Easy Come, Easy Go: Phone Enabled Small-Scale Financial Grift

Amelia Lee Doğan
Information School
University of Washington
Seattle, WA, USA
dogan@uw.edu

Meira Gilbert
Information School
University of Washington
Seattle, WA, USA
mhg25@uw.edu

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

Abstract

Over 30 million Kenyans use M-PESA everyday to access financial systems, and many of them face fraud and scam attempts. In this study, we explore categories of financial scams that Kenyan M-PESA users face and how they mitigate the exposure to these scams. Through a survey with 73 Kenyans, we find the most common scams are M-PESA impersonation, lucky draw, loan offers, job offers, and education-related scams. We also find that users employ a variety of detection and responses strategies to mitigate their exposure to fraud. We discuss how modeling user mitigation strategies with existing cybersecurity frameworks allows us to better understand user behavior in complex ecosystems and suggest future mitigation strategies and research directions.

CCS Concepts

• **Security and privacy** → **Social aspects of security and privacy**; • **Human-centered computing** → **Empirical studies in HCI**.

Keywords

mobile money, fraud, mitigation

ACM Reference Format:
Amelia Lee Doğan, Meira Gilbert, and Lindah Kotut. 2025. Easy Come, Easy Go: Phone Enabled Small-Scale Financial Grift. In *ACM SIGCAS/SIGCHI Conference on Computing and Sustainable Societies (COMPASS '25), July 22–25, 2025, Toronto, ON, Canada.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3715335.3736315

1 Introduction

In a recent survey, more than half of mobile money users in Kenya reported facing scams or fraud [11]. This is particularly concerning given that mobile money has a penetration rate of over 77% in Kenya [16].

Mobile money has received significant attention in the HCI community, particularly within the context of the Global South [4, 6, 8, 12, 21, 32]. However, limited prior research has documented how fraud, grifts, and scams pose a substantial challenge for users with limited information, especially those residing in rural areas [18, 19, 22]. Despite Kenya's mature and pervasive mobile money system, existing research on fraud and scams on M-PESA users remains limited.

This study presents an exploratory online survey with 73 participants conducted in Kenya to investigate mobile money fraud enabled through text and social media. Through this initial exploratory investigation, we contribute: i) a comprehensive typology of scams reported by Kenyan users; ii) in-depth analysis of their spam detection and response strategies; and iii) propose a set of future research directions that would enable HCI researchers to expand the scope of mobile money fraud research, model user behavior with existing cybersecurity frameworks, and encourage more nuanced mitigation strategies that incorporate cultural relevance.

2 Background

Mobile money is a system that allows users access to financial services without formal banking relationships [31]. In Kenya, this mobile money system is known as M-PESA. Launched in 2007, M-PESA makes it possible for customers to transfer, withdraw, and deposit money using a feature phone or smartphone [7, 30]. Today, M-PESA has become ubiquitous in Kenya, with 34 million customers [23] who can deposit and withdraw money through agents, buy air time, purchase goods in local stores, access formal bank accounts, gain overdraft protections, and take out small loans [20, 24, 30, 31]. M-PESA is operated by Safaricom, the largest telecom provider in Kenya, which profits by charging a small fee on each transaction [30].

As M-PESA's popularity has grown, its ubiquity and trust have enabled the scaling of offerings. However, this growth has also increased the risk of fraud [1, 11] as malicious actors exploit knowledge asymmetries and system design. To mitigate these risks, M-PESA has introduced several measures: (i) *"hakikisha"*, a recipient verification system that provide a quick lookup service showing the recipient's full name and offering an option to cancel the transaction [11]; (ii) a transaction reversal service that allows a person to request one in case of an accidental transaction [25]; and (iii) services (*"pochi la biashara"* and/or *buy goods/paybill*) that are specific for businesses—that among other amenities, it prevents the reversal of transactions to foil opportunistic and malicious transaction reversal requests. While these examples showcase the intent and practice for protecting transactions, the seamless nature of transactions and users' lack of knowledge are leveraged to still make financial scams possible.

