbeh and R. Solomon, "Sok: Privacy-preserving computing in the blockchain era," in *2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2022, pp. 124–139.
- [16] E. Androulaki, J. Camenisch, A. D. Caro, M. Dubovitskaya, K. Elkhayyouchi, and B. Tackmann, "Privacy-preserving auditable token payments in a permissioned blockchain system," in *ACM AFT*, 2020, pp. 255–267.
- [17] E. B. Sisson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *2014 IEEE S&P*. IEEE, 2014, pp. 459–474.
- [18] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: Short proofs for confidential transactions and more," in *Symposium on Security & Privacy*. IEEE, 2018.
- [19] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed e-cash from bitcoin," in *Symposium on Security & Privacy*. IEEE, 2013, pp. 397–411.
- [20] "Jitambulisse – voice biometrics," <https://www.safaricom.co.ke/media-center-landing/frequently-asked-questions/jitambulisse-voice-biometrics>, (Accessed on 08/25/2024).
- [21] E. Mathieu, "Mobile money accounts are surging globally, especially in africa and asia - our world in data," <https://ourworldindata.org/data-insights/mobile-money-accounts-are-surging-globally-especially-in-africa-and-asia>, June 2024, (Accessed on 11/11/2024).
- [22] L. Malephane, "Digital divide: Who in africa is connected and who is not," Afrobarometer Report (PDF), 2022, (Accessed on 09/19/2024).
- [23] B. Reaves, J. Bowers, N. Scaife, A. Bates, A. Bhartiya, P. Traynor, and K. R. Butler, "Mo (bile) money, mo (bile) problems: Analysis of branchless banking applications," *ACM TOPS*, vol. 20, no. 3, pp. 1–31, 2017.
- [24] H. Darvish and M. Husain, "Security analysis of mobile money applications on android," in *Big Data*. IEEE, 2018, pp. 3072–3078.
- [25] S. Castle, F. Pervaiz, G. Weld, F. Roesner, and R. Anderson, "Let's talk money: Evaluating the security challenges of mobile money in the developing world," in *ASCD*, 2016, pp. 1–10.
- [26] J. Bowers, B. Reaves, I. N. Sherman, P. Traynor, and K. Butler, "Regulators, mount up! analysis of privacy policies for mobile money services," in *SOUPS*, 2017, pp. 97–114.
- [27] E. Mogaji and N. P. Nguyen, "The dark side of mobile money: Perspectives from an emerging economy," *Technological Forecasting and Social Change*, vol. 185, p. 122045, 2022.
- [28] Z. Faux, "Tech Startups Are Flooding Kenya With Apps Offering High-Interest Loans," Feb 2020, <https://www.bloomberg.com/news/features/2020-02-12/tech-startups-are-flooding-kenya-with-apps-offering-high-interest-loans>.
- [29] A. Hecht, "2.5 billion people around the world don't have a credit score-here's why that's a problem," Aug 2019, <https://www.cnbc.com/2019/08/22/tala-aims-to-help-anyone-with-an-android-phone-have-access-to-loans.html>.
- [30] S. Adams, "How Tala Mobile is using phone data to revolutionize microfinance," Sep 2016, <https://www.forbes.com/sites/forbestreptalks/2016/08/29/how-tala-mobile-is-using-phone-data-to-revolutionize-microfinance/?sh=c3bf17e2a9f2/>.
- [31] J. Bowers, I. N. Sherman, K. R. B. Butler, and P. Traynor, "Characterizing Security and Privacy Practices in Emerging Digital Credit Applications," in *Proc. WiSec*, 2019.
- [32] C. W. Munyendo, Y. Acar, and A. J. Aviv, "'Desperate Times Call for Desperate Measures': User Concerns with Mobile Loan Apps in Kenya," in *Proc. IEEE S&P*, 2022.
- [33] D. Ramesh, V. Kameswaran, D. Wang, and N. Sambasivan, "How platform-user power relations shape algorithmic accountability: A case study of instant loan platforms and financially stressed users in india," in *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*, 2022, pp. 1917–1928.
- [34] M. Saritha, "Demystifying the misery behind loan apps in india," *Indian Journal of Finance and Banking*, vol. 13, no. 1, pp. 104–109, 2023.
- [35] A. Ali and V. B. Marisetty, "Are fintech lending apps harmful? evidence from user experience in the indian market," *The British Accounting Review*, p. 101269, 2023.
- [36] V. Aggarwal, N. Aggarwal, B. Dhingra, S. Batra, and M. Yadav, "Predatory loan mobile apps in india: A new form of cyber psychological manipulation," in *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)*. IEEE, 2024, pp. 1918–1922.
- [37] O. Akgul, S. T. Peddinti, N. Taft, M. L. Mazurek, H. Harkous, A. Srivastava, and B. Seguin, "A decade of privacy-relevant android app reviews: Large scale trends," in *Proc. USENIX Security*, 2024.
- [38] D. Temoshok, C. Abruzzi, Y.-Y. Choong, J. Fenton, R. Galluzzo, C. LaSalle, N. Lefkovitz, and A. Regenscheid, "Digital identity guidelines: Identity proofing and enrollment," National Institute of Standards and Technology, Tech. Rep., 2024.
- [39] S. Teleanu and J. Kurbalija, "Stronger digital voices from africa: Building african digital foreign policy and diplomacy," DiploFoundation, Tech. Rep., 2022.

