Terms and Conditions (Do Not) Apply: Understanding Exploitation Disparities in Design of Mobile-Based Financial Services

Lindah Kotut
kotut@uw.edu
Information School, University of Washington
Seattle, Washington, USA

Abstract

Mobile-based financial services have made it possible for the traditionally unbanked to access infrastructure that have been routinely unattainable. Researchers have explored how these systems have made for safer environments to send and receive money and have expanded financial opportunities such as increased borrowing. With this expansion, challenges such as detrimental interest rates, lack of access to policy documents, and inadequate user protective guardrails emerge, amplifying the risks due to technology-aided unethical financial practices that are aided by design patterns. Supported by user interviews, we detail user experiences of mobile-based financial transactions and explore the foundations and guidelines that undergird the financial service provisions: highlighting both affordances and harms enabled in the design of such systems. We discuss the findings by highlighting financial exploitation disparities, deliberating strategies for mitigation of risks and enabling recovery from harms caused by the technology use. We then recommend guidelines for empowering design approaches that support users' mechanisms of trust, their understanding of technological processes, and determination of risks.

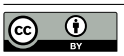
CCS Concepts

• **Human-centered computing** → **User studies**; • **Applied computing** → **Electronic commerce**; • **Security and privacy** → *Social aspects of security and privacy*; • **Social and professional topics** → Privacy policies.

Keywords

Financial Disparities, Information Asymmetry, Harm Recovery, Design Ethics, Mobile Transactions, Privacy Policies, M-PESA

ACM Reference Format:
Lindah Kotut. 2025. Terms and Conditions (Do Not) Apply: Understanding Exploitation Disparities in Design of Mobile-Based Financial Services. In *The 5th Biennial African Human Computer Interaction Conference (AfriCHI 2025), November 4–8, 2025, Cairo, Egypt*. ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3757232.3757238



AfriCHI 2025, November 4–8, 2025, Cairo, Egypt

ACM ISBN 979-8-4007-1849-6/2025/11
https://doi.org/10.1145/3757232.3757238

1 Introduction

In envisioning steps to address pressing issues in developing economies (spanning concerns over economy, gender, health and sustainability), and inspired by the new millennium, the United Nations set a 15-year, eight-goal strategy called the Millennium Development Goals (MDG) in 2000 [44]. The first MDG goal was aimed towards halving the rate of poverty and hunger, and spurring employment [44]. In response to this goal, and to expand access to credit: the M-PESA[1] platform was developed, piloted, and launched in Kenya. The platform was intended to bridge the financial access gap, and to provide the convenience of mobile-based financial services without the necessity of physical banking infrastructure or a traditional bank account [22].

The success of the M-PESA platform was owed to the design approach informed by the understanding of how Kenyans used their mobile phones. For example, the use of airtime as alternative currency to address safety concerns with transporting cash: given that the airtime credit could be transferred across individuals with no fee, and converted to cash without any loss of value [17]. Since its unveiling, M-PESA has served as a case study for approaching expansion to those without access to financial services (called the unbanked), and users without smartphones, as all the options are available through Short-Message Service (SMS) codes and Unstructured Supplementary Service Data (USSD) menus [71]–making it safer to use than cash for most users [22].

With the affordances that M-PESA has provided to marginalized users, new challenges arise resulting from coupling telecommunication and financial infrastructures. Early research identified user adoption being negatively impacted by the transaction fees and the lack of interoperability across mobile providers [19]. The ease of access to finances also led to increased incidences of financial fraud [58] and other security-related events [37]–the people affected by these events often the most vulnerable. Our work builds upon research that have sought different approaches to address these threat concerns spanning research, industry and policy directives, that have identified among others: challenges related to the mismatch between profit-motives and user needs [14], stakeholders lacking the technical know-how [70], and the lack of awareness and easy access to the terms of use and privacy policy documents [38].

With technological evolution, it has become possible for other services to be built on top of the M-PESA infrastructure, and new mobile loan providers now use the M-PESA platform to lend money and receive payments through the service. While this has led to more people accessing credit, it has also made it possible for the

[1] M-PESA: "M" an acronym for "Mobile" and "Pesa" a Swahili word for "Money"

users to be disenfranchised through onerous document and data requirements, and/or be saddled with high interest rates on microloans [60]. The laws and policies intended to protect the users tend to be broad: lacking clarity and scope [56], with enforcement–if mandated, often occurring after demonstrated financial harm/financial loss [46]. This is both an emerging and ongoing phenomenon, and while enumerated harms are reported in the Kenyan press, the research implications and design guidelines remain broadly unaccounted for in research.

We explored the challenges at these intersections, considering the activities involving the launching of a financial service, the demonstrated abuse, and the effectiveness of responses mandated by policy in addressing the abuse and preventing future re-occurrences. We did so by conducting an interview-based study with 17 participants seeking to understand their experience with mobile-based financial services: against the prescribed guidelines of the UN sustainability goals [45]. We examine user interactions, the trust signals used to mitigate risks–alongside their experience with fraud and financial exploitation, and if/how they recovered from harms. Given this asymmetric context, we use postcolonial computing [24] to examine the power differentials and colonial traces inherent in design for developmental contexts. In doing so, we examine the types of financial transactions that are conducted, the vulnerabilities faced by the users, and the user awareness on available protective mechanisms–towards seeking design guidelines for supporting trustworthy frameworks that also involve and inform policy.

We detail the inefficiencies of current tools and systems in protecting and informing the users of existing risks, in mitigating loss of money, and in assigning responsibility for harm repair. We also foreground the demonstrated user resilience (learning, recovering, warning others, etc.) and their custom use of technology. We then discuss the gaps in policy coverage, and opportunities for researchers, designers, and policy makers to address them in support of infrastructures and user knowledge, and to engender accountability and other design considerations in service of underrepresented users in this uniquely African context.

We make two contributions with this work. First, we highlight the nature of financial-based risk exposure in developmental contexts where there is laxity in policy enforcement and infrastructural support. The resulting user apathy and technology abandonment provide insights to designs intended to support policy, and adds to the nuance of users actions that do not reflect their stated preferences e.g., financial safety. Second, we highlight how users leverage design signals and trust signals to identify risks and evade harms. The findings has implications on HCI researchers who seek to design and envision systems to support users in addressing risks and assist in their harm recovery.

2 Background and Related Work

The first of the eight Millennium Development Goals (MDG) presented in 2000 was to "eradicate extreme poverty and hunger" [44]–in part by making it possible for people most threatened by poverty to access financial infrastructure. MDG was succeeded in 2016 by the UN Sustainable Development Goals (SDG) whose first goal describe a need to "promote sustained, inclusive and sustainable economic growth, full and productive employment and decent work for all... [with a target to] ...strengthen the capacity of domestic financial institutions to encourage and expand access to banking, insurance and financial services for all" [45]. In this work, we follow the path of how this goal has been operationalized in Kenya through the M-PESA platform, the impact on the unbanked, and the opportunities and challenges that have arisen as a result.

2.1 Mobile-Based Financial Services

While the envisioning of the M-PESA platform followed the MDG on reducing poverty by supporting job creation through entrepreneurship, the success of the platform is owed to the confluence of three factors in observance of how the unbanked interacted with money: *transfer and savings, borrowing,* and *alternative currency*. In the absence of banking infrastructure, the dangers inherent in the transfer and saving of cash was understood both by the unbanked–who had limited alternatives–providing the opportunity for M-PESA to supply means of safely doing so. Additionally, the M-PESA platform was chiefly modeled after how people borrowed money through informal and small-scale table banking[2] systems (called *chamas*) [26], and formal microfinance institutions [40].

The design of the M-PESA platform was also made possible by imitating how the unbanked leveraged cash alternatives for safety, and for access to a quasi-financial infrastructure. The people envisioned ways of overcoming safety and access challenges by re-selling airtime and phone scratch cards, a common practice in developing economies [17]: as they incur no overhead fees, and can be bartered or used as equivalent currency. All this was aided by the quick adoption of mobile services by Kenyans [35]; and the eager stakeholder participation in creating new infrastructures in the absence of appropriate policy directives [22].

Researchers have generally supported the M-PESA vision for enabling economic growth and well-being across rural/urban divide, gender, and socio-economic status [16], and envisioned the need for supporting infrastructures to scaffold the new needs for regulations, and identity management–especially in the face of differing contextual use, differential access to traditional critical infrastructure [27], and users without conventional forms of proof of identity [36]. For instance, a retrospective study of M-PESA highlighted factors such as greater access to agents, to financial instruments, and women successfully transitioning from farm work to engaging in commerce in centers [71] to be good metrics of on-the-ground success of the financial platform.

