"Who is protecting us? No one!" Vulnerabilities Experienced by Low-Income Indian Merchants Using Digital Payments

Pranjal Jain*
Research & Development
theUXWhale
India

Rama Adithya Varanasi*
Department of Information Science
Cornell University
New York, NY, USA

Nicola Dell
Department of Information Science
The Jacobs Institute, Cornell Tech
New York, NY, USA

ABSTRACT

Low-income merchants in India, who conduct business via makeshift shops and handcarts, are increasingly using digital payment systems for business operations. Although these merchants are a key stakeholder in digital payment ecosystems, they have not yet received much attention from the research community. We present a qualitative study consisting of observations and interviews with 24 low-income merchants and 10 agents that explores the vulnerabilities merchants experience as they adopt and use digital payments. Using the notion of vulnerability as a lens, we show how socio-technical interactions between merchants and agents contribute to at least four different types of vulnerabilities: access-based, identity-based, financial, and informational vulnerabilities. We discuss how agents, customers, and fraudsters take advantage of merchants' vulnerabilities to commit different types of fraud that lead to serious harm for merchants. We show how merchants developed strategies to combat fraud that lead to more work and extra burdens for merchants. Our research suggests a cyclic model of vulnerability that exposes the cumulative effects of vulnerabilities, frauds, and harms experienced by merchants. We end by providing practical recommendations for digital payment companies to break this cycle and better serve low-income merchants.

CCS CONCEPTS

• **Human-centered computing → Empirical studies in HCI**.

KEYWORDS

Vulnerabilities; privacy; digital payments; merchants; digital financial services; fraud; Global South; DFS; ICTD; HCI4D

ACM Reference Format:
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 (COMPASS) (COMPASS '21), June 28-July 2, 2021, Virtual Event, Australia.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3460112.3471961

*Both authors contributed equally to this research.

COMPASS '21, June 28-July 2, 2021, Virtual Event, Australia

ACM ISBN 978-1-4503-8453-7/21/06…$15.00
https://doi.org/10.1145/3460112.3471961

1 INTRODUCTION

Digital payment systems are becoming an integral part of people's lives, with 2020 reports estimating that digital payments produced a global revenue of about 5.4 trillion dollars [26]. In India, where our research is situated, the adoption and use of digital payments has been accelerated by government initiatives, including the demonetization of currency in 2016 [29, 31]. Although digital payment systems promise to bring new benefits to low-income communities, including last-mile financial inclusion [19, 70, 73], they also open people up to new vulnerabilities and the potential for fraud, especially for new technology users that do not understand how digital payments work or how to protect themselves from harm.

A growing body of HCI and ICTD work has examined the benefits and pitfalls of digital payment systems, including factors influencing adoption [32, 42, 56], trust [11, 18], security and privacy [9, 35, 72], and more. However, for the most part this work focuses on the experiences of *customers* (i.e., individuals purchasing goods and services). Much less attention has been paid to understanding the experiences of low-income *merchants*, who run makeshift shops and handcarts, selling vegetables, snacks, cheap electronic accessories (e.g., screen protectors, earphones, and chargers), and more. These merchants are key stakeholders in digital payment ecosystems, and increasingly rely on digital payments for business operations [64, 80]. Thus, there is a need for more research to understand merchants' experiences, including the vulnerabilities, frauds, and harms that arise when using digital payment systems.

We contribute a qualitative study that focuses on the following research questions: **RQ1:** What vulnerabilities do low-income merchants face as they adopt and use digital payment systems? **RQ2:** What kinds of fraud, and corresponding harms, do merchants experience in light of these vulnerabilities? and **RQ3:** What strategies have merchants developed to try and combat the fraud they experience? To answer these questions, we conducted field observations and interviews with 24 low-income merchants and 10 agents who were employed by digital payment companies to recruit and onboard merchants. We use the notion of *vulnerability* as a lens to examine the socio-technical interactions between merchants and agents. In particular, we draw inspiration from McDonald and Forte's identity-based vulnerability [51] and Calo's perspectives around situational vulnerability [15] to unpack the different kinds of vulnerabilities, and corresponding harms, that merchants encounter. We organize our findings around the three phases of the Moneywork framework, which separates interactions into *pre-transaction*, *at-transaction*, and *post-transaction* activities [66].

For RQ1, we show how socio-technical interactions between agents and merchants contributed to at least four types of vulnerabilities across all three phases of the Moneywork framework.