3 Related Work

3.1 Mobile Money and Related Scams

Recent work has focused on how mobile money scams and cybercrimes are carried out. Our study focuses on smishing, where

COMPASS '25, Toronto, ON, Canada

ACM ISBN 979-8-4007-1484-9/25/07
https://doi.org/10.1145/3715335.3736315

"fraudsters send delirious emotional text messages to trick users [or]... fraudsters posing as employees of mobile service providers send fake text messages to customers that they have won a promotional prize" [15]. Smishing attacks comprise the majority of previous HCI work on mobile and SMS scams which forms the majority of our typology in 5.1. At times these attacks can escalate to phone call scams [15, 22].

Several studies in HCI have explored SMS and mobile fraud using user-centric approaches. Pervaiz et al. [18] in Pakistan found the most common fraud schemes were related to lottery schemes (which we call lucky draw), followed by damsel in distress, and credential theft through texts about services being disabled. Extending research on mobile frauds, Razaq et al. [22] through interviews in Pakistan, found various fraud types such as lucky draw, governmental subsidy fraud (BISP fraud), bank fraud through impersonating officials, and romantic advance fee frauds (damsel in distress). We did not see any damsel in distress or romance-related fraud in our dataset. The only work in HCI we are aware of that addresses mobile money scams in Kenya is by Shah et al. [29]. Through a social media analysis of grievances in six countries (Ghana, India, Kenya, Pakistan, South Africa and Uganda), they identified fraud to be one of the top three issues raised by Twitter users. Additionally, they highlighted Kenya's well-developed mobile money ecosystem and called for a fraud classification system, a need that our typology addresses.

3.2 Mobile Fraud Mitigation Strategies

Prior research on mobile fraud mitigation strategies focus on how technical interventions help financial institutions develop effective in-house prevention and mitigation strategies. In a literature review of 248 articles on mitigation strategies for phishing, researchers found that the most prevalent approach was using machine learning based algorithms and techniques, while only 33/248 focused on "human-centric" interventions (such as training and awareness, and recommendations and guidelines) [13]. Technical strategies are important to help financial institutions and mobile money operators better detect and prevent fraud but do not always address the needs of individual mobile money users as Pervaiz et al. [18] and Razaq et al. [22] offer.

Pervaiz et al. [18] identified three strategies for combating fraud in Pakistan: education, disabling attackers' phone numbers, and a fraud detection app. They suggest a broad educational approach to tackle SMS schemes, noting that previous attempts by the Pakistan Telecommunication Authority and banks, though informative, were mixed with non-educational messages, potentially causing users to overlook them. Instead, Pervaiz et al. [18] recommend a regular schedule for public fraud alerts, without detailing the specific format. Razaq et al. [22] also proposed formal educational campaigns as a key mitigation strategy due to limited success of reporting. To address users without smart phones or internet, or those located in rural areas, previous work proposes empowering mobile money agents to educate users [21, 22]. Razaq et al. [22] also suggest that campaigns led by authority figures, such as game host shows or government ads, including messages in "caller tunes," could effectively raise awareness. Our findings indicate many users already utilize fraud detection apps similar to those recommended by Pervaiz et al. [18], but these apps exclude users without smartphones or internet.

4 Method

The work is part of a larger study considering the relationship between financial technology, government oversight, and user interactions with related policies. The study is led by the third author who is licensed by National Commission for Science, Technology and Innovation (NACOSTI) to conduct research in Kenya.

4.1 Survey

The online survey was conducted in Kenya in 2023, and the University of Washington Institutional Review Board deemed the study exempt. Participants were recruited through convenience sampling where interview participants in the larger study could optionally complete the survey to provide additional information (e.g., screenshots). We also leveraged snowball sampling through links shared on WhatsApp and Facebook. Participants agreed to a consent form before being asked about the scams they had encountered, scams they were aware of, their technology use, and their news sources. Participants were compensated Ksh 100. After cleaning the survey, we kept 73 participant responses with 89 separate scams. For all survey questions and participant demographics, see supplemental materials.