- [40] S. Government, "Singpass app," <https://app.singpass.gov.sg/>, (Accessed on 11/13/2024).
- [41] P. Drozdowski, C. Rathgeb, A. Dantcheva, N. Damer, and C. Busch, "Demographic bias in biometrics: A survey on an emerging challenge," *IEEE Transactions on Technology and Society*, vol. 1, no. 2, pp. 89–103, 2020.
- [42] R. Chamboko, R. Cull, X. Giné, S. Heitmann, F. Reitzug, and M. Van Der Westhuizen, "The role of gender in agent banking," *Development Research*, 2020.
- [43] N. McDonald, S. Schoenebeck, and A. Forte, "Reliability and Inter-Rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice," *Proc. ACM Hum.-Comput. Interact.*, vol. 3, no. CSCW, 2019.
- [44] T. Dinev, H. Xu, J. H. Smith, and P. Hart, "Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts," *European Journal of Information Systems*, vol. 22, no. 3, pp. 295–316, 2013.
- [45] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model," *Information systems research*, vol. 15, no. 4, pp. 336–355, 2004.
- [46] H. Xu, T. Dinev, J. Smith, and P. Hart, "Information privacy concerns: Linking individual perceptions with institutional privacy assurances," *Journal of the Association for Information Systems*, vol. 12, no. 12, p. 1, 2011.
- [47] E. Yongo, C. Lowe, and Y. Theodorou, "Access to mobile services and proof of identity 2021," GSMA, Tech. Rep., 2021.
- [48] A. Martin and L. Taylor, "Exclusion and inclusion in identification: Regulation, displacement and data justice," *Information Technology for Development*, vol. 27, no. 1, pp. 50–66, 2021.
- [49] K. N. B. of Statistics, "Kenya_preliminary-report_sdg5b1.pdf;" chrome-extension://efaidnbmnnibpcajpcgclefindmkaj/https://data.unwomen.org/sites/default/files/documents/Publications/Kenya_Preliminary-Report_SDG5b1.pdf, 2022, (Accessed on 11/05/2024).
- [50] H. Armelius, C. Claussen, and I. Hull, "On the possibility of a cash-like cbdc," chrome-extension://efaidnbmnnibpcajpcgclefindmkaj/https://www.riksbank.se/globalassets/media/rapporter/staff-memo/engelska/2021/on-the-possibility-of-a-cash-like-cbdc.pdf, 2021, (Accessed on 11/08/2024).
- [51] R. Auer and R. Böhme, "Central bank digital currency: The quest for minimally invasive technology," chrome-extension://efaidnbmnnibpcajpcgclefindmkaj/https://www.bis.org/publ/work948.pdf, 2021, (Accessed on 11/08/2024).

Appendix

1. Interview Script - Agents

Thank you for participating in our study. We are in the process of testing mobile money transfer processes for a new product called MoMoPesa from a company called MoMoCom. I am going to be showing you some of their processes, and asking you for your feedback. The purpose of the study is to help us evaluate the usability of the new processes. Remember we are not evaluating you as an agent in any way. We are evaluating the new mobile money process from MoMoCom. I also want to let you know that I don't work for MoMocom, so your feedback won't hurt my feelings.

Standard Transaction Process

Show a demo of the standard process that the customers usually follow.