For instance, during onboarding, agents used coercive strategies to convince merchants to hand over their smartphones, resulting in *access-based vulnerability*. Agents then used the device to access and share merchants' personal information without their consent, leading to *identity-based vulnerability*. Subsequently, merchants' lack of training on digital payment apps led them to rely predominantly on SMS messages to verify customer payments, contributing to *financial vulnerability* that opened up opportunities for customers to commit fraud. Meanwhile, lack of access to information and support resulted in *informational vulnerabilities* that created opportunities for merchants to fall prey to scams.

Turning to RQ2, we demonstrate how agents, customers, and fraudsters took advantage of different vulnerabilities to commit many types of fraud that resulted in serious harm for merchants. For example, agents took advantage of access-based vulnerabilities to enter the wrong bank account details into the merchant's digital payment account. During face-to-face purchases, customers took advantage of merchants' identity and financial vulnerabilities to commit fraud by faking payment verification messages, and fraudsters took advantage of informational vulnerabilities to send intimidating messages that tricked merchants into sending them large sums of money. The types of harm we encountered constitute both objective harm, such as livelihood loss, and subjective harm in the form of anxiety, stress, humiliation, and embarrassment [14].

For RQ3, we saw merchants use different coping strategies to try and minimize the harm they experienced, such as seeking support from companies' customer care, agents, and family. A few merchants also used cheap webcams to capture photos of fraudsters and stuck them to the shop to humiliate the customers. These strategies had varying degrees of efficacy and placed additional burdens on merchants via the time, energy, and extra work they required.

We discuss how our findings suggest a *cyclic* relationship between socio-technical actions, vulnerabilities, fraud, and harm, rather than the linear relationship suggested by prior work [14, 15, 51]. For example, lack of training on digital payment apps led to financial vulnerability during customer purchases, resulting in opportunities for customers to commit fraud, which led to livelihood harm for merchants. This harm pushed merchants to seek support from customer care that was ineffective, contributing to information vulnerability, which led to more fraud and harm.

We close by discussing practical recommendations for digital payment companies to better engage, train, and support merchants, disrupting this cycle of vulnerabilities, frauds, and harms, and leading to better experiences for merchants.

In sum, our research expands existing knowledge of digital payment systems by examining the experiences of low-income merchants, an understudied but key stakeholder in this ecosystem. We discuss many vulnerabilities, frauds, and harms that merchants encounter when adopting and using digital payment systems, and suggest practical ways for companies to improve their training and support programs to better serve low-income merchants.

2 RELATED WORK

Digital payments in the Global North. Digital payment systems have been the focus of HCI and CSCW research in Western contexts. In particular, studies have focused on payment systems' adoption [20], perceived usefulness and ease of use [47], and end-users' agentic practices [25, 47]. Other studies have explored users' security and privacy challenges in the real world [7, 68]. A cluster of studies have explicitly focused on the shortcomings of digital payment systems, such as end-users' difficulty managing their balance in the digital wallet [48], the limitations of collaboration [82], end-users' lack of trust [20], privacy attitudes [5], and perceived risks [81, 83] associated with digital payment systems.

Beyond studying the experiences of end-users/customers, studies have also sought to include other stakeholders [6, 69]. For example, Ondrus et al. adopted a multi-stakeholder perspective, looking at motivations and perspectives of merchants adopting digital payment systems [36, 62]. Several factors, such as cost of the customer base, ease of use, and reliability were taken into consideration while studying merchants' use of the payment system. In a similar study, Mallat also highlighted how merchants tend to be an important link in digital payment systems [49]. This small set of studies emphasize the need for a stronger understanding of merchants' experiences, since they are critical to complex commerce ecosystems. Our work expands the focus of this research to the Global South, where merchants may experience different constraints and challenges.

Digital payments in the Global South. Digital payment systems have also been an important focus of ICTD research and are frequently considered important tools for last mile financial inclusion [30, 70]. Much of this research is again centered on customers, focusing on adoption [32, 42, 56], usability [52, 53, 65], trust [11, 18], security [9, 72], financial literacy [45] and privacy [35]. For instance, Ibtasam et al.'s work showed how digital payment apps installed on men's smartphones were shared in the household, providing women with financial accessibility [38]. Razaq et al. explored different types of financial fraud that targeted individuals, demonstrating social engineering techniques that led to financial harm [71].

Beyond customers, research has shown that agents have been instrumental in assisting with adoption and financial literacy in low resource contexts [33]. Several studies have examined the role of agents in enabling long-term adoption and use of financial services by providing support infrastructure [1, 23, 39, 54]. Within the context of digital payment systems, studies have explored how agents assist individuals in onboarding, solving day-to-day issues, conducting transactions on users behalf, and distributing benefits [33, 44, 77]. In particular, Odoom and Kosiba showed how agents play a crucial role in influencing end-users' decision to adopt and use digital payment apps [60]. However, the major focus of these studies has been on agents who cater to *customers'* needs.