4.2 Analysis

First, we cleaned survey results to filter out participants not located in Kenya and other irregular responses. Any responses not in English were translated by the third author, a fluent speaker of Kiswahili. The first two authors met for initial open coding [28] and focused on survey data specifically about participants' experiences with scams, including user-submitted screenshots, descriptions, and user-described mitigation strategies. From open coding and existing literature [18, 22, 29], the authors created an initial codebook of scams and mitigation strategies to code the data with. After meeting to review data and conduct coding, the authors divided mitigation strategies into detection and response strategies, taking language from the US Department of Commerce National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 [14]. With the revised codebook, the second author revisited the data before meeting to agree on all codes with the first author.

5 Findings

We present findings from our survey, including eight types of scams, five scam detection strategies, and three scam mitigation strategies.[1]

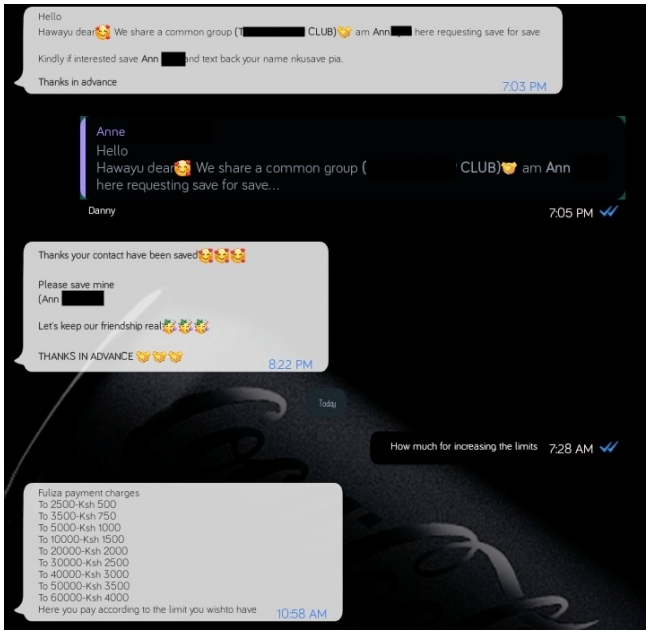
5.1 Scams

5.1.1 M-PESA Impersonation (n=32). The most common type of scam was an M-PESA impersonation when scammers tried to replicate official M-PESA communication. The scam followed a fairly formulaic pattern, often mimicking a message such as *"[confirmation code] Confirmed.You have received Ksh2,850.00 from [name, phone number] on 28/2/23/New M-PESA balancce is KshLOCKED.Pay*

[1] Some participants reported multiple or overlapping scam, detection, and/or mitigation strategies, so the *n* may be more than response on the survey.

to POCHI TODAY. Click [url]." This type of scam is most similar to other types of bank fraud that are intended to gain users' credentials [22]. This often came from an unofficial number, although at times an official or verified number was spoofed or used and included incorrect or blocked MPESA account amounts.

(a) Screenshot of a Twitter (now X) private message example of a lucky draw scam for crypto



(b) Screenshot of WhatsApp message attempting social engineering through a save for save offer for a loan offer scam

Figure 1: Example of scams shared by survey respondents.

5.1.2 Lucky Draw (n=19). In lucky draws, we saw characteristics of messages about winning drawings or investments that were too good to be true and may require advance payment. Lucky draws are a well documented type of fraud and scam [22] that use specific language [18] as seen in Figure 1(a).

5.1.3 Loan Offer (n=13). For loan offers, similar to lucky draw language, participants were offered loan terms that were often too good to be true. At times these loan offers referenced fuliza, Safaricom's own overdraft and loan service [3] and other official loan providers. These could mimic official communication, similar to M-PESA impersonation, such as *"Dear Customer KCB M-PESA soft loan is now Available to ALL M PESA USERS, send 555555 to [phone number] Request LOAN from Ksh10,000-Ksh250,000 Call [phone number].....".* Other times, loan offers came from impersonators employing social engineering tactics to gain trust of participants, such as in Figure 1(b).