As M-PESA usage expanded, and more was understood about the usage patterns, opportunities arose to compare approaches across different jurisdictions and contexts of use. Researchers have reported on atypical use of devices and technology such as ownership of multiple SIM cards and devices [28], and highlighted the lack of platform interoperability [34]. More recently, the monopolization of the M-PESA financial infrastructure [14] have wrought concerns on fairness, especially to the more financially vulnerable. In this landscape, researchers reported people across different countries were disadvantaged by service fees increased through the use of

[2]Short for "Cash collected on the table". This is a funding strategy–often involving women, who meet weekly and contribute a mandated amount (called a share) to a shared kitty. Members can borrow from the kitty at small agreed interest rates. At the end of the year, the interest earned (and fines paid for late fees or late attendance to meetings) are distributed to each member according to their share.

the platform, and therefore used the mobile payment system to purchase airtime, and little else beside that [19, 78]–highlighting the practical limitations of the platform in service of the UN SDGs. As it currently stands, M-PESA is not only a bank, but also a platform, and a service. Its popularity assured through the coupling with Safaricom (the largest mobile provider), and its accessibility across devices from feature phones (leveraging USSD options) to smartphones (through both SIM kits and mobile applications).

With the increased adoption of smartphones, the financial infrastructure access has morphed into the financial technology (fintech) space, where there are new affordances for users to manage their finances [32]. The financial applications typically scaffold on the M-PESA platform to enable the transfer of money. This is tightly coupled for users who do not have traditional bank accounts and rely primarily on M-PESA to provide that service.

As the applications in the fintech space have increased in number, researchers have advised caution in their design and distribution: highlighting the harms inherent in the use of western lens to explain non-western contexts that influence behaviors and communal beliefs [70]. This has been compounded by the fact that majority of smartphone-based financial applications hold the customer liable for money lost in case of fraud [59], not accounting for those that occur in transit e.g., man-in-the-middle (MITM) attacks that do not originate from the customer's device. This is underscored by the known difficulty of keeping up with changes to the permission requirements [38] and terms of use documents [30]: emphasizing the exponential financial loss through fraud–that disproportionately impact people in rural and other marginalized contexts [23, 57].

These reports highlight the scope creep of financial instruments that M-PESA heralded: from a platform to transfer and store money, to a platform that enabled borrowing of money. With these changes, associated challenges and threats have arisen, and form the basis for our approach in using the postcolonial computing lens [24] to explore how people have interacted with M-PESA as a base platform, related services that are scaffolded on the platform, and other applications in the fintech space in Kenya.

2.2 Contextual Implications on Platform Trust

We pull back the lens, and consider how cultural contexts have generally impacted device and technology use. For example, researchers have investigated the impact of communal society and sharing cultures and found nuances involved in the sharing based on needs, gender, communal obligations, etc. [9, 28]. African-based studies have found phone ownership to be skewed towards men, the educated, and older members–often from larger households with higher expenditures [6]. Other findings showcased how sharing patterns varied across friends, family groups [39] and with generational variance [31]. Device usage was also found to be impacted by access to traditional infrastructure (e.g., connection to the electrical grid), and the cost of maintenance of devices [77]. In the presence of these structural barriers, phone ownership also tended to amplify the existing inequalities–more than it served to address poverty [29, 39].

The notion of personal privacy in the context of a sharing culture has also served to reveal the nuances of gender–given geographical restrictions on movement across socio-economic and education status [23]. This has foregrounded the need to support contextual privacy/data secrecy boundaries, and to account for the shared use paradigm [1, 28]–with implications on the customer policy data requirements [18, 30], and government-mandated biometric registrations, raising concerns on surveillance [2].

Given the challenges of identity management in the face of shared device culture, researchers have considered how people establish trust–especially in spaces where there are often ethically dubious practices and lax protection of personal information [7, 59]. Studies have explored user-inferred flags on smartphone applications: popularity, customer rating, presence of privacy policy, etc., as a predictor of over-privileging of applications [12]. The findings reveal nuances, that while there was no one reliable predictor of trust, the key enablers of mobile fraud tended to be influenced by a pipeline of events: lack of informed consent, lack of education, and a sense of shame in reporting fraud [57, 58]. This is further compounded by poor communications, weak standards, and lax regulations–which in turn impact all stakeholder relationships, from the customer, to the agent, to the mobile provider [37, 43]. Trust signals, when combined with financial literacy and practices, highlight the need to design for trust: for instance through validating successful reversible/irreversible transactions and providing transparent fee structures [4].

We center these insights in this work–examining user actions in the face of these policies, seeking to understand the structural concerns: how users leverage their contextual trust signals given the protections they require; and how we might approach design to account for these factors. We also seek to understand where these trust signals fail, how they have evolved, and in case of acknowledged harm through fraud, when, how, or if trust was recovered.

2.3 Privacy and Security Considerations

Given the focus on trust and finances, and the sensitivity of information collected from users, we are also informed by research on privacy and cybersecurity scoped within the HCI for development umbrella. Researchers have considered this intersection of users, platform/app security hygiene and adversarial impact, to understand threat ramifications and the gaps they reveal, including user awareness and education and lax/unrevised policies [5]. Instrumentation studies have also highlighted the variability in the security and privacy standards, leading to the prevalence of unsecured mobile-based financial applications [3, 7, 11]. Other approaches have considered the problem from the adversarial incentives angle, seeking to understand how people fall for financial scams [69], in an effort to inform the design of resilient systems.

The lack of formal policy and privacy frameworks to inform interoperability [34], and financial regulation requirements (e.g., "know-your-customer" (KYC) compliance) to protect collected personal information, may expose customers to targeted advertising and abuse [20]. Cultural practices, knowledge gaps, unintended technology use, and long term use of devices have also added complexity and challenged the traditional security/privacy models [75].

Users are burdened with having to find responsive channels to report noncompliance [67], in addition to navigating the dearth of educative sources to inform how they defend themselves from fraud [25]. Application developers are burdened with devising structures

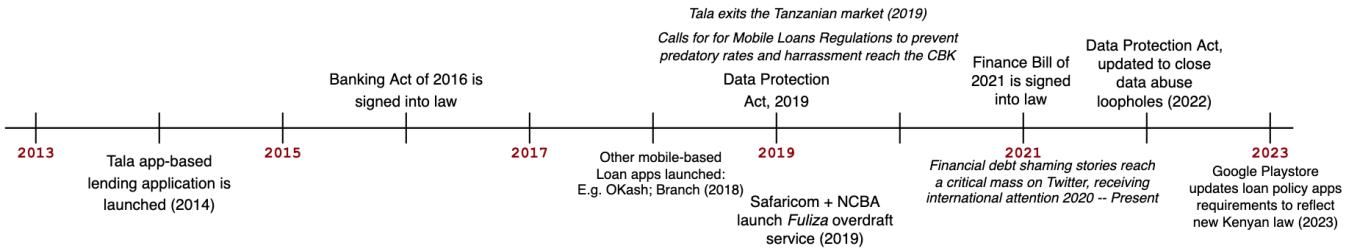


Figure 1: A ten-year timeline that highlights the gaps between the initial offering of a financial-based mobile application, when loopholes and harms were evidenced, and when policies/laws were updated or enforced.

to inform how they develop technology and handle user information in the financial space: often resulting in patchwork placeholder frameworks [22] that are difficult to replicate, and may be prone to obsolescence [10] and abuse [7]. These burdens make it more likely that the mobile-based financial services use outdated security practices, lack coherence between disclosures provided in the policy document(s) and the actual actions conducted, and lead to abdication of responsibility in cases of harm.

We focus on the harms in the contextual description below, with the aim of offering a snapshot of the current landscape given the policy historical imperatives. We expound on how adversarial methods have evolved given the changes in policy, how the users have been affected as a result, and the mechanisms by which they use to recover from harm–with implications on design, policy, and research.

2.4 Context: Mobile-Financial Landscape in Kenya

Micro loans are in the spirit of UN SDGs–enabling marginalized groups and others without credit histories to have access to loans at reasonable interest rates: avenues for lifting themselves out of poverty [22, 45]. This started in the early 90's in Kenya with microfinance institutions such as the Faulu Microfinance Bank and the Kenya Women Microfinance Bank (KWFT) both offering micro loans in addition to financial awareness training [40]. The institutions were formalized within the law in 2006 [49], and thereafter, the ubiquity of mobile phones and subscription to the M-PESA service made it possible for the microfinance infrastructure to be offered through mobile devices. These mobile-based unsecuritized[3] loans are typically between Ksh. 100 and Ksh. 20,000[4], with a 30-day payment period at roughly 7% monthly compounded interest rate (when annualized, can translate to roughly 90% interest–compared with ~13% per annum that is the threshold set by the Central Bank of Kenya for regular bank loans) [52].