Digital payment systems in India became particularly important after the government's demonetization of currency in 2016 [29, 31]. Companies like Google, Amazon, and PayTM employed on-the-ground agents to convince and onboard merchants to their payment platform [13, 28, 78]. Early studies have looked at this space by examining merchants' adoption practices [17]. Pal et al. examined merchants' perceptions of demonetization and the challenges adopting payment systems in urban markets, hinting at decreased usage of digital payment apps [64]. Vashistha et al. examined the perceived benefits and pitfalls of using digital payments for customer-merchant transactions, finding that customers were

interested to adopt digital payments for referral rewards and sign-up incentives, but were hesitant to use them regularly, whereas merchants saw digital payments as an unnecessary burden [80].

Our contributions. We expand this literature in several ways. First, we examine the interactions between merchants and the agents (as opposed to customers) employed by digital payment companies to onboard them to the company's platform. Second, we highlight vulnerabilities merchants face when using digital payments, and demonstrate how these vulnerabilities lead to fraud and subsequent harm for merchants. We also discuss strategies merchants have developed to try and mitigate the vulnerabilities and fraud they experience.

Vulnerability as a lens. Our study uses the notion of *vulnerability* as a theoretical lens, adopting two main perspectives. First, we draw inspiration from McDonald and Forte's work on the notion of identity-based *vulnerability* in the context of privacy in HCI systems [51]. They define vulnerable populations as those whose safety and well-being are likely to be affected by privacy violations [51]. They argue that existing privacy theories [3, 58, 84] focus and argue at the level of the collective and overlook individuals on the margins who do not have voice. This is also true in contexts outside privacy where McDonald and Forte's perspective stands in strong contrast with Fineman's *vulnerability theory*. Fineman considers vulnerability as a universal part of the human condition that is shared by everyone [27]. In reality, this is not the case as the structural barriers and social inequalities have subdued voices and experiences of marginalized individuals [21]. Dym and Fiesler highlighted that such conditions make vulnerable populations, such as LGBTQ+ people, face intensified privacy risks through information sharing when compared to other communities [24].

Second, we draw inspiration from Calo's complementary perspective on vulnerability suggesting that, in addition to identity-based vulnerability, situational circumstances also render a person vulnerable [15]. Within this perspective, Calo indicates that vulnerability is not a product of "happenstance". Instead, it is a by-product of engineered circumstances that can be controlled and mitigated with appropriate actions. Chancellor et al. demonstrated how hashtag moderation strategies implemented by Instagram to curb pro-eating disorder practices were successful with certain tags while pushing individuals to find new tags that made them more vulnerable [16]. We draw on both McDonald and Forte's [51] and Calo's [15] perspectives in our study of low-income merchants, a marginal population whose voices have thus far been underrepresented in digital payment research and practice [10].

3 METHODS

We conducted an IRB-approved qualitative study focused on the following research questions: **RQ1:** What vulnerabilities do low-income merchants face as they adopt and use digital payment systems? **RQ2:** What kinds of fraud, and corresponding harms, do merchants experience in light of these vulnerabilities? **RQ3:** What strategies have merchants developed to try and mitigate the effects of fraud they experience? To answer these questions, we recruited 34 participants: 24 low-income merchants and 10 agents over five months. The study was conducted in Delhi, Mumbai, and Hyderabad in India and all fieldwork took place before the COVID-19 pandemic (Sept 2019 - Jan 2020). We first describe the context in which our research took place before discussing our methods.

Context: India's digital payment ecosystem. India's digital payment system is built on the Unified Payment Interface (UPI) initiative launched by the government in 2016 as part of their Digital India program [43]. UPI enables users to initiate real-time inter-bank money transfer through a unique UPI ID assigned to each individual [64]. In the last five years, more than fifty companies have used UPI to launch digital payment apps. To initiate a digital transfer, a customer either 1) scans a merchant's unique QR code (see Figure 1.A), 2) enters the UPI ID, or 3) inputs the phone number linked to the UPI ID. To drive adoption of their platform, payment systems regularly offer users periodic cashback or digital points services that can be redeemed against future purchases.

Within the payment ecosystem, our study focuses on the experiences of low-income merchants. These merchants sell different kinds of commodities in makeshift shops and handcarts, such as vegetables, snacks and tea, electronic accessories like screen protectors, earphones, and chargers, and prepaid mobile top-ups (see Figure 1.A). Their gross daily revenue is around ₹400-1000 (appx. US$6-13), putting them in the low-income category [10, 41, 44]. To enroll merchants into their program, companies use agents to approach, advertise, and onboard the merchants. Agents are allocated dedicated areas within the city to visit and advertise the digital payment platform to the merchants.