5.1.4 Job Offer (n=9). In job offer scams, participants were offered jobs or job training unexpectedly or with unrealistic compensation ranges. Many of the job offers were to produce low-cost English essays or transcription: *"Have you ever done Academic and Article writing before? At [company name] we are hiring freelance academic writers to complete homeworks, assignments, papers, research, and projects for pay[.] Unskilled people will get online training."*

5.1.5 Education (n=9). In the education scam, drawing on traditional impersonation and scam tactics, scammers would often impersonate loved ones and ask for money for school supplies or bus money to visit home from boarding school (which are quite prevalent in Kenya [33]): *"Hi mum, I do not have a calculator and clipboard, and they are needed tomorrow as we have an exam. Please send 1950 to the teacher. But call them first."*

5.1.6 Other Scams (n=10). We saw three other types of scams within our dataset: *false sensitive disclosure (5), cryptocurrency (3),* and *tenant (2).* In a *false sensitive disclosure* scam, the scammer would pretend to have sent personal information to a participant and then backtrack to urge the participant not to use it. Sometimes, this was used to build trust with the participant before engaging in the final scam. In the *cryptocurrency* scam, scammers leveraged cryptocurrency opportunities in an attempt to obtain credentials from users. In the *tenant* scam, a scammer would impersonate the participant's landlord and inform them of a new rental payment system that did not exist, presumably to defraud them.

5.2 Scam Detection Strategies

5.2.1 Checking M-PESA Number (n=32). The most common mitigation strategy was for users to compare the number that sent the scam message against the official M-PESA number. It appeared many users knew Safaricom would only contact them through the official M-PESA number and verified channels rather than a random private number. Other users described detecting a scam because the numbers were automatically attached to someone's contact information (*"I knew it was a scam because it was not from mpesa rather than from another person as the number was visible rather than the mpesa name"*).

5.2.2 Checking M-PESA Balance (n=11). If the scam type indicated a change in M-PESA balance (5.1.1), users verified the activity by checking if their M-PESA balance had changed. Because some M-PESA scams have the users' balance blocked from the message (i.e.: *"[confirmation number] Confirmed. You have received Ksh2,530.00 from [name] on 26/10/22.New M-PESA balance is ksh(*LOCKED*)"*), some users knew that "locked" or "blocked" balances were indications of a scam message. This mitigation strategy was frequently paired with checking M-PESA number (5.2.1) indicating that users can avoid M-PESA impersonation scams with a variety of tactics.

5.2.3 Spam Detection Tools (n=10). Users also leveraged spam detection tools to determine if a message was a scam or not. Tools included those built into their phones, with users referencing how Android systems ask if users want to report unknown numbers as spam as well as spam call blocking apps, such as TrueCaller.

5.2.4 Verifying Identity (n=9). Users also detected scams by attempting to verify the true identity of the spam number. Some users contacted the numbers themselves to verify identity. For example, in response to a tenant scam (5.1.6), one user described how they attempted to call the scammer directly: *"They had texted me that the rent paying account number for our apartment had changed, I almost fel for it because I didn't have the number of our caretaker so I tried calling the number to confirm, and it was off."* Others described not sending money to unknown people and contacting Safaricom to confirm if a transaction is real or not.

5.2.5 Doubt (n=8). Some users did not describe specific tactics to identify or mitigate scam messages, but suggested more general behaviors to avoid scams including *"being alert," "be[ing] aware,"* and *"just being careful."* Users described being vigilant about checking details (5.2.2, 5.2.1) if they doubted the messages, and also many relied on previous scam experiences to determine if a message is a scam or not.

5.3 Scam Response Strategies

5.3.1 Reporting (n=14). To protect themselves against being contacted in the future, users report spam messages within their phone's operating systems (*"I block spam messages or rather I report the number"*) as well as directly to Safaricom. None of our participants reported turning to social media like in Shah et al. [29] to remedy their experiences with scams.

5.3.2 Protecting Personal Information (n=9). Many users indicated they protect themselves by avoiding sharing personal information. This is especially relevant in response to scams because users will refuse to give out their M-PESA credentials or PINs (*"I ensure that information am getting is from a true source and I don't disclose my mpesa credentials)"*.

5.3.3 Dispute Transaction (n=1). If a user believed they were incorrectly sent or charged money, they may attempt to dispute the transaction directly with the scammer (*"I advice the sender to reverse his money if confused the number"*). However, this strategy was only mentioned once and is likely only relevant in instances of false sensitive disclosure or overpayment scams.