In 2012, M-Shwari–a USSD-based loan service was released by the mobile provider Safaricom (serviced through Commercial Bank of Africa) as an online-only service [63]. This provided an opportunity for subscribers who used M-PESA for storing and sending money, to become eligible to borrow loans. The leveraging of Safaricom's wide reach across the country and the existing infrastructure, as well as the users' familiarity with the M-PESA interface, made the program a success. This led to other USSD and venture-backed app-based competition: Tala in 2014 [68], followed in 2018 by Branch, OKash and others [60]. Notably, **there was lack of sufficient oversight for these new financial offerings**, and the market was rife with prohibitively high interest rates and short repayment periods that disadvantaged the very same people who stood to most benefit from access to microloans.

As a remedy for the unfair interest rates and the disproportionate impact this had on marginalized groups, the Kenyan government enacted the Banking (Amendment) Bill of 2016 [50]: limiting the interest rates to not exceed the threshold set by the Central bank of Kenya (CBK). However, this failed after a court challenge by the financial institutions–who argued that mobile loans were exempt from the interest caps set by the new law, since they were classified as microfinance entities: their terms agreement showcasing that they charged "facilitation fees" and not the traditionally understood "interest rates". In practice, this also meant that unpaid micro loan balances were also charged a "roll-over fee" (essentially a compound interest) after 30 days [21]–at a rate that was far above what was set by the CBK. This was done with the knowledge that **feature phone users had no access to these online policy documents**, and further led to onerous burdens on people who often found themselves in debt almost twice the size of the original loan.

Users who sought app-based microloans were usually required to surrender their contact list and transaction history as conditions for loan approval. **Access to these details were often abused by the lenders**: as they called the people in the borrower's contact list to ask them to relay messages to the borrower to repay their defaulted loan. This practice of shaming borrowers and the general terrible user experiences created enough national and international furor [33, 42, 46, 48, 61] that the Banking Act was amended in 2021, and the CBK was formally placed by law as the governing authority over all loan-provision services including mobile-based microfinance loans [51]. This finally closed the five-year loophole on the microfinance exemptions on interest rates. In addition, the Data Protection Act was amended to curb the abuse of personal and financial information [53], and additionally required the digital lenders to submit a proof of license to operate in Kenya–extending the CBK's governance to include loan-service apps that are available in the app stores [47]. Figure 1 provides a timeline overview.

[3]Unsecuritized means that there are no traditional forms of collateral used to secure the loan, making it a higher risk for the entity offering the loans. The risk is offset by the lower amount offered and higher interest rates charged.
[4]Roughly $1 to $200 in US Dollars

Code	Gender	Age	Occupation	Code	Gender	Age	Occupation
P1	Woman (W)	18	Student	P11	M	63	Retired Office Worker
P2	W	20	College Student	P12	M	68	Business Man
P3	Man (M)	24	University Graduate	P13	W	72	Retired Civil Servant
P4	M	25	Shopkeeper	P14	W	79	Volunteer (Wildlife Services)
P5	M	28	Entrepreneur (Livestock)	P15	W	81	Entrepreneur (Hospitality)
P6	W	32	Museum Docent	P16	M	86	Farmer
P7	M	41	(Religious) Ministry Worker	P17	M	91	Retired Farmer
P8	M	53	Driver				
P9	W	60	Green Grocer				
P10	W	61	Retired Teacher				

Table 1: Summary of interview participants ranked by age (from 18 years to 91 years). The occupations are self-described by participants. We include addendum in parenthesis to provide additional context.

3 Method

We interviewed 17 participants (8 women, 9 men), aged between 18 and 91 years (Median 53.1) across three locations in Kenya: Nairobi (the capital city), Mombasa (a coastal city) and the rural areas surrounding the highland town of Eldoret. The participants were recruited through convenience sampling–from quick surveys and word of mouth–the first author having had a long-term research relationship in various locations in Kenya. We sought participants who had had experiences with, or had been witness to attempted and/or successful tech-enabled harms, and we further restricted this to those who had borrowed money using mobile-loan services and were aware if not on exact interest rate, then the exact amount of money either deducted from the initial loan remitted or the extra amount required to be repaid.

The interviews provided opportunities to incorporate participants in urban and rural contexts; those who had different familial responsibilities: with variance in literacy skills, socio-economic status, and technological know-how. The interviews were conducted either in person at locations we set up, or in public settings according to participants preferences e.g., shopping centers, cafes, or a participant's place of business (Table 1 provides a summary). When feasible, participants were encouraged to share screenshots to support their interview–these were collected through a survey [15]. The study underwent institutional ethics review and approval.

We sought to understand how the participants leveraged mobile-based financial transactions using M-PESA and other applications involving money transfer, savings and loans. We were interested in their understanding of the nuances of interest rates and penalties for late repayment, in addition to other experiences of lost money (or near misses) due to outright fraud. We iteratively sought responses with each participant until we could no longer add new experiences and/or noted multiple redundancies in their responses. In elucidating their experiences, the participants offered insights on how they coped with threats/known harms, and if applicable and available, the tools and resources they leaned on for support and guidance.

Each interview lasted between 20 and 50 minutes, and was conducted in English or Kiswahili according to a participant's preference, and was also audio recorded with permission. The interviews were led by the first author who is Kenyan born and raised: with fluency in both languages and their variance–the background serving to engender trust, and support open conversations with the participants. Each participant received Ksh. 500 (≈$3 USD) in remuneration.

3.1 Analysis

We assembled a written corpus to use in the analysis. The corpus consisted the transcribed and translated transcripts from the audio files, additional notes from the interviews and the descriptions of participant-contributed artifacts (e.g., SMS Screenshots). We used open coding to elicit concepts and subsequently grouped them into categories that help to explain themes based on participants' experiences [13]. We then supported the themes using contextual details given the mobile-based financial landscape in Kenya, as detailed in Section 2: framing the participants' experience given the background and insights surrounding the Kenyan financial landscape that is otherwise inappreciable when considering individual/isolated situations. We discuss our findings using postcolonial computing [24] as lens. This approach provides the space to contend with colonial influence on the designs, contrast cultural approaches to technology use, and the power asymmetries inherent in the technology design and infrastructure enabled by technology.

4 Findings

Through their awareness and experience with the M-PESA infrastructure, the participants articulated their means of determining trust signals of legitimate transactions (*origin signals, spam filters* and *claim verification*), and how they navigated and/or understood how others navigated through similar issues–including the impact to personal dignity if tricked by deceptive transactions.

4.1 Awareness and Verification

Participants utilized various signals to distinguish between legitimate and deceptive financial-related messages–with most implementing different aspects of **origin signals**. For Safaricom subscribers, the short code assigned to M-PESA system often has the name "MPESA" as pre-filled contact without having to be saved in a subscribers address book (as shown in Figure 2).

> *"I didn't know at first glance it was a scam until I realized that it was a message from an individual number,*

> *not the official M-PESA number..." (P14) "[...] it actually seemed real but the message itself was not sent through the M-PESA code, and then instead of showing you the balance in the message, it instead said 'locked': definitely a scam." (P1)*

The M-PESA short-code message service supports only one-way (outgoing) communication. Some participants classified messages as deceptive if they did not follow expected behavior of legitimate messages.

> *"I noticed two things: the message came from a personal phone number, and also supported replies." (P6)*

Other participants leveraged **device or platform-provided** spam filters supported natively in their devices or through third-party applications, to automatically identify deceptive messages:

> *"My phone has an internal spam detector so the message was automatically archived as spam ..." (P5) "[...] I have Truecaller[5] installed on my phone and some of these messages come directly into my spam folder in Truecaller." (P2)*

Participant approaches that leveraged **claim verification** did so in two ways: first by verifying their balance directly through typical practice, for example: *"The message said I had received money in my M-PESA account but when I checked my account there wasn't any money" (P7).* Alternative approaches verified claims by employing third-party verification:

> *"The message indicated that I should deposit my rent to a new account number and that it was a change from the management. I had just spoken to them in person in the past week and they hadn't said anything so when I called to understand the change, that is when I found out that they were not the ones who had sent the text, and it was probably a scam. The message was very believable though." (P8)*

The experience by P8 evidences both the changing deceptive strategies and the limited knowledge-base that users have to determine veracity. For example, while the participants could easily identify the parent/child deception category (*"The sender wanted me to send money to buy a calculator for a son at a certain high school, but I'm not a parent" (P2)*), whenever the deceptive message better matched a user's context, determination was murky.

> *"They had texted me that the rent paying account number had changed. I almost fell for it because I didn't have the number of our caretaker so I tried calling the number to confirm, but it was unreachable." (P4)*

Other deceptive approaches take advantage of the likelihood of young adults to be job searching and expected involvement of financial corruption to craft believable messages. While there are circumstances where verification using trusted circles (as exemplified in Figure 3) is possible, this is not uniform.