A typical onboarding process involves multiple agents, each assigned to different parts of the process. For instance, one agent approaches the merchant and advertises the idea of digital payments. They pass the information to another agent who works with the merchant to download, install, and register them on the app. A third agent completes the verification process (also called Know Your Customer, KYC) and links the QR code to the merchant's bank details through the digital payment app. All the agents, along with their supervisor, coordinate their work to complete the steps, onboard merchants, and meet daily targets set by the company. Assigning multiple agents for different stages allows digital payment companies to recruit and train more agents, each only requiring training on the part of the process they specialize in, rather than having to train all agents on all parts of the onboarding process.

As part of their onboarding, merchants receive a QR code sticker that is mapped to their new UPI ID that customers can scan to pay and purchase an item. Merchants receive the money in their app instantaneously upon successful transaction, along with an SMS and in-app notification. In our study we observed merchants using an average of three different payment apps for their business. The onboarding ends with agents' pay providing necessary training to use the app, techniques for troubleshooting basic issues, and promoting awareness of prevalent kinds of fraud.

Agents are compensated via an incentive-based model. In a typical scenario, agents are paid ₹80-120 or US$1-3 at each stage of the onboarding process. For instance, if the agent completes installation of the app on the merchant's phone and registers them in the system, he receives a portion of the commission. Consequently, agents pay is dependent on the number of customers they are able to onboard. Companies often prescribe daily targets for agents and push them

to onboard as many merchants as they can. Once the merchant is onboarded, agents do not receive any further commission.

Participant recruitment. To recruit merchants, we explored different market areas in Delhi, Mumbai, and Hyderabad where low-income merchants conduct their business. These cities are known for their large curbside markets. We approached one merchant after another, explaining the objectives of our study. To diversify our recruitment, we reached out to merchants in at least two different markets within each city. To be eligible as a participant, merchants had to be actively using at least one digital payment app in their business for at least six months (avg=1 year 10 months, max=2 years 4 months). Based on this criteria, we recruited 24 merchant participants (23 men). Table 1 provides participants' demographic details. Out of the 24 merchants, 13 merchants were daily users of the digital payment systems, nine merchants stopped using at least one of their payment systems, and two merchants reported actively refusing onboarding attempts from at least one agent.

Agents were recruited through snowball sampling [34]. A few merchants willingly provided the phone number of the agent who completed their onboarding process. We started by reaching out to those agents over a phone call and describing our research objectives. To diversify our participants, we leveraged agents' daily social congregations to recruit participants from diverse payment companies. We approached merchants during these daily meetings and invited them to participate in our research. As shown in Table 1, we recruited a total of 10 agents (all men).

Observations. We started our study with observations to understand the daily business activities of merchants and agents around digital payments. We closely observed five different merchants' interactions while they conducted their business in their makeshift shops and used their payment apps. In particular, we paid close attention to how merchants (1) negotiated and conducted financial transactions with their customers, (2) rectified issues around the payment app(s), and (3) reviewed their daily business.

We also conducted observations with three agents. We followed them as they went on about their work, such as participating in the morning briefing meetings. We observed as they (1) shortlisted a neighborhood to onboard merchants, (2) negotiated and convinced merchants to install and use their payment app, (3) collaborated with their peers to onboard the merchants, and (4) conducted follow-ups with merchants in their allocated area.

We conducted observations with each merchant and agent, with each session lasting between one to four hours, spanning 2.5 months. During observations, we took detailed notes and asked probing questions whenever our participants took a break. All observations were conducted in Hindi.

Interviews. To complement our observation data, we also conducted in-person semi-structured interviews in Hindi with both agents and merchants. We interviewed 19 additional merchants. We started our interviews by asking about their motivations for using digital payments, adoption experiences, the challenges they experienced while using digital payments, and the role agents played in solving these issues. We also explored merchants' privacy practices and relevant issues with different kinds of digital payment systems. We compensated participants for their time by buying commodities worth about ₹150 (US$2). Interviews lasted 45 minutes to one hour.