6 Discussion

6.1 Contextualizing Findings

Through an exploratory survey in Kenya, we contribute a typology of eight scams in text and messaging platforms. We confirm previous work showing that lottery/lucky draw scams (5.1.2) and bank fraud scams, which we term M-PESA impersonation scams (5.1.1), are also common in Kenya [18, 22]. We identify two previously undocumented scams in HCI literature including variations of exploiting personal relationships or creating false emergencies [27] in the case of the education and tenant scam. We also note how cryptocurrency scams (5.1.6) have expanded to include M-PESA-related fraud and how scammers may deliberately overshare information with victims to facilitate sensitive disclosure fraud (5.1.6).

6.2 Adopting Cybersecurity Framework Language

We use language from the NIST CSF [14] to better differentiate and describe user mitigation strategies. While previous research describes a wide variety of user tactics, technical solutions, and educational campaigns as *mitigation strategies*, we further break down these user strategies to *detection* and *response*. *Detection* involves ways of identifying a message as a scam. Strategies include users checking their M-PESA balance (5.2.2), confirming an official source sent the message (5.2.1), and leveraging fraud detection apps (5.2.3). We also find that detection does not solely rely on technical solutions, but also includes user's preemptive attitudes like doubt (5.2.5), as well as cultural techniques (5.2.4), such as one user asking for an acquaintance's home name (*"Jina ya mtaa?"*), a traditional name used by community members [17]. *Response* includes actions taken once a user is aware of a scam. These strategies include protecting personal information (5.3.2), reporting the scammer (5.3.1, and disputing the transaction (5.3.3). Using language from cybersecurity frameworks like the NIST CSF [14], MITRE ATT&CK [5], ISO 27001 [9], and General Data Protection Regulation [2] could help HCI researchers clearly articulate and differentiate user and attacker strategies in fraud and scam cases. Although designed for organizations, the NIST CSF's functions for responding to cybersecurity incidents also apply to other contexts, such as our study's complex fraud and scam ecosystem.

6.3 Future Mitigation Strategies

While our study is exploratory, users did express interest in addressing knowledge asymmetry through large-scale educational campaigns [18, 22]. We suggest that educational campaigns are carried out by mobile money agents and are regularly updated based on local fraud datasets, such as messages reported to Safaricom [21, 22]. This would mean existing reporting infrastructures can be used to alert the public to new and emerging scams. We also see opportunity for public messaging to adopt existing cybersecurity frameworks to ensure mitigation methods suggested by public messaging are informed by cybersecurity best-practices. Additionally, Safaricom's limited existing public messaging on mitigation strategies [26, 27] could be updated with strategies, such as non-technical ones, we outline above.

6.4 Limitations and Future Work

Our survey was meant as an exploratory research tool to develop a baseline of mobile money scams in Kenya, and was limited in scope–with a participant pool skewed toward younger, more-educated individuals who used smartphones. For more in-depth research, interviews and targeting rural populations could be helpful [10, 22] or more comparative work around how scam execution differs by geography [29]. We also encourage researchers to expand mitigation strategies more broadly to include cultural practices and to reach users with feature phones, since 68% of Kenyan users have feature phones compared to 60% of users using smart phones [16].

7 Conclusion

Utilizing an exploratory survey, our study contributes novel user-reported mobile money scams and mitigation strategies in Kenya over text and messaging platforms. We propose future public messaging around mitigation leverages existing reporting mechanisms and includes strategies that are not just technical. Finally, we encourage more in-depth research into fraud in Kenya and suggest that future HCI research adopt language from widely accepted cybersecurity frameworks to describe the fraud ecosystem.

References

[1] 2009. *M-Money Channel Distribution Case – Kenya.* Technical Report. International Finance Corporation World Bank Group. https://documents1.worldbank.org/curated/pt/832831500443778267/pdf/117403-WP-KE-Tool-6-7-Case-Study-M-PESA-Kenya-Series-IFC-mobile-money-toolkit-PUBLIC.pdf

[2] 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). http://data.europa.eu/eli/reg/2016/679/oj/eng Legislative Body: EP, CONSIL.