- 1) Is the process I have just shown to you similar to the current process that customers currently follow when they are withdrawing money?
- 2) Currently when you register users and when users are using mobile money, how do you know who they are? (probe: What do you use to confirm their identity?)
- 3) Why is this confirmation important/necessary?

- 4) How often do you need to verify people's identity?
- 5) What do you think about using IDs to authenticate your customers?
- 6) Is there anything you would change about the authentication process using IDs that you use at the moment?
 - a) Probe: are there any difficulties or challenges you experience from using physical ID to authenticate mobile money users?
- 7) What information is contained in the current transaction messages you receive as a summary of the customer's transaction?
- 8) Your telco provider wants to change the content of the message you receive about the customer's transaction by removing unnecessary information. They have come to you to know the following:
 - a) What information is necessary for your records that you would want to keep in the SMS you receive? How is it useful?
 - b) What information do you think is unnecessary, or you could do without? How is the information useful?

Privacy Preserving Process

Show privacy preserving process and show both the face/finger and voice authentication processes on the smartphone and basic phone prototypes:

- 9) In the new process you have seen, customers will not need to show their ID when transacting. They will follow the process that I have just demonstrated to register and authenticate themselves.
 - a) What do you think about using such a process where customers authenticate themselves instead of relying on IDs?
 - b) Do you see any challenges using this method of authentication?
 - c) If your MoMo provider gave you a choice either to authenticate customers using their ID or to have customers use the new process to authenticate themselves using a selfie, their fingerprint or voice, which one would you choose? (Why?)
 - d) Is there any situation where you would prefer to use IDs?
- 10) Is there any situation where you think customers would prefer to still use their IDs instead of authenticating themselves this way?

Show redacted message and also show what the customer would receive:

- 11) What do you think of this transaction message that you would receive when a customer transacts?
 - a) Which message would you prefer? This one or the one you currently get? Why?

Proxy-Withdraw Privacy Preserving Process

Before showing the proxy-withdraw process, ask:

- 12) Has any of your customers ever transacted and sent someone else to collect the money? If yes, how do customers normally do this? If no, imagine someone (a child or an adult) comes to your shop and says they have been sent by someone who happens to be your customer who has withdrawn some money using your agent number.
 - a) As the agent, how do (would) you know or verify who the sender is? Does the sender need to do anything to facilitate verification e.g., calling the agent to say who they will send? Sending someone mutually known? Does the agent call the supposed customer?
 - b) As the agent, how do (would) you know that the person collecting the money is the right person who was sent?
 - c) Does (would) the person who has been sent need to provide any information? (If yes, what information?)
 - d) How about the sender. Do (would) they need to provide any information? (If yes, what information?)
 - i) How do (would) they provide this information to you?
 - ii) Do (would) you store this information for future use (say when the person sending someone else is your customer) or does the customer need to provide it all the time?
 - iii) (If (ii) above is yes), how do you store the information (probe: What exactly do you store?)
 - e) How does the customer get the agent number to withdraw the money given they are not at your shop when they are transacting?
 - f) At what point do (would) you decide to actually give the person who has been sent the money. (Probe: What will make you confident to give this other person the money?)
- 13) As an agent, is there anything you like or dislike about this process where customers transact away from your kiosk and send other people to collect the money?
 - a) Is it possible to give money to the wrong person?

- b) Have you or another agent ever given money to the wrong person in this situation when someone says they have been sent?

After showing the proxy withdraw process, ask:

- 14) When customers are sending other people to collect money, they can either provide the person they are sending or to you specific information about the transaction, or they can use the process I have just shown you. As an agent, given the option to educate customers on one of these methods, which one would you point them to? Why?
- 15) Is there anything you like about such a MoMo process where a customer can send someone else?
- 16) Is there anything you dislike about it?
- 17) Are there any challenges you foresee in such a process?

Other Questions

- 18) Are you aware of data privacy laws in Kenya?
- 19) (If yes), What are your responsibilities as a mobile money agent as defined by these laws?

2. Interview Script - Users

Introduction

Thank you for being here. We are in the process of testing mobile money transfer processes for a new mobile money product called MoMoPesa from a company called MoMoCom. I am going to be giving you some activities to do, and asking you for your feedback as you work on these tasks. The purpose of the study is to help us learn more about the usability of the new processes from MoMocom. The tasks are not in any way a test of your skills. So just do the best you can and if there are things that don't make sense to you just let us know.