We also recruited seven more agents from four different payment companies and conducted interviews at the end of their work day. We began by explaining the purpose of the study. Then we asked questions to understand their perceptions around specific aspects of their work such as (1) on-boarding, (2) merchant verification, and (3) troubleshooting specific merchant issues. Example questions included: "*How do you decide which merchants to approach and onboard?*", "*How do you convince the merchants to show your payment app?*", and "*What kind of issues do you receive from the merchants after onboarding?*". All agent interviews were conducted in a public setting like makeshift cafes. The interviews lasted between 45 and 90 minutes. To comply with companies' established rules around the payment of agents, we did not compensate agent participants.

Although our interview protocol explored topics common to merchants and agents, we also deviated from the protocol where required to capture interesting and emergent topics that arose.

Data Analysis. We collected 51 hours of observation data via detailed notes and 29 hours of audio-recorded interviews. The recordings were translated into English and transcribed. We analyzed the transcripts thematically [12] using MAXQDA software. We started by reading through the transcripts carefully. Both the first and second author took multiple passes on the transcribed data before conducting open-coding. We avoided using any presupposed codes and instead let the codes emerge from our data. Credibility was established in two major ways. First, we used the process of member checking [22] with a few participants to go over our initial analysis. We also used prolonged engagement with our participants in the field to solidify our understanding and take pluralistic perspectives into account. Coding disagreements were resolved through multiple rounds of peer-debriefing in which all authors participated [22]. At the end of multiple passes, our analysis produced 44 codes. Examples include *adoption challenges*, *compensatory practices*, and *informational privacy*. We iteratively refined the codes before clustering related codes into six themes that represent our findings. Example themes included *strategies to onboard merchants*, *frauds experienced by merchants*, and *coping mechanisms*.

To organize and present our themes we used the notion of Moneywork [66]. Perry and Ferreira define Moneywork as *"the physical and social actions individuals undertake to enable financial transactions"*. They divide interactions intro three distinct phases. *Pre-transaction* includes planning activities that individuals undertake before making purchases. *At-transaction* includes activities that help individuals carry out purchases successfully. Lastly, *post-transaction* includes activities that occur after the completion of transactions. Using Moneywork as an analytical lens has proven effective for several prior studies [37, 57, 63] and is also well-suited to our context.

Researcher Positionality. Our interpretation of our data is undoubtedly shaped by our background, subjective experiences, and conversations with the merchants. Of the paper's three authors, two are from India and one from Africa. The first author, who conducted the fieldwork, currently lives and works in India. The other two authors are based at a U.S. university; each has years of experience conducting research with communities in the Global South.

Merchants (n=24)		**Agents (n=10)**	
Participants	Observations & Interviews: 5, Interview only: 19	Participants	Observations & Interviews: 3, Interview only: 7
Gender	Women: 1; Men: 23	Gender	Women: 0; Men: 10
Age	Min: 18; Max: 57; Avg.: 35; S.D.: 10.96	Age	Min: 20; Max: 37; Avg.: 27.9; S.D.: 6.3
Payment apps used	Google Pay: 8; Amazon: 8; BhimPay: 8; Paytm: 24; PhonePay: 14	Payment apps used	Amazon: 1; Paytm: 3; PhonePay: 3; MSwipe: 3
Shop type	Product sellers: 20; Service providers: 04	Status of the job	Active: 06; Resigned 04
Gross income (₹/day)	Min:0-200; Max: 800-1,000; Avg.: 400-600.	Gross income (₹/month)	Min:15,000; Max: 25,000; Avg.: 20,000;
Cities covered	Delhi; Mumbai; Hyderabad	Cities covered	Delhi; Mumbai; Hyderabad
Education	Secondary school: 12; High school: 10; Graduate: 2	Education	High school: 3; Graduate:5; Post-graduate: 2

Table 1: Demographic details of merchants and agents.

4 FINDINGS

We present our findings according to the three stages of the Moneywork framework [66]. We begin with *pre-transaction* activities, including onboarding and installation, and demonstrate how agents use coercive techniques to convince merchants to adopt digital payments (Section 4.1). Next, we discuss challenges merchants experience during *at-transaction* activities, primarily when interacting with customers (Section 4.2). Finally, we describe *post-transaction* activities beyond customer interactions (Section 4.3). While describing these activities, we demonstrate different kinds of vulnerabilities and fraud that merchants experience and the corresponding coping mechanisms they developed to safeguard themselves.

4.1 Pre-transaction: Adoption

In this section, we discuss sociotechnical practices between merchants and agents that happen before merchants start using digital payments for their business. In the process, we demonstrate several challenges and vulnerabilities experienced by the merchants, exposing them to potential fraud.