[3] Nafisa Abdulhamid. 2020. Disruptive Technology, Mobile Money, and Financial Mobilization in Africa: M-Pesa as Kenya's Solution to Global Financial Exclusion? In *Disruptive Technologies, Innovation and Development in Africa*, Peter Arthur, Kobena T. Hanson, and Korbla P. Puplampu (Eds.). Springer International Publishing, Cham, 187–202. https://doi.org/10.1007/978-3-030-40647-9

[4] Joshua E. Blumenstock, Michael Callen, Tarek Ghani, and Lucas Koepke. 2015. Promises and pitfalls of mobile money in Afghanistan: evidence from a randomized control trial. In *Proceedings of the Seventh International Conference on Information and Communication Technologies and Development (ICTD '15)*. Association for Computing Machinery, New York, NY, USA, 1–10. https://doi.org/10.1145/2737856.2738031

[5] The MITRE Corporation. 2024. MITRE ATT&CK®. https://attack.mitre.org/

[6] Changyang He, Lu He, Zhicong Lu, and Bo Li. 2023. "I Have to Use My Son's QR Code to Run the Business": Unpacking Senior Street Vendors' Challenges in Mobile Money Collection in China. *Proc. ACM Hum.-Comput. Interact.* 7, CSCW1 (April 2023), 60:1–60:28. https://doi.org/10.1145/3579493

[7] 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 (April 2007), 63–81. https://doi.org/10.1162/itgg.2007.2.1-2.63

[8] Samia Ibtasam, Hamid Mehmood, Lubna Razaq, Jennifer Webster, Sarah Yu, and Richard Anderson. 2017. An Exploration of Smartphone Based Mobile Money Applications in Pakistan. In *Proceedings of the Ninth International Conference on Information and Communication Technologies and Development (ICTD '17)*. Association for Computing Machinery, New York, NY, USA, 1–11. https://doi.org/10.1145/3136560.3136571

[9] ISO. 2022. ISO/IEC 27001:2022. https://www.iso.org/standard/27001

[10] 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 CHI Conference on Human Factors in Computing Systems*. ACM, Honolulu HI USA, 1–14. https://doi.org/10.1145/3613904.3642874

[11] Rafe Mazer and Shana Warren. 2021. *Consumer Protection Survey of Digital Finance Users: Kenya.* Technical Report. Innovations for Poverty Action. https://dataverse.harvard.edu/citation?persistentId=doi:10.7910/DVN/F8ZRPF Artwork Size: 1061285 Pages: 1061285.

[12] Indrani Medhi, S.N. Nagasena Gautama, and Kentaro Toyama. 2009. A comparison of mobile money-transfer UIs for non-literate and semi-literate users. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '09)*. Association for Computing Machinery, New York, NY, USA, 1741–1750. https://doi.org/10.1145/1518701.1518970

[13] Bilal Naqvi, Kseniia Perova, Ali Farooq, Imran Makhdoom, Shola Oyedeji, and Jari Porras. 2023. Mitigation strategies against the phishing attacks: A systematic literature review. *Computers & Security* 132 (Sept. 2023), 103387. https://doi.org/10.1016/j.cose.2023.103387

[14] National Institute of Standards and Technology. 2024. *The NIST Cybersecurity Framework (CSF) 2.0.* Technical Report NIST CSWP 29. National Institute of Standards and Technology, Gaithersburg, MD. NIST CSWP 29 pages. https://doi.org/10.6028/NIST.CSWP.29

[15] Alima Nzeket Njoya, Franklin Tchakounté, Marcellin Atemkeng, Kalum Priyanath Udagepola, and Didier Bassolé. 2023. Mobile Money Phishing Cybercrimes: Vulnerabilities, Taxonomies, Characterization from an Investigation in Cameroon. In *Towards new e-Infrastructure and e-Services for Developing Countries*, Rashid A. Saeed, Abubakar D. Bakari, and Yahya Hamad Sheikh (Eds.). Springer Nature Switzerland, Cham, 430–445. https://doi.org/10.1007/978-3-031-34896-9_26

[16] Communications Authority of Kenya. 2024. *Sector Statistics Report Q4 2023-2024.pdf.* Technical Report. https://www.ca.go.ke/sites/default/files/2024-10/Sector%20Statistics%20Report%20Q4%202023-2024.pdf

[17] Belindah Okello. 2021. What's in a name? Reinventing Luo naming system in Kenya's ethnopolitical landscape. *African Identities* 19, 1 (Jan. 2021), 77–90. https://doi.org/10.1080/14725843.2020.1791687 Publisher: Routledge.