> *"I went through an interview process and was very hopeful that I would get the job, but then they texted me after the call with the same number requesting for money for me to get the job. I thought it was just the usual corruption stuff, but I found out later that this is a common scam, and they didn't actually have any jobs available." (P3)*

Deceptive practices extended to approaches accounting for other demographic characteristics and their likely financial-related practices such as M-PESA supported betting: a common practice aided in part by majority of radio and TV stations that offer betting-related trivia competitions.

> *"They actually called me and said they were from [radio station] and that I had won the betting sweepstakes, but that I should first send some money to a paybill number before they would then send the rest of the money. It is true that I participated in the sweepstakes, but who would ask you to pay money to then get more money? It didn't make any sense." (P9)*

The various means of verification were based on user-elicited signals. While the participants were aware of mobile-providers campaigns to create awareness for deceptive practices, the specifications and strategies provided in these campaigns did not feature in the participants' own practices.

4.2 Responsibility, Dignity, and Shame

Participants also employed different strategies for navigating mobile-enabled micro loans. Emergent themes surrounded **dignity** and **shame**–chiefly in the context of borrowing loans. By virtue of surrendering access to their contact list as a condition for mobile loan approval, borrowers were liable to experience any person on the list being called by the loan provider as a tactic to compel and shame the borrower into repaying the loan. Shame as a theme also extended to participants' feelings after having been defrauded.

Older participants were also likely to have abbreviated formal education and experience with the M-PESA USSD menu. One participant (P16), beyond noting that they had lost money, declined to articulate how they were defrauded and the amount they lost.

> *"I can't tell you. It was too bad [...] it led me to lose a lot. My family does not know this, actually I've never told anyone. I don't want them to know about it." (P16)*

The success of deceptive strategies that focused on micro-loan provision can be attributed to those with no borrowing history–often first time users of loan offerings through M-PESA. These users have little awareness over fair rates and had no choice but to accept onerous repayment requirements. They are also more likely to hesitate reporting their loss, as they often deem their cases as too insignificant to be taken seriously by the Directorate of Criminal Investigations (DCI)–the government agency with oversight over fraud investigations.

> *"They sent me a message claiming that they were giving away [Bank Name] loans at an interest of 20% and they give you a number to call. When I called, they told me to send money as a service fee to them for the loan to be disbursed. It was a reasonable fee, especially given the loan I was to receive [...] But then I never heard from them again." (P1)*

[5] A third-party crowd-sourced caller ID service. https://www.truecaller.com/

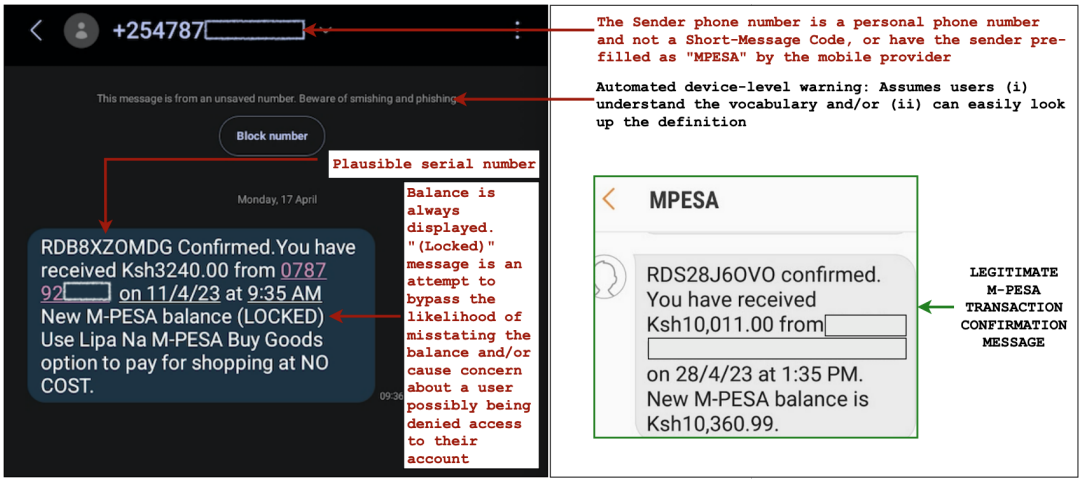


Figure 2: Example of an M-PESA scam: Fake confirmation deposit originating from a personal number. An inset text message showcases what the transaction details provided in legitimate confirmation message.

Neither the farmer (P16) nor the student (P1) reported the numbers used to deceive them to authorities. The student knew the means to report to the service provider, but felt that since the mobile provider did not have the reach and effectiveness of the government agency, they would not be of help in restoring the money lost.

With the low reporting incidences and assumptions to navigate unassisted through their losses, the participants compensated for their lack of control by withdrawing to known maxims: elevating their technology distrust levels and/or reverting to proven verification means. For some, harassment through unceasing phone calls led them to revert to solely relying on locally-organized microfinance structures, abandoning mobile-based services altogether.

> *"I got tired of the phone calls [from mobile-based loan providers]. Now I would rather borrow from my "chama" [table-banking group] than to go through all of that again." (P11)*

Other participants became wary of unsaved numbers as they had previously fallen victim to the financial fraud. They considered the scammers as untouchable and had no recourse in stopping the harassment.

> *"The scammers claim to be the true agents because they have your information. But they use vulgar language when you catch on to their trick. I don't think they care if you report them." (P10)*

The relative age of the two participants (P10 and P11) above also reflect the general patterns of behavior we observed across the rest of the participants. The older participants often had one phone number they had owned throughout their history of mobile ownership and so their strategies would resort to ignoring phone calls and messages as a tactic to avoid harassment from loan-providing agencies and scammers.

The younger participants approached this challenge by purchasing new alternate phone numbers, and then sought and used devices with dual SIM card capability, or handled multiple devices with separate use. While this will not erase their financial history, nor have an impact in improving/lessening their loan eligibility, it is a step that they found useful in addressing the harassment element.

> *"I have separated my life. I use one line for calling and texting regularly, and use the other line for M-PESA and Equitel [bank] services. (P5)*

The use of multiple phone lines had additional utility for avoiding overdraft repayment strategies. M-PESA has a *fuliza* service affording users with the capability to overdraft their M-PESA account with a daily interest of 1% and a repayment period of 30 days [65]. After this period, any money received through M-PESA would automatically be used to defray the *fuliza* balance before the recipient can access any remaining amount.

> *"I have two M-PESA accounts. The original one has fuliza [overdraft loan] on it. So I always have to be careful to specify which number I give to receive cash or airtime." (P4)*

The coping strategies that users adopt as a result of this landscape highlight the impact of trust not only to the specific offending services, but also on the whole financial landscape.

4.3 Impact on Agency and Privacy

Beyond the individualized trust signals and coping strategies, there are larger tension patterns that emerge: First, the notion of **agency**. Older participants were more likely to be targeted with, and believe SMS-type scams that request financial assistance, while the younger members were more likely to fall into loan/financial-access related scams. The eldest members leaned more on others to verify their transactions–distrusting their own judgment.

> *"I stopped sending the money myself. I wait until [family] is around and have them help." (P17)*

While this supported use provides a measure of trust, there is an emerging tension that this necessity erodes personal agency in addition to deepening dependency on others to understand nuances on scams. This upends the cultural community hierarchical order

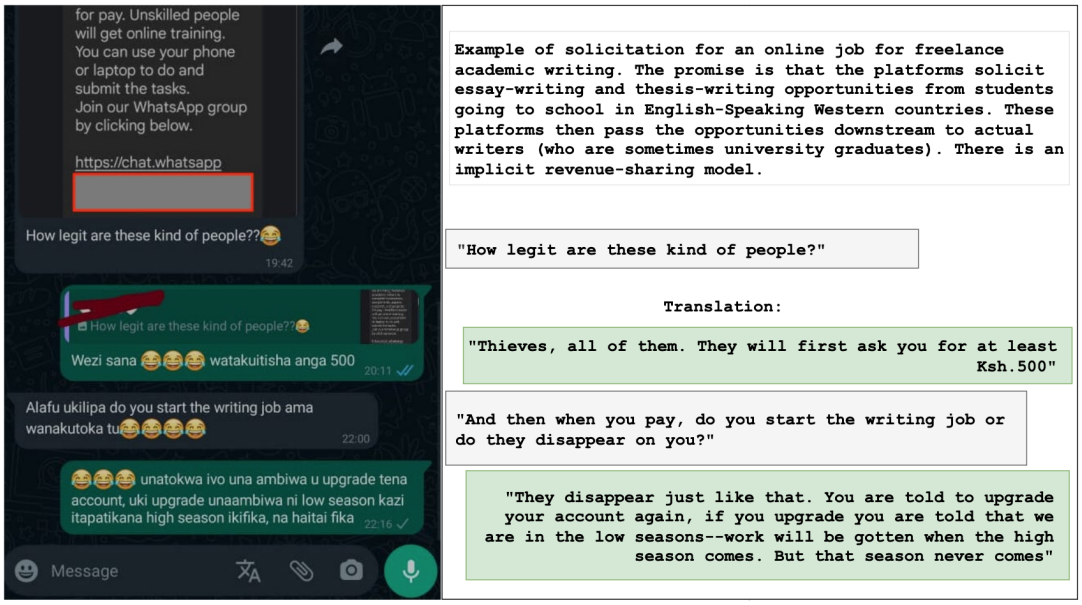


Figure 3: Participant-shared example of how a young adult leveraged their trusted circle to determine the trustworthiness of a job opportunity in an ethically-gray area. They sought to understand the deceptive approaches and potential financial loss.

where elders are depended upon to dispense wisdom and guide actions–into elders viewed as dependents: stripping their dignity.