Convincing merchants to try the app. All merchants in our study interacted with agents prior to using digital payment apps in their business. Agents started their adoption strategy with techniques that enabled them to approach the merchant, establish a connection, and *"get their foot in the door"* to advertise their company app. A common technique used by the agents (n=6) was to stick a promotional sticker of their company on the target merchants' shop without the merchants' awareness (see Figure 1.B). The promotional sticker then gave subsequent agents a form of credibility to approach and strike up a conversation with the merchants, who were otherwise cautious of such interactions and refused to entertain the agents. Agent 8, who worked for Amazon Pay, described how he routinely stuck the company's QR code stickers beside other competing digital payment companies to establish contact with the merchants:

> *"We don't need permission from the merchant to put our QR code stickers on the shop as we are just advertising. Putting the sticker is like sharing the advertisement for the Amazon company's app. My colleague goes the next day and uses the sticker as a way to introduce the company.... He tells the merchants that it would be beneficial for them and their customers as everyone will receive cashback if they use the app... The stickers are very useful because they allow us to put our foot inside their door... otherwise they don't receive us well at all."*

Agents also leveraged their local community knowledge to persuade merchants to adopt their payment system. For instance, several agents shared fabricated *"success"* stories of nearby shops that they onboarded and the resultant gain in customers, making merchants feel insecure about the future of their business. This coercive technique convinced the merchants to try their company's digital payment app. We observed Agent 7, a PhonePay agent, describing this strategy to Merchant 12 in his own words:

> *"Look, whether you like it or not, digital is the future. If you do not use these digital systems then you will not be able to make big profits... Everyone is adopting it. Even that tea vendor who earns less than you is using it. Now he is earning ₹600 more daily. Don't you want to be part of digital India? Or do you want to lose your money to him?"*

Agents resorted to fear-instilling conversations that referred to merchants losing a significant portion of their customers to competitors who were willing to install and use the app. In our observations, just a few minutes of such intimidating conversation led Merchant 12 to open up to the agent's proposal and ask further questions about the app. Agents described how they used these techniques to increase their chances of successfully onboarding the merchant and fulfilling the ambitious targets set by their company. On average, we found that agents were required to onboard eight merchants per day in a ten hour work shift to meet their goals and earn a decent commission.

Vulnerabilities during installation. After establishing a connection with the merchant, agents convinced them to hand over their smartphone to install the app. Agents did this by showing screenshots of lucrative app features, such as cashback or microloan offers. After taking the merchant's smartphone, the agent went straight to the Play store and installed their company app (see Figure 1.C,D).

While downloading the app, agents found small pockets of time, often while the merchant was dealing with a customer, to peek at the merchants' information in order to profile them. We observed agents scanning other competitor apps installed on the merchant's phone to understand their daily cash flow, total transactions, usage frequency, and the cashback they received. For instance, Agent 9 described how he glanced at the SMS containing daily transaction information that a merchant received in the last five days while

the merchant was busy. The information in the SMS helped him understand the merchant's usage. Agents then used the information to form strong arguments to convince the merchant to open an account with their company. Agent 9, on seeing relatively few transactions and perceiving a risk of losing the merchant, promised them a new speaker that came with the app to attract the merchant and convince him to register. Other agents used merchants' information to promise higher cashback prices than their competitors, assure efficient support, affirm swift transfer of money from their apps to the bank, and promise creation of a business profile for the merchant on the app. A few agents even pushed merchants to delete competitors' apps.

Our analysis shows that merchants had minimal understanding of agents' actions on their phones. Merchant 03 described how an agent took his smartphone to install the app and make an account:

"The agent was using both his smartphone and mine for making my digital account. He told me that he has downloaded the app on my mobile phone through which I could get money digitally. He was doing something on my smartphone and his smartphone, going back and forth at the same time. He kept doing multiple things without telling me. He was sometimes opening my gallery and SMS, but I let it happen as he told me it is important."

Agents' tactics made merchants vulnerable when they lost access to their own personal smartphones to the agents during the adoption process. Merchants experienced reduced agency when they were unable to say *"no"* to the actions that agents did on their device, creating *access-based vulnerabilities*. Merchant 05 described his loss of agency and *"helplessness"* in a similar situation where an agent pushed him to delete other apps and install their own:

" The agent suggested me to use his app only and remove others as he said that it is giving the best cashback. I asked how much cashback I will get by using the new app. He said it is better than the one I am using. I don't not know how he came to know that. Also if I remove the app, I lose customers, but if I miss this app, I lose high cashback. I feel helpless as a person who does not know much about these things."

Marques et al. defined access-based vulnerability as a state in which an individual's reduced or complete lack of access exposes them to potential harm [50]. Previous research shows that trust in the other party plays a key role in encouraging individuals to give up their access, despite feeling vulnerable, because of their positive expectations of the other party's intentions [46, 50]. Despite their apprehension, merchants in our study decided to trust the agents and put themselves in a vulnerable position because agents promised positive business opportunities through digital payments.