[18] 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 (COMPASS '19)*. Association for Computing Machinery, New York, NY, USA, 195–205. https://doi.org/10.1145/3314344.3332500

[19] Rowan Phipps, Shrirang Mare, Peter Ney, Jennifer Webster, and Kurtis Heimerl. 2018. ThinSIM-based Attacks on Mobile Money Systems. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies (COMPASS '18)*. Association for Computing Machinery, New York, NY, USA, 1–11. https://doi.org/10.1145/3209811.3209817

[20] Kelsey Piper. 2020. What Kenya can teach its neighbors — and the US — about improving the lives of the "unbanked". *Vox* (Sept. 2020). https://www.vox.com/future-perfect/21420357/kenya-mobile-banking-unbanked-cellphone-money

[21] Anandita Raghunath, Innocent Ndubuisi-Obi, Hosea Mpogole, and Richard Anderson. 2024. Beyond Digital Financial Services: Exploring Mobile Money Agents in Tanzania as General ICT Intermediaries. *ACM J. Comput. Sustain. Soc.* 2, 1 (Jan. 2024), 3:1–3:26. https://doi.org/10.1145/3616386

[22] 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. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (April 2021), 1–30. https://doi.org/10.1145/3449115

[23] Safaricom. 2024. 5/12/2024 - Safaricom's M-PESA Hits 34 Million Customers in Kenya. https://www.safaricom.co.ke/media-center-landing/press-releases/safaricoms-m-pesa-hits-34-million-customers-in-kenya

[24] Safaricom. n.d.. Do More With M-PESA. https://www.safaricom.co.ke/main-mpesa/m-pesa-services/do-more-with-m-pesa

[25] Safaricom. n.d.. M-PESA Fraud. https://www.safaricom.co.ke/fraud-awareness/m-pesa-fraud

[26] Safaricom. n.d.. M-PESA Reversal. https://www.safaricom.co.ke/media-center-landing/terms-and-conditions/m-pesa-reversal

[27] Safaricom. n.d.. Scams/Extortion. https://www.safaricom.co.ke/fraud-awareness/scams-extortion

[28] Johnny Saldana. 2009. *Coding Manual for Qualitative Researchers.* SAGE Publications, London, UNITED KINGDOM. http://ebookcentral.proquest.com/lib/washington/detail.action?docID=585421

[29] 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 (ICTD '19)*. Association for Computing Machinery, New York, NY, USA, 1–6. https://doi.org/10.1145/3287098.3287123

[30] Christian Stadler. 2024. M-PESA: Why The World's First Large Mobile Payment Platform Keeps On Winning. *Forbes* (2024). https://www.forbes.com/sites/christianstadler/2024/06/11/m-pesa-why-the-worlds-first-large-mobile-payment-platform-keeps-on-winning/ Section: Leadership Strategy.

[31] Tavneet Suri. 2017. Mobile Money. *Annual Review of Economics* 9, 1 (Aug. 2017), 497–520. https://doi.org/10.1146/annurev-economics-063016-103638

[32] 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 (COMPASS '18)*. Association for Computing Machinery, New York, NY, USA, 1–10. https://doi.org/10.1145/3209811.3209863

[33] Kosgei K. Zachariah and Keter K. Joshua. 2016. Conflict and Trade-Offs between Efficiency and Access: A Case of Day and Boarding Secondary Schools in Kenya. *Journal of Education and Practice* 7, 26 (2016), 111–119. https://eric.ed.gov/?id=EJ1115859 Publisher: IISTE ERIC Number: EJ1115859.

Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant No. DGE-2140004. This work was also completed with support from the University of Washington's Graduate School's Office of Graduate Student Equity & Excellence (GSEE).