Second, beyond the age considerations, the different participants exposure to the different types of fraud highlight the nuances between literacy (ability to read and write) and education (deductive reasoning and awareness). This is showcased by how smartphone users are still at a disadvantage to new exploitation mechanisms.

> *"You know, I am even suspicious of shopping apps and the like. A friend recommended this app but on install, it started sending messages to my contacts pretending to be me and asking for an amount of money. I mean, I didn't think that was even possible to be tricked like this and I have a university degree." (P3)*

Only two participants knew how to search for the terms and conditions documents to one/multiple of the mobile-based application in their devices. Participants with smartphones had trouble parsing the language used in the terms and conditions documents. Participants with feature phones–who could read, could not access the document at all as their devices were not equipped with internet capability: highlighting the tension between **education** and **access**.

Third, the inaccessible language describing how the technical mechanisms of mobile-based transactions occur. This is in addition to the lack of transparency over how the systems work, information collected, and how that information is shared. This combination has served to increase suspicion and highlight the user burdens in managing the repercussions wrought by the shared information: chiefly, **technology and data suspicions**.

> *"They knew details about me, I don't know how they got them. I felt like I was being monitored and did not feel safe because I felt like I was very susceptible to lose my little cash." (P2)*

The college student (P2) concerns surfaces not only the technological ability of the attackers, but also in the lack of clarity about data origins. People often infer their data to have originated from the app-based mobile service providers–given their rampant violation of privacy boundaries. The updated personal privacy law (2019) in Kenya is intended to protect against the unanticipated use of collected information. However, it fails to adequately address how personal information is collected/stored/reused, which we anticipate will have continued impact on the consumers' use of other measures of control.

5 Discussion

Through this work, we sought to understand how participants navigated the use of mobile-based financial infrastructure afforded by the M-PESA platform and service, how they established trust in operations, and handled the threats engendered by the close coupling of personal SIM card with finances. In this section, we situate our findings within other research: to critically examine the technology affordance, and use the insights to offer recommended steps to approach the scrutiny, the design and the responsibility for technology–especially those intended for developmental contexts.

5.1 Interventions for Exploitation Disparities

Access to financial instruments for the unbanked in Kenya has been supported by the easy availability of mobile-based micro loans. However, as the participant experience has shown, access to the financial infrastructure cannot be associated with equitable access. While mobile-based financial infrastructure addressed the scaling limitations inherent in the traditional microfinance infrastructure [40] and table banking/*chamas* [26], the profit motives have served to undermine aims inspired by both the UN Millennium and UN

Sustainability goals. The prohibitively high interest rates [55] compared with reasonable rates provided to those with access to conventional bank accounts [52] highlight the key disparity: that the low-resourced often face unavoidable worse options.

Describing the mobile-based financial landscape amplified by the M-PESA platform underscored the policy aspects of the mobile-loan services and highlighted the fact that deliberately designed application actions–even when negatively impacting marginalized users, were in compliance with prevailing laws [46, 56]. It is only when policies were amended and oversight instituted, that protective mechanisms were finally put into place. This action was only possible due to unceasing demands from stakeholders who were able to showcase systematic harms. We note this example to highlight that existing claimed ethical guidelines were used to exaggerate compliance and advantages of access, but did not explore the impact of harms, nor equitable access to financial infrastructure. Researchers have highlighted how traditional design decision-based signals such as app-permissions [38] and terms of use documents while they have been unable to highlight the harms to the users, provide opportunities to audit and showcase systematic harms especially when the providers do not follow their documented policies [60]. The experience shared by participants further underscored their lack of access, lack of trust and lack of understanding of the terms and conditions documents: a feeling that extended to their felt lack of recourse in case of impacted finances.

5.2 Trust Signals and Strategies for Risk Mitigation

Validation strategies leveraged by mobile users on **what** financial-related messages are legitimate include assigning trust to text messages originating from short-code numbers [64] and scrutinizing the serialization of receipt numbers on M-PESA receipts (as demonstrated in Figure 2). These design and stylistic-based approaches are failure-prone to new deceptive strategies that thwart user scrutiny, or if the mobile provider amends how messages are conveyed.

This landscape highlights the need for asking for caution on how new user requirements are effected. This is compounded by the tensions in policy updates intended to protect the users, the burdens that the compliance places on the most marginalized, and the opportunity for deceptions in the gap. For example, to protect user M-PESA account security that were risked by the use of counterfeit devices, the government in 2012 mandated that everyone had to own an IMEI[6]-registered device, with a switch-off planned for unregistered devices [76]. The most impacted were users who could not distinguish between counterfeit and authentic devices, and when those devices were switched off, they often could not afford new devices. Similar patterns emerged ten years later, when Kenyans were mandated to register their SIM cards in order to verify ownership and curb the use of SIM cards in fraudulent schemes [74]. However, it was left to the service providers to enforce registration compliance. As a result, new verification deception tactics found success in targeting those without proper documentation or who could not physically travel to present their documentation to a service provider agent.

[6]IMEI: International Mobile Equipment Identity-a unique numeric handset identifier.

The participants experience underscore that the mechanisms of **how** the deceptive strategies work–are complicated by lack of sufficient explanation from official methods–often because fraudsters leverage lesser known USSD codes to lead users to unknowingly perform actions that make them liable for attacks such as SIM-swapping [73]. The official guidance about these sophisticated attacks are vague [72], providing no specifics to aid the user in defending themselves [66]. We found that even when the participants knew about the anatomy of a scam (i.e **what** it was), they could not articulate **how** it worked. What enforcement mechanisms exist are balkanized, because platforms are informally tasked with enforcing compliance. The prosecutorial powers are wielded only when large amount of money is lost. the severity engendering attention. There is an additional element of shame to being duped by these types of scams which serve to dampen the likelihood of victims reporting and proactively warning others. Participants often expect to absorb the losses–even when they use mechanisms provided by the platform to report scams for review and potential remediation.

The issues brought about by the process of achieving policy compliance adds to the HCI research that has explored how people across different contexts have navigated the challenge. For example, highlighting the data concerns in the process of compliance whether this is expressed [67], or reflected through user actions [2]. This, in addition to the wrong assumptions and lack of uniformity in eliciting trust signals for determining trust of app-based systems [38], and the surfacing of lack of warning systems to users who face threats to their financial posture through text messages [58].

The three dimensions: (i) validation strategies to inform trust signals; (ii) how the users understood the deception to work; and (iii) their use of protective authorities to report cases of fraud, or to seek remedy; inform the user awareness and sensitivity to these types of financial threats and represent the goal for designers and researchers to address the policy gaps and support the users in ways to mitigate possible harms.

We found that successful risk mitigations revolved around verification, and involved users triangulating for trust–their methods dependent on the resources at hand: calling a second source, verifying with trusted circle, leveraging official dedicated service-provider lines, etc. This was true for both older adults who are likely to fall into deception involving threats towards policy compliance, and young adults who are more likely to fall victim as they seek access to income or mobile-based loans. The triangulation mechanisms should ideally operationalize steps from awareness campaigns, which in turn will demystify how the deceptive operations work. In this manner, design approaches will be accountable to users in supporting their agency, and augment their existing trust structures across literacy skills, education level and technology know-how.

5.3 Supporting Harm Recovery

HCI research has highlighted how the use of off-the-shelf technology is a poor fit for use in developmental contexts [8]. The building of M-PESA showcased a successful case that was built based on learning from how people locally approach financial transactions [22]. Its sustained success is a testament for this design approach. However, the acceleration of the financial tech space, and the profit

motives submerging developmental goals have served to undermine any original design intent–and often disadvantages users long after they have ceased using the technology. This is observed by how these approaches have spurred changes in user behaviors to protect their privacy and agency: in some cases, leading them to view technology with suspicions or abandoning use altogether.