You will be working on a mobile phone which happens to be on paper. This is *name of assisting researcher* and she will be playing as our mobile phone today and handing you the different screens based on your actions. And this is *name of assisting researcher* and she will be playing the role of an agent today. So imagine that this is your phone area and your screens will be placed here. Use this pen to interact with the phone. Point to things you will normally select, and where you would normally type something, just tell me what you would type for example "I will enter my phone number" which is "then say the phone number." MoMoPesa is the picture on your screen that looks like a wallet. So why don't we try this:

- Show me what you would select to open the MoMoPesa menu.
- Would you show me the option for saving for your business?
- Please show me now what you would select if there was an option to identify yourself on the screen.
- Now show me what you would do to call a number: 0770800900 that is not saved in your phone book.

[Researcher's note: These are a test that the participant can read. Observe to make judgments on this. Only continue if participant passes tests]

Thank you. For the purpose of the tasks today, we will assign you a name, a phone number and an ID number to use wherever these will be needed. Here is your ID. Please keep it where you other ID is. (Researchers note: Ensure the participant has kept this ID where their national ID is) These are your other details (Researcher to hand the participant the paper with their created profile). While working on the tasks you might encounter areas that we do not have a screen for, and that's okay, we will guide you through it. As you work on your activities, please tell us what you are thinking and what's going through your mind. For example, you might say, "I was expecting a different screen," "I am feeling confused" "this is different from what I am used to" or any other such thoughts that may come to your mind. All of this information is important for us to know. Remember we are not evaluating you in any way, we are evaluating the new mobile money process from MoMoCom. I also want to let you know that I don't work for MoMocom, so you won't hurt my feelings if you don't like something. During the activities, please imagine that you are transacting as you normally would in your regular life. When you finish a task, please let me know you are done. You may ask questions while doing the activity, however, I may not be able to answer all of them until the end of the session. Do you have any questions?

[Researcher's note: Test that the participants understand the role play] Please take a look at the paper profile I gave you. Remember you are going to pretend to be this person today. Tell me, what is your name today? And fake study name? What is your phone number? ID number?

Before we start, I would like to show you how I would think aloud when I want to call someone called Eko Kolipo on my phone.

Task 1: Participant Withdraws Using Standard Current Process

Instructions and Task

In this first task, you want to withdraw Ksh 500 from an agent. Please complete this process as you would using mobile money. *Name* will be your agent. Interact with them as you would when you go to an agent. *[Researchers note: During each task, ask the participant to repeat the task they are required to complete. If the participant is not thinking aloud, prompt with things like: Tell me what you are thinking about right now. What are you looking at? What are you looking for? What are you trying to decide?]*

Interview Questions

- 1) What were your impressions of this process? (prompt: what makes it *their response*) *[Researcher's note: Also ask about any observations that were not addressed through the think aloud: I noticed that...]*
- 2) Was the procedure you just completed similar to the process you would usually follow when cashing out mobile money?
 - a) (If no) What about it was different?
 - b) Anything you particularly liked about this process?
 - c) Anything you did not like?
- 3) Why do you think you are asked to provide your ID when you transact at an agent?
- 4) Have you ever been inconvenienced by the need to show your ID when withdrawing mobile money? (If yes) How so?
- 5) What information do you think the agent receives when you transact using the procedure you just followed? (prompt with: Did the agent receive your name? Your ID? Your phone number? How much money you wanted to transfer?)
 - a) Is there any situation where you would not want to share any of this information with the agent? (prompt for what and why)
- 6) What information do you think is sent to the *MoMo provider* when you initiate a withdrawal using the procedure you just followed?
 - a) Is there any situation where you would not want to share any of this info with the MoMo provider? (prompt: what and why?)
- 7) Have you seen a sample message the agent gets when you transact?

Additional Questions - After Being Shown the Agent Notification

I will now show you a sample agent notification message of your just completed transaction. *[Researcher's note: Show the Swahili or English message depending on what language participant uses for their MoMo]*

- 8) Consider the transaction summary that the agent received.
 - a) What do you think about it?
 - b) Did the content of the message surprise you?
 - c) (If yes) What surprised you?
 - d) (If no) Why were you not surprised?
 - e) Would you change the information contained in the message?
 - f) (If yes) How would you change it? (What would you add/remove?) Why?
 - g) (If no) Why would you not change anything?
 - h) When transacting via MoMo, would you consider any of this information personal? (name, mobile number, amount, ID number, PIN, time of Transaction, balance)?
- 9) Is there anything you would change about the process you just used? If yes, what and why?