Interestingly, the practice of agents taking merchants' smartphones contradicted the best practices laid out by agents' companies, whose official directives explicitly discourage this behavior. Instead, agents are supposed to guide the merchants through installing the app on their own. However, none of the agents we observed followed these practices because it took too much time and therefore impacted agents' remuneration. Agent 7 who onboarded Merchant 24, said he would have lost commission from onboarding two other merchants if he had Merchant 24 do all the steps on his own. Agent 7 described how his supervisor pushed him to think along these lines:

"When I became an agent, I was appointed to a supervisor who gave directives to all of us ... I still remember on my first day he told me – 'The only thing that is important for you is to reach your daily target. So keep your head down, make sure to not waste your time, go to a shop, onboard them as quickly as possible, get lost and go to the next shop. That is it... As long as you are meeting your numbers you will be fine.'"

Vulnerabilities and fraud during account creation. The next step in the process involved agents persuading merchants to create an account in their newly installed app. Frequently, agents convinced merchants to let them do this by promising to delete the account later. During account creation, agents acted as *intermediaries*, collecting sensitive information from merchants, such as their phone number, photos of the merchant and their shop, and Aadhaar [1] details. They also collected financial information, such as bank account details, daily earnings, and tax details. In addition to entering these details in the official agent app provided by the companies, agents often shared these details via unofficial channels, such as WhatsApp groups, to coordinate and seek assistance from peer agents to onboard merchants. For instance, we observed Agent 1 initiating a video call while sharing Aadhaar and shop details of the merchant on WhatsApp when he had trouble validating the merchant's credentials and linking his bank account. Agent 5 described a similar process:

"Sharing information and coordination is vital in our network. As multiple agents visit the same shop, we achieve daily targets faster if we share the information over WhatsApp groups... we share proofs [photos of the IDs] along with strategies to onboard the merchant. This might include information like, 'merchant likes cashback offers, talk about cashback when you visit.'"

Disregarding the official instructions provided by their company, agents did not explain to merchants their sharing practices or why they needed certain pieces of information they requested. Consequently, participants like Merchant 24 described how they felt frustrated during the onboarding process:

"No information was given to me when he [Agent 7] made my account on this payment app. He took my phone... asked me for my bank details, my mobile number, my Aadhaar number and entered those in his phone and mine ... I don't know what he was doing or how he used that information to make the digital account. He even took a photo of the shop. What is the need of taking the photo of my shop, I don't know!... I tried to ask him but he told me that I don't have to worry and that company asks for these details while creating an account."

Sambasivan et al. [75] defined a *proximate-enabling* intermediary as an individual who extends the limited technology knowledge of end-users while fulfilling their objectives. Sambasivan showed how individuals used this position of power to assist marginalized users. Departing from this definition we saw that our intermediaries took advantage of their position of power to share personally identifiable information, contributing to vulnerability in the form of identity loss. Identity-based vulnerability has been described by Solove as a situation where an individual's identity is jeopardized through

[1] A 12-digit unique biometric ID used in India to establish proof for residency.

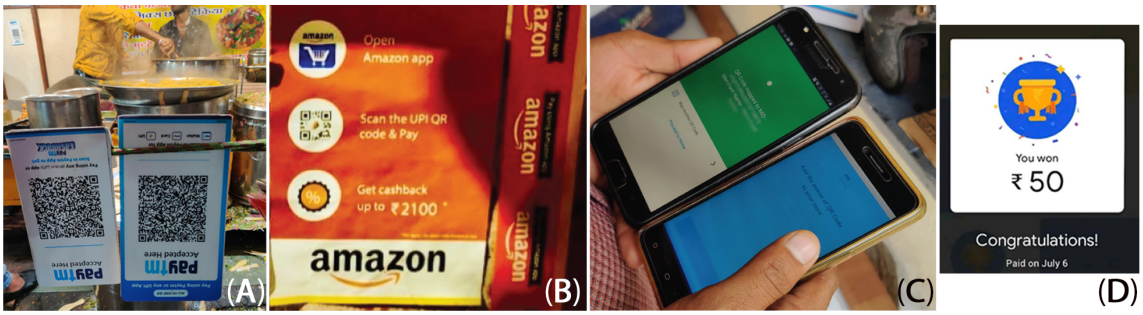

Figure 1: (A) A low income merchant displaying QR codes on his food cart; (B) Promotional sticker advertising cashback opportunities; (C) An agent using a merchant's phone and his phone side-by-side; (D) Typical example of cashback received by merchants.

information sharing practices that are outside individual's control, contributing to opportunities of identity theft [76].