Participants' needs on supporting harm recovery involve two policy-driven aspects: restoring lost funds to users; and in penalizing the abusers. The latter is now being effected in Kenya: the new policies guiding charges and fines for breaching data laws [41] and on deceptive scams perpetuated by individuals [72]. They form the genesis of justice process, but there is a long way to go to identify the marginalized users and enact fair adjudications. There is need curb the shame in this domain and processes: by demystifying how scams operate, illustrating the underlying schemes, creating awareness of deceptive patterns, showcasing scale, and creating redundancies in support by empowering users with knowledge–strategies that all fall within designers' purview. This can be done in addition to reevaluating how to explain terms to users with no access to internet, or an understanding of the English language–and ultimately exposing when platforms act against standing policies and the terms and conditions they provide to users.

5.4 Other Design Guidelines and Implications

Researchers have identified mechanisms for conducting research with underrepresented communities, and have studied the impact of technology design for/with these communities from postcolonial [24] and decolonial approaches [62]. For design mechanisms that offer services and/or audits to be successful, the metrics of success need to transcend simply "poverty reduction" and to consider users' mental models regardless of their literacy level: a measure of awareness; of understanding of the threat landscape; and importantly, how they can defend themselves–as means of supporting their agency in decision making and therefore their own pathways for addressing poverty.

For design-based recommendations to be effective, they have to be undergirded by on-the-ground policies. However, as we have found, the policies are often enacted when there is sufficient proof or a crisis point. In this way, design approaches should be in service to the users by offering knowledge, support and infrastructure: demystifying the decision-making structures, easing the process of understanding compliance, and providing comparisons–highlighting existing disparities. This meta approach we argue, beyond providing reference and tools for users to advocate for themselves, would also be in service of policy makers to determine courses of action that do not depend on sufficient marginalized users being harmed as an impetus and proof.

Successful and reparatory design-based recommendations ought to lean into the supportive financial infrastructure and organization: learning from similar approaches leveraged in locally-organized table-banking/*chamas* and how the group sustains and supports individual members. This should be in addition to the spirit of microfinance offerings–with the intent to empower the borrowers context-specific financial advice as well as providing access to capital at fair rates.

The affordance tensions presented in this paper represents ongoing struggles with development and advantages of access, and highlight the cyclical patterns of how harms are effected. To wit, initial projects are provided with development agenda, then the profit opportunity become apparent as new users are identified, after which new providers emerge to take advantage of the market, followed by the profit motives causing harm to same users who were marginalized. Therefore, new/updated policies are effected to mitigate harms... then the cycle repeats. The case study on mobile-based loans showcases how this issue cycle has abided since 2013–and can be considered as a clarion call to examine other dimensions of provisions intended for marginalized users [54] and the emerging concerns about disparities enabled through design.

5.5 Limitations and Future Work

We specifically recruited participants with experience of tech-enabled harms in the context of the Kenyan financial landscape, and further restricted this to those who had experience with borrowing money through M-PESA, financial applications that scaffold on the M-PESA service, or applications relying on traditional banking service. We included a diversity of users across urban and rural areas, with various literacy and socio-economic backgrounds and technological know-how. These inclusion/exclusion criteria resulted in 17 participants. While this was useful for coherence and depth in understanding of the financial harms, the sample size is limited, and may impact generalizability across other financial experiences.

Future work should consider the broader financial landscape, increasing the possibility to provide nuances of the financial offerings, and providing comparisons across individual, group, and systematic-based contexts. This focus will provide an understanding of the financial landscape and asymmetric impacts, and make possible longitudinal analysis and sufficient scale for comparisons with other financial landscapes outside of the Kenyan context.

6 Conclusion

We explored the usage of mobile-based money transfer and loan servicing applications: the affordances and access it provides to the marginalized, but also the weakness of policy and ethical guardrails to protect users on account of fraud and scams. We interviewed 17 participants who use these services to understand their contexts of use, the challenges that they face, and to highlight the gaps in policy, research and design presenting insights on individual actions based on evasion of harm, harm encounter, and harm recovery.

We presented strategies for contextual design considerations learned from how participants use their devices. This was borne out of how they interact with prevailing systems–even as they are aware that they are being harmed in the process–but having no choice in the matter. This highlights the dearth of governing policies to support users, and provide opportunities for researchers and designers to offer utilities in support of user awareness, and to aid policy-makers by creating tools and designs to offer clarity in the performance of existing protective guardrails, and where needed, spotlight the necessity for new approaches to address evolving technology.

References

[1] Syed Ishtiaque Ahmed, Md. Romael Haque, Jay Chen, and Nicola Dell. 2017. Digital Privacy Challenges with Shared Mobile Phone Use in Bangladesh. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW, Article 17 (dec 2017), 20 pages. https://doi.org/10.1145/3134652

[2] Syed Ishtiaque Ahmed, Md. Romael Haque, Shion Guha, Md. Rashidujjaman Rifat, and Nicola Dell. 2017. Privacy, Security, and Surveillance in the Global South: A Study of Biometric Mobile SIM Registration in Bangladesh. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 906–918. https://doi.org/10.1145/3025453.3025961

[3] Waqas Ahmed, Aamir Rasool, Abdul Rehman Javed, Neeraj Kumar, Thippa Reddy Gadekallu, Zunera Jalil, and Natalia Kryvinska. 2021. Security in Next Generation Mobile Payment Systems: A Comprehensive Survey. *IEEE Access* 9 (2021), 115932–115950. https://doi.org/10.1109/ACCESS.2021.3105450

[4] Savita Bailur and Hélène Smertnik. 2021. Making Digital Financial Services More Trustworthy for Women. *Interactions* 28, 2 (mar 2021), 104–107. https://doi.org/10.1145/3448556

[5] Yahel Ben-David, Shaddi Hasan, Joyojeet Pal, Matthias Vallentin, Saurabh Panjwani, Philipp Gutheim, Jay Chen, and Eric A. Brewer. 2011. Computing Security in the Developing World: A Case for Multidisciplinary Research. In *Proceedings of the 5th ACM Workshop on Networked Systems for Developing Regions* (Bethesda, Maryland, USA) *(NSDR '11)*. Association for Computing Machinery, New York, NY, USA, 39–44. https://doi.org/10.1145/1999927.1999939

[6] Joshua Blumenstock and Nathan Eagle. 2010. Mobile Divides: Gender, Socioeconomic Status, and Mobile Phone Use in Rwanda. In *Proceedings of the 4th ACM/IEEE International Conference on Information and Communication Technologies and Development* (London, United Kingdom) *(ICTD '10)*. Association for Computing Machinery, New York, NY, USA, Article 6, 10 pages. https://doi.org/10.1145/2369220.2369225

[7] Jasmine Bowers, Imani N. Sherman, Kevin R. B. Butler, and Patrick Traynor. 2019. Characterizing Security and Privacy Practices in Emerging Digital Credit Applications. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks* (Miami, Florida) *(WiSec '19)*. Association for Computing Machinery, New York, NY, USA, 94–107. https://doi.org/10.1145/3317549.3319723

[8] E. Brewer, M. Demmer, B. Du, M. Ho, M. Kam, S. Nedevschi, J. Pal, R. Patra, S. Surana, and K. Fall. 2005. The case for technology in developing regions. *Computer* 38, 6 (2005), 25–38. https://doi.org/10.1109/MC.2005.204

[9] Jenna Burrell. 2010. Evaluating Shared Access: social equality and the circulation of mobile phones in rural Uganda. *Journal of computer-mediated communication* 15, 2 (2010), 230–250.

[10] Sam Castle, Fahad Pervaiz, Galen Weld, Franziska Roesner, and Richard Anderson. 2016. Let's Talk Money: Evaluating the Security Challenges of Mobile Money in the Developing World. In *Proceedings of the 7th Annual Symposium on Computing for Development* (Nairobi, Kenya) *(ACM DEV '16)*. Association for Computing Machinery, New York, NY, USA, Article 4, 10 pages. https://doi.org/10.1145/3001913.3001919

[11] Sen Chen, Lingling Fan, Guozhu Meng, Ting Su, Minhui Xue, Yinxing Xue, Yang Liu, and Lihua Xu. 2020. An Empirical Assessment of Security Risks of Global Android Banking Apps. In *Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering* (Seoul, South Korea) *(ICSE '20)*. Association for Computing Machinery, New York, NY, USA, 1310–1322. https://doi.org/10.1145/3377811.3380417

[12] Pern Hui Chia, Yusuke Yamamoto, and N. Asokan. 2012. Is This App Safe? A Large Scale Study on Application Permissions and Risk Signals. In *Proceedings of the 21st International Conference on World Wide Web* (Lyon, France) *(WWW '12)*. Association for Computing Machinery, New York, NY, USA, 311–320. https://doi.org/10.1145/2187836.2187879

[13] Juliet Corbin and Anselm Strauss. 2023. *Basics of Qualitative Research (3rd ed.): Techniques and Procedures for Developing Grounded Theory.* SAGE Publications, Inc., Thousand Oaks, Chapter 8 - 10, 159 – 245. https://doi.org/10.4135/9781452230153

[14] Christopher Csikszentmihalyi, Jude Mukundane, Gemma F. Rodrigues, Daniel Mwesigwa, and Michelle Kasprzak. 2018. The Space of Possibilities: Political Economies of Technology Innovation in Sub-Saharan Africa. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3173574.3173880

[15] Amelia Dogan, Meira Gilbert, and Lindah Kotut. 2025. Easy Come, Easy Go: Phone Enabled Small-Scale Financial Grift. In *Proceedings of the 8th ACM SIGCAS/SIGCHI Conference on Computing and Sustainable Societies* (Toronto, Canada) *(COMPASS '25)*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3715335.3736315

[16] Jonathan Donner. 2008. Research approaches to mobile use in the developing world: A review of the literature. *The information society* 24, 3 (2008), 140–159. https://www.tandfonline.com/doi/full/10.1080/01972240802019970

[17] The Economist. 2013. Airtime is money: The use of pre-paid mobile-phone minutes as a currency. https://www.economist.com/finance-and-economics/2013/01/19/airtime-is-money.