Task 2: Participant Withdraws Using Privacy-Preserving Process Advertisements Material

Thank you *fake name* for completing the first task. Before we move on to the other two tasks, I will show you a sample advertisement from MoMoCom explaining some of the features of their new product MoPESA, that will provide a different way to verify your identity and also allow a person to either withdraw cash themselves, or to withdraw and send someone else to collect. *[Researcher's note: Show ad(s) and demo]*

- *This is the advertisement showing the different ways you can use to be identified:* Show the general ad with the three identity processes.
- *Now, I will show you how their registration of identification would work - In your case, it would be preferred biometric option.*

Comprehension Questions

- What are the ways you can identify yourself from the advertisement?

Instructions and Task 2

Now that you have an idea of the process from MoMoCom we will move to the second task. Assume that you already registered your preferred biometric: face or voice. Using this next process, I'd like you to withdraw Ksh 500 from an agent. This time, you are withdrawing yourself and not sending someone else. *Name* will be your agent today. Interact with them as you would whenever you go to an agent.

[*Researchers note: Ask the participant to repeat the task*]

Interview Questions

Thank you for completing the last tasks. I will now ask you some questions about this process that you have just used to withdraw money.

- 10) What did you think of this process? (What makes it *their response*)
- 11) Is there anything you liked about this process compared to the process of withdrawing money that you normally follow? (prompt for how e.g., if they say it was more secure)
- 12) Is there anything you disliked about this process compared to the process that you normally follow? (prompt for how/what e.g., if they say it was difficult to use)
- 13) If your provider (e.g., Safaricom) offered you a choice between this process and the one you use, which one would you choose? (Why?)
- 14) Why do you think you did not have to provide your ID when completing the transaction using this process?
- 15) Compared to the previous process where you had to show your ID:
 - a) Anything you liked about the new process of being identified?
 - b) Anything you disliked about the new process of being identified?
 - c) If your provider gave you a choice of using either your ID, or this new process of being identified, which one would you use?
 - i) Why? What makes *their option* better for you?
- 16) What information do you think the agent received when you transacted using this process? (prompt: Did the agent receive your name? ID? phone number? How much money you wanted to transfer?)
 - a) Is there any situation where you would not want to share any of this information with the agent?
 - b) (If yes) which information would you not want to share and why?
- 17) What information do you think is sent to the mobile money provider when you complete the transaction using this process?
 - a) Is there any situation where you would not want to share any of this information with the mobile money provider?
 - b) (If yes) Which information would you not want to share and why?

Now I will show you a sample agent notification message that the agent received when you transacted using this process (Note: Show message and show previous one for process 1)

- 18) Consider the transaction summary that I have just shown you.
 - a) Did you notice any difference in this message from the one you saw earlier? (If yes), what was different?
 - b) Do you think the notification provides the agent any way to be sure he is giving the money to the right person?
 - i) (If yes), how so? (No), what should be included?
 - c) What did you like or dislike about the content of the agent notification message?
 - d) Would you change the info contained in the notification message?
 - e) (If yes) How would you change it? (What would you add/remove?) Why?
 - f) (If no) Why would you not change anything about it?
 - g) Which message would you prefer that the agent receives about your transaction? Why?(prompt: How so where appropriate)
- 19) Is there anything about this whole process you would change? (prompt: Like anything you are concerned about, or something you feel could be better?) If yes, what and why?

Task 3: Proxy Withdraw Using Privacy-Preserving Process

Pre-Task Interview

Thank you for completing the second task. We have one more task, but before you start, I would like to ask some questions to help me understand how people use MoMo. Sometimes, people send others to withdraw money for them and there are many different reasons why people would do this.

- 20) Have you ever sent someone else to withdraw money or to collect money that you have withdrawn? (If yes) Please tell me how you usually go about the process. (If not) Give scenario: Imagine you

were sick and could not get to the agent and so you needed to send someone; how would you go about this?