[18] Shikoh Gitau, Gary Marsden, and Jonathan Donner. 2010. After Access: Challenges Facing Mobile-Only Internet Users in the Developing World. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Atlanta, Georgia, USA) *(CHI '10)*. Association for Computing Machinery, New York, NY, USA, 2603–2606. https://doi.org/10.1145/1753326.1753720

[19] Eva Gutierrez and Tony Choi. 2014. Mobile money services development: the cases of the Republic of Korea and Uganda. https://elibrary.worldbank.org/doi/abs/10.1596/1813-9450-6786

[20] Andrew Harris, Seymour Goodman, and Patrick Traynor. 2012. Privacy and security concerns associated with mobile money applications in Africa. *Wash. JL Tech. & Arts* 8 (2012), 245. https://digitalcommons.law.uw.edu/wjlta/vol8/iss3/5/

[21] David Herbling. 2016. Banks come under pressure over expensive M-Pesa loans. https://www.businessdailyafrica.com/corporate/Banks-come-under-pressure-over-expensive-MPesa-loans/539550-3382958-3o35laz/index.html.

[22] Nick Hughes and Susie Lonie. 2007. M-PESA: mobile money for the "unbanked" turning cellphones into 24-hour tellers in Kenya. *Innovations: technology, governance, globalization* 2, 1-2 (2007), 63–81. https://direct.mit.edu/itgg/article/2/1-2/63/9485/M-PESA-Mobile-Money-for-the-Unbanked-Turning

[23] Samia Ibtasam, Lubna Razaq, Haider W. Anwar, Hamid Mehmood, Kushal Shah, Jennifer Webster, Neha Kumar, and Richard Anderson. 2018. Knowledge, Access, and Decision-Making: Women's Financial Inclusion In Pakistan. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies* (Menlo Park and San Jose, CA, USA) *(COMPASS '18)*. Association for Computing Machinery, New York, NY, USA, Article 22, 12 pages. https://doi.org/10.1145/3209811.3209819

[24] Lilly Irani, Janet Vertesi, Paul Dourish, Kavita Philip, and Rebecca E. Grinter. 2010. Postcolonial Computing: A Lens on Design and Development. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Atlanta, Georgia, USA) *(CHI '10)*. Association for Computing Machinery, New York, NY, USA, 1311–1320. https://doi.org/10.1145/1753326.1753522

[25] Pranjal Jain, Rama Adithya Varanasi, and Nicola Dell. 2021. "Who is Protecting Us? No One!" Vulnerabilities Experienced by Low-Income Indian Merchants Using Digital Payments. In *ACM SIGCAS Conference on Computing and Sustainable Societies* (Virtual Event, Australia) *(COMPASS '21)*. Association for Computing Machinery, New York, NY, USA, 261–274. https://doi.org/10.1145/3460112.3471961

[26] CM Kariuki and PK Ngugi. 2014. The effect of table banking on the performance of micro and small enterprises in Nairobi County. *International Journal of Current Business and Social Sciences* 1, 2 (2014), 339–360.

[27] Minjin Kim, Hanah Zoo, Heejin Lee, and Juhee Kang. 2018. Mobile financial services, financial inclusion, and development: A systematic review of academic literature. *The Electronic Journal of Information Systems in Developing Countries* 84, 5 (2018), e12044. https://onlinelibrary.wiley.com/doi/full/10.1002/isd2.12044

[28] Lindah Kotut and Hummd Alikhan. 2024. "Things on the Ground are Different": Utility, Survival and Ethics in Multi-Device Ownership and Smartphone Sharing Contexts. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3613904.3642874

[29] Lindah Kotut and D Scott McCrickard. 2020. Amplifying the Griot: Design Fiction for Development as an Inclusivity Lens. *EasyChair Preprint* -, - (2020).

[30] Lindah Kotut and D. Scott McCrickard. 2022. The TL;DR Charter: Speculatively Demystifying Privacy Policy Documents and Terms Agreements. *Proc. ACM Hum.-Comput. Interact.* 6, GROUP, Article 23 (jan 2022), 14 pages. https://doi.org/10.1145/3492842

[31] Lindah Kotut and D. Scott McCrickard. 2022. Winds of Change: Seeking, Preserving, and Retelling Indigenous Knowledge Through Self-Organized Online Communities. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 257, 15 pages. https://doi.org/10.1145/3491102.3502094

[32] Makayla Lewis and Mark Perry. 2019. Follow the Money: Managing Personal Finance Digitally. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3290605.3300620

[33] Felix Maringa and Abu-Bakarr Jalloh. 2023. Millions of Kenyans indebted to mobile app lenders. https://www.dw.com/en/millions-of-kenyans-indebted-to-mobile-app-lenders/a-65349197.

[34] Bossi Masamila. 2014. State of mobile banking in Tanzania and security issues. *International Journal of Network Security & Its Applications* 6, 4 (2014), 53. https://doi.org/10.5121/ijnsa.2014.6405

[35] Moses Muia Masika, Gregory Barnabas Omondi, Dennis Simiyu Natembeya, Ephraim Mwatha Mugane, Kefa Ogonyo Bosire, and Isaac Ongubo Kibwage. 2015. Use of mobile learning technology among final year medical students in Kenya. *Pan African Medical Journal* 21, 1 (2015). https://www.panafrican-med-journal.com/content/article/21/127/full/

[36] Bill Maurer. 2012. Mobile money: Communication, consumption and change in the payments space. *Journal of Development Studies* 48, 5 (2012), 589–604. https://www.tandfonline.com/doi/full/10.1080/00220388.2011.621944

[37] Joseck Luminzu Mudiri. 2013. Fraud in mobile financial services. *Rapport technique, MicroSave* 30 (2013). https://www.microsave.net/files/pdf/RP151_Fraud_in_Mobile_Financial_Services_JMudiri.pdf

[38] Collins W. Munyendo, Yasemin Acar, and Adam J. Aviv. 2022. "Desperate Times Call for Desperate Measures": User Concerns with Mobile Loan Apps in Kenya. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, New York City, New York, 2304–2319. https://doi.org/10.1109/SP46214.2022.9833779

[39] Laura L Murphy and Alexandra E Priebe. 2011. "My co-wife can borrow my mobile phone!" Gendered Geographies of Cell Phone Usage and Significance for Rural Kenyans. *Gender, Technology and Development* 15, 1 (2011), 1–23. https://journals.sagepub.com/doi/10.1177/097185241101500101

[40] Angela W. Mutua. 2009. *Strategic Change Management at Faulu Kenya.* Master's thesis. School ofBusiness.

[41] Kabui Mwangi. 2023. Whitepath, Regus slapped with Sh5m fine for breaching data laws. https://www.businessdailyafrica.com/bd/corporate/companies/whitepath-regus-slapped-with-sh5m-fine-for-breaching-data-laws-4196536.

[42] Waihiga Mwaura. 2021. Kenya outrage over debt collectors' shaming tactics. https://www.bbc.com/news/world-africa-57985667

[43] Moses Namara, Daricia Wilkinson, Byron M. Lowens, Bart P. Knijnenburg, Rita Orji, and Remy L. Sekou. 2018. Cross-Cultural Perspectives on EHealth Privacy in Africa. In *Proceedings of the Second African Conference for Human Computer Interaction: Thriving Communities* (Windhoek, Namibia) *(AfriCHI '18)*. Association for Computing Machinery, New York, NY, USA, Article 7, 11 pages. https://doi.org/10.1145/3283458.3283472

[44] United Nations. 2000. United Nations Millennium Development Goals (2000-2015). https://www.un.org/millenniumgoals/.