- a) How would you decide about whether you would send someone or wait to do it yourself? (prompt: amount of money, location, a new agent vs known agent, urgency, collector is the receiver?)
- b) Who would you send?
- c) What would (or did) you have to do to ensure that the person collects the money successfully? (prompt: What would (or did) you provide to the person you are sending?)
 - i) Ask for all mentioned: Why would the info be useful?
 - ii) (For information) How would (or did) you provide this info? (prompt: do you write down, do you call?)
 - iii) Is there any situation where you would not want to share some or all of the information you mentioned with the person you were sending?
 - iv) (If yes) Which information and why?
- d) What would (or did) you have to provide to the agent to ensure the person you sent collects the money without any problems?
 - i) How would (or did) you provide this information?
 - ii) Is there any situation where you would not want to share some or all of the information you mentioned with the agent?
 - iii) (If yes) Which information and why?
- 21) Is there anything you wish you could change about the way you currently send someone?

[*Researcher's note: I will show you one more ad from Momocom that shows the different ways you can withdraw using their new process*

Comprehension Questions

- What are ways you can withdraw money from the advertisement?

Task 3: Instructions and Task

Part 1: This is our third and last task. During this task, you might encounter some screens where we use X to hide part of the phone number and only show the last 4 digits like this (show sample screen). Now Imagine you want to withdraw Ksh 500 and send someone else to collect it for you from the agent. I would like you to initiate the transaction. Remember to keep telling me what you are doing. I will act as the person you would have sent in real life.[My name is Mimi Koleta and this is my phone number.] *Name* will continue to play the role of the agent. [*Researchers note: Ask the participant to repeat the task they are required to complete.*]

Part 2: Now *fake name*, I would like you to imagine that I am your friend and I would like to send you to go and collect for me Ksh 1000 that I have withdrawn. I have already initiated the transaction as you just did with your own transaction a few minutes ago. Now imagine that you are already at the agent and complete the cash collection for me. [*Researchers note: Ask the participant to repeat the task they are required to complete.*]

Interview Questions

Thank you. I will now ask you some questions about your experience with these two processes of sending someone and collecting for someone.

- 22) What did you think of the process?
- 23) Is there anything you liked about this process compared to the current one that people use when sending someone else to collect?
- 24) Anything you disliked about this process compared to the current one that you (would) use when sending someone else to collect?
- 25) Is there anything you found difficult? (if yes, what and how so?)
- 26) Is there anything you found confusing? (if yes, what and how so?)
- 27) If you were using this process:
 - a) What would you consider more carefully compared to when you send someone the normal way?
 - b) What would you consider less carefully (or what would be less important) compared to when you send someone the normal way
 - c) Would your decision of who you send change because of using this process? (If yes) how so?
- 28) Are there any reasons why you would not use this process?
- 29) What info did the person you were sending need to have or see when you sent them to collect using the procedure you just followed?
 - a) Is there any situation where you would not want to share some or all of the information you mentioned with the person you were sending? (If yes) What and why not?
- 30) What information do you think the agent received when you transacted using this last procedure that you just followed?

- a) Is there any situation where you would not want to share any of this information with the agent? (Note: correct participant after they respond if they have a wrong perception of what was sent)
 - 31) What information do you think was sent to the mobile money provider when you transacted using this procedure?
 - a) Are you comfortable with the mobile money provider having access to this information? Why or why not?
 - b) Is there any situation where you would not want to share any of this information with the mobile money provider?
 - 32) If you were to send someone to collect, would you want them to use this new process of collection or would you prefer the current method you use? Why?
 - 33) If you were to collect money for someone else, would you want to
- use this new process of collection? Why?
- 34) Overall, if you needed to withdraw money and send someone else to collect and your MoMo provider offered you this process as an option, which one would you choose – Would you use this process or would you prefer not to use this process at all? Why?
 - 35) Is there anything about this process you would change? (Additional probe: Like anything you are concerned about, or something you feel could be better). If yes, what and why?