[45] United Nations. 2017. Sustainable Development: 17 Goals. https://sdgs.un.org/goals.

[46] Annie Njanja. 2021. Kenya cracks down on digital lenders over data privacy issues. https://techcrunch.com/2021/10/25/kenya-cracks-down-on-digital-lenders-over-data-privacy-issues/.

[47] Annie Njanja. 2023. Google to ban unlicensed loan apps in Kenya as new rules take effect. https://techcrunch.com/2023/01/31/google-to-ban-unlicensed-loan-apps-in-kenya-as-new-rules-take-effect/.

[48] Allan Odhiambo. 2023. Fintech loans leave trail of regret and shame on Kenyans. https://www.theeastafrican.co.ke/tea/business/kenya-s-fintech-loans-leave-trail-of-regret-4050142

[49] Central Bank of Kenya. 2014. The Microfinance Act, 2006. https://www.centralbank.go.ke/wp-content/uploads/2016/08/MICROFINANCEACT2006.pdf.

[50] Central Bank of Kenya. 2016. The Banking (Amendment) Act 2016. https://www.centralbank.go.ke/uploads/banking_circulars/1456582762_BankingCircularNo4of2016-TheBankingAmendmentAct2016.pdf.

[51] Central Bank of Kenya. 2021. Enactment Of The Law To Regulate Digital Lenders And Issuance Of The Corresponding Draft Regulations For Public Comment. https://www.centralbank.go.ke/uploads/press_releases/139697899_PressRelease-EnactmentoftheLawtoRegulateDigitalLenders.pdf.

[52] The Central Bank of Kenya. 2023. Commercial Banks Weighted Average Rates. https://www.centralbank.go.ke/commercial-banks-weighted-average-rates/.

[53] Office of the Data Protection Commissioner. 2021. The Data Protection Act, 2019. https://www.odpc.go.ke/dpa-act/.

[54] Quincy Okoth. 2023. Tweet. https://twitter.com/_skilli/status/1656951932542484481.

[55] Dominic Omondi. 2018. The rise of Kenya's new 'shylock' economy. https://www.standardmedia.co.ke/business/article/2001300058/the-rise-of-kenya-s-new-shylock-economy.

[56] Dominic Omondi. 2021. How M-Shwari outpriced itself from lucrative mobile loans (Archived). https://web.archive.org/web/20210930185941/https://www.standardmedia.co.ke/business/financial-standard/article/2001418106/how-m-shwari-outpriced-itself-from-lucrative-mobile-loans.

[57] Fahad Pervaiz, Rai Shah Nawaz, Muhammad Umer Ramzan, Maryem Zafar Usmani, Shrirang Mare, Kurtis Heimerl, Faisal Kamiran, Richard Anderson, and Lubna Razaq. 2019. An Assessment of SMS Fraud in Pakistan. In *Proceedings of the 2nd ACM SIGCAS Conference on Computing and Sustainable Societies* (Accra, Ghana) *(COMPASS '19)*. Association for Computing Machinery, New York, NY, USA, 195–205. https://doi.org/10.1145/3314344.3332500

[58] Lubna Razaq, Tallal Ahmad, Samia Ibtasam, Umer Ramzan, and Shrirang Mare. 2021. "We Even Borrowed Money From Our Neighbor": Understanding Mobile-Based Frauds Through Victims' Experiences. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW1, Article 41 (apr 2021), 30 pages. https://doi.org/10.1145/3449115

[59] Bradley Reaves, Jasmine Bowers, Nolen Scaife, Adam Bates, Arnav Bhartiya, Patrick Traynor, and Kevin R. B. Butler. 2017. Mo(Bile) Money, Mo(Bile) Problems: Analysis of Branchless Banking Applications. *ACM Trans. Priv. Secur.* 20, 3, Article 11 (aug 2017), 31 pages. https://doi.org/10.1145/3092368

[60] Hindenburg Research. 2020. Opera: Phantom of the Turnaround – 70% Downside. https://hindenburgresearch.com/opera-phantom-of-the-turnaround/.

[61] Antoaneta Roussi. 2020. Airtime is money: The use of pre-paid mobile-phone minutes as a currency. https://www.ft.com/content/16c86479-e88d-4a28-8fa4-cd72bace5104.

[62] Muhammad Sadi Adamu. 2021. Rethinking Technology Design and Deployment in Africa: Lessons from an African Standpoint. In *3rd African Human-Computer Interaction Conference: Inclusiveness and Empowerment* (Maputo, Mozambique) *(AfriCHI 2021)*. Association for Computing Machinery, New York, NY, USA, 75–83. https://doi.org/10.1145/3448696.3448704

[63] Safaricom. 2014. Safaricom and CBA Launch Ambitious Plan to Grow M-Shwari Customers. https://www.safaricom.co.ke/media-center-landing/press-releases/safaricom-and-cba-launch-ambitious-plan-to-grow-m-shwari-customers.

[64] Safaricom. 2015. Mobile Banking Codes/Paybills. https://www.safaricom.co.ke/images/Mobile_Banking_Codes_Paybill.pdf

[65] Safaricom. 2023. Fuliza Terms and Conditons. https://www.safaricom.co.ke/media-center-landing/terms-and-conditions/fuliza-terms-and-conditons

[66] Safaricom. 2023. M-PESA USSD fraud. https://www.safaricom.co.ke/fraud-awareness/m-pesa-fraud/m-pesa-ussd-fraud.

[67] Kushal Shah, Shrirang Mare, and Richard Anderson. 2019. Understanding Mobile Money Grievances from Tweets. In *Proceedings of the Tenth International Conference on Information and Communication Technologies and Development* (Ahmedabad, India) *(ICTD '19)*. Association for Computing Machinery, New York, NY, USA, Article 27, 6 pages. https://doi.org/10.1145/3287098.3287123

[68] Jonathan Shieber. 2018. With loans of just $10, this startup has built a financial services powerhouse in emerging markets. https://techcrunch.com/2018/04/18/with-loans-of-just-10-this-startup-has-built-a-financial-services-powerhouse-in-emerging-markets/.

[69] Frank Stajano and Paul Wilson. 2011. Understanding Scam Victims: Seven Principles for Systems Security. *Commun. ACM* 54, 3 (mar 2011), 70–75. https://doi.org/10.1145/1897852.1897872

[70] Sharifa Sultana, Md. Mobaydul Haque Mozumder, and Syed Ishtiaque Ahmed. 2021. Chasing Luck: Data-Driven Prediction, Faith, Hunch, and Cultural Norms in Rural Betting Practices. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 89, 17 pages. https://doi.org/10.1145/3411764.3445047

[71] Tavneet Suri and William Jack. 2016. The long-run poverty and gender impacts of mobile money. *Science* 354, 6317 (2016), 1288–1292. https://www.science.org/doi/10.1126/science.aah5309

[72] Nikko Tanui. 2022. Main suspect in SIM swap fraud arrested amid DCI investigations. https://www.standardmedia.co.ke/national/article/2001464127/main-suspect-in-sim-swap-fraud-arrested-amid-dci-investigations.

[73] Mate Tongola. 2022. How to protect yourself from SIM swapping fraud. https://www.standardmedia.co.ke/business/sci-tech/article/2001446801/how-to-protect-yourself-from-sim-swap-fraud.

[74] Jared Too. 2022. Long queues as Kenyans rush to beat SIM card registration deadline. https://www.standardmedia.co.ke/counties/article/2001442654/long-queues-as-kenyans-rush-to-beat-sim-card-registration-deadline

[75] Aditya Vashistha, Richard Anderson, and Shrirang Mare. 2018. Examining Security and Privacy Research in Developing Regions. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies* (Menlo Park and San Jose, CA, USA) *(COMPASS '18)*. Association for Computing Machinery, New York, NY, USA, Article 25, 14 pages. https://doi.org/10.1145/3209811.3209818

[76] Wanyama wa Chebusiri. 2012. Kenya's battle to switch off fake phones. https://www.bbc.com/news/world-africa-19819965

[77] Susan P. Wyche and Laura L. Murphy. 2012. "Dead China-Make" Phones off the Grid: Investigating and Designing for Mobile Phone Use in Rural Africa. In *Proceedings of the Designing Interactive Systems Conference* (Newcastle Upon Tyne, United Kingdom) *(DIS '12)*. Association for Computing Machinery, New York, NY, USA, 186–195. https://doi.org/10.1145/2317956.2317985

[78] Sarah Yu and Samia Ibtasam. 2018. A Qualitative Exploration of Mobile Money in Ghana. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies* (Menlo Park and San Jose, CA, USA) *(COMPASS '18)*. Association for Computing Machinery, New York, NY, USA, Article 21, 10 pages. https://doi.org/10.1145/3209811.3209863