3. Additional Figures

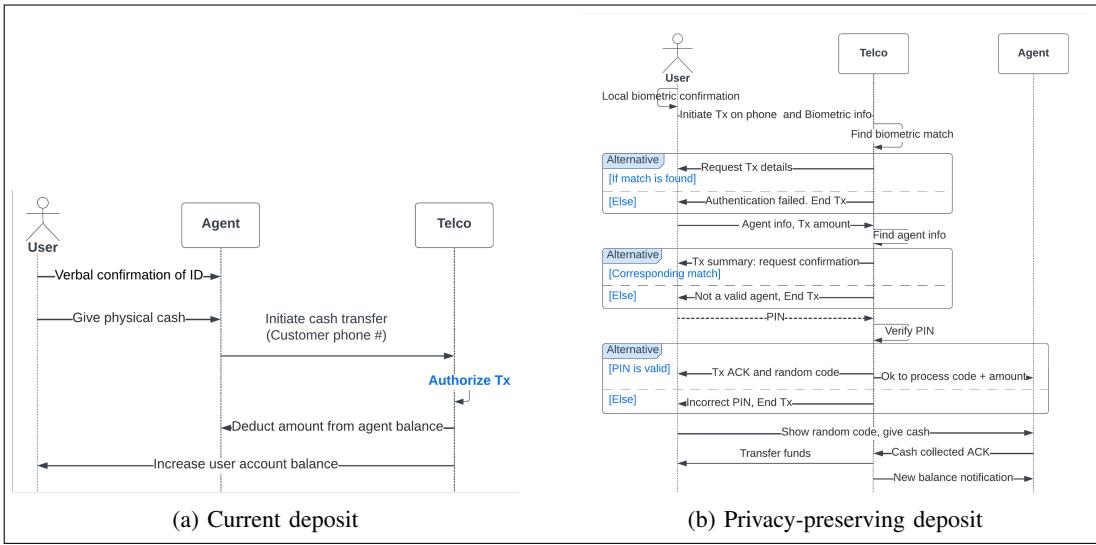


Figure 5: Current and privacy-preserving techniques for depositing money

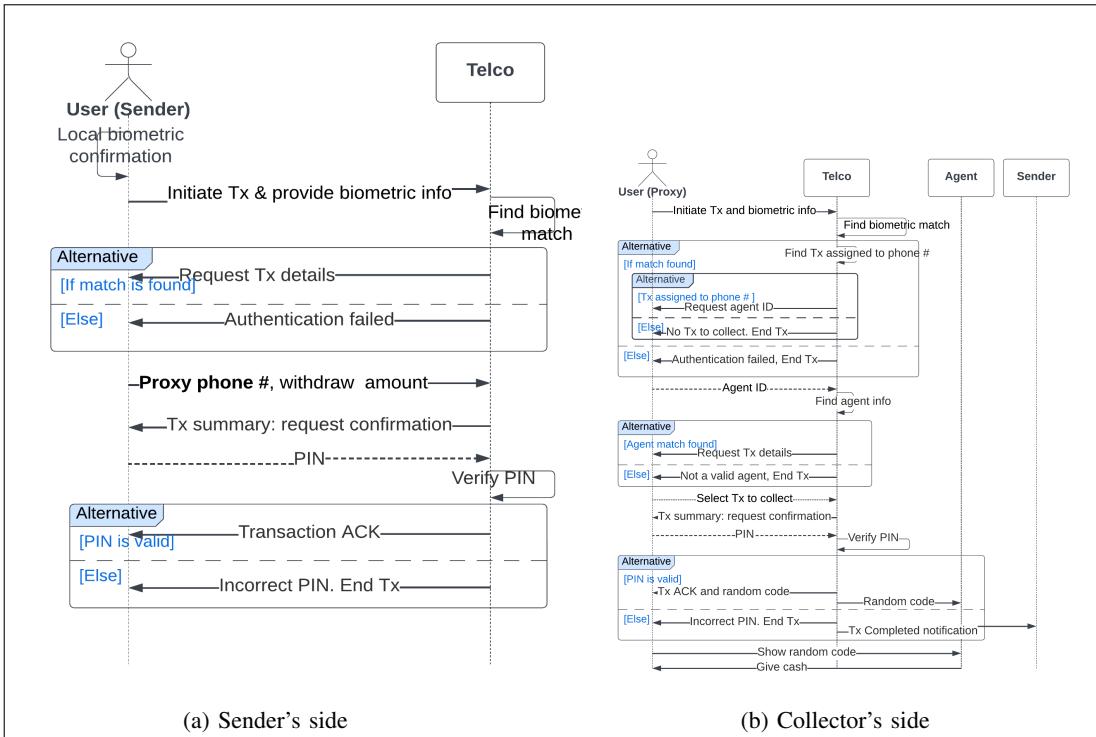


Figure 6: Collector's and sender's side of the privacy-preserving delegated withdrawal