A few agents took advantage of the merchants' vulnerabilities during onboarding to defraud the merchants. Four merchants described how agents stole their earnings by entering the agents' bank account details during onboarding, instead of the bank details provided by the merchants. Merchant 9, who owns a small electronic repair shop, described his experience:

> *"As the customers started using the payment service to pay me, the problem started. I was not receiving the money that customers were giving to me through the app. I was getting the SMS that the transfer happened but money was not going to my account. When I checked the transaction confirmation SMS, I saw that the bank's last four digits were not mine in the SMS ... Agent had entered some other account number while making the account. I strongly suspect the agent entered his details because he is not even picking up my call now."*

Two merchants described how their lack of trust on the agent prompted them to record agents' activities through their spouse's or friend's phone to capture evidence of any fraud agents might commit while handing their phone. Merchants felt that the act of recording in itself deterred agents from any foul play. A few merchants used alternative techniques. For instance, Merchant 8 took a picture of the agent's ID without his knowledge, noted his name and number, and then audio-recorded their conversation.

Lack of training on using payment apps. After onboarding, despite being part of their official responsibilities, agents did not provide adequate training to the merchants around using the app and troubleshooting basic issues. None of the three agents we observed made merchants aware of prevalent types of fraud they might encounter. As a result, merchants developed an incomplete or inaccurate mental model of the digital payment app and corresponding processes. Eighteen merchants were uncertain about how their digital earnings moved from the payment app to the bank and how to modify those settings. Merchant 8 explained his confusion:

> *"Even today I don't know how to check my bank account and how much money is currently in the app wallet, and how much has gone to the bank. The app does not show the money that is available in my bank... I panicked one day when I saw that app was showing zero rupees... My neighbor finally told me that app had transferred to my bank."*

4.2 At-transaction: Customer Purchases

We now move to *at-transaction* activities. Perry and Ferreira outlined the at-transaction stage as comprising of face-to-face purchase-related activities between the merchant and the customer [66]. In our study, activities that contributed to challenges included receiving payments from customers, verification of transactions, and managing social interactions around transactions.

Fraud via fake payment confirmation. Several merchants in our study (n=12) shared how customers defrauded them when making payments for purchases. Customers showed the screenshot of a successful transaction from the previous day to avoid paying for the merchandise they bought from the merchant. That way the screenshot of the app showed the same amount, same shop owner, and a tick mark indicating a successful transaction, which merchants checked to confirm, but did not check the date of the screenshot. Merchant 24 described how he was cheated by a customer who showed him a transaction of a big amount of ₹500 (US$9). Merchant 24 realized his mistake when he never received an SMS that confirmed the transaction. Merchant 2 described a similar situation:

> *"When the customer pays through the app, then I need to believe it ... One day the customer paid through Paytm and said his money had been deducted from his account. But I did not receive any SMS. I asked him how I can believe him, if I am not getting the message. He said something about the issue with phone towers and signals, which might cause the message to come late. I did not know all this. So I did not argue. I still insisted on seeing some proof. He did something on his phone for a few minutes and showed me the screen. It said successful transfer. I was convinced. I let him go ... I never saw him again. At night my son told me he committed fraud by showing an old transaction. I did not know you could do that! My son told me to check especially date and time ... they are so small and easy to miss!"*

Fraud via fake QR code stickers. Fraudsters also tampered with the QR codes that merchants displayed on their cart or makeshift shop. They printed and stuck fake QR codes over the original ones.

While the fake QR code looked visually similar to the ones provided by the companies, it contained a different UPI address that was mapped to the fraudster's bank account, instead of the merchant. As a result, every transaction that the customers did through the QR code was credited to the bank account of the fraudster. Merchant 3 was one of the three merchants who was a victim of such fraud.

Merchants were unaware of the possibility of such fraud. When asked, Merchant 3 shared his disbelief on how a physical sticker could be used for such a purpose. He felt that "*it is unimaginable to think someone could cheat such complicated pattern that is not understood by anyone.*" As a result, merchants did not inspect their stickers after they were installed. Merchant 3 suspected something was wrong when he stopped receiving SMS notifications from one of his digital payment apps despite multiple customers showing successful transactions. After taking his sticker down, he sought assistance from his nephew who tested the app by transferring a small amount. To his surprise, the name that appeared on the app when he scanned the QR code was different from the owner. When he inspected the QR code sticker closely, he realized that someone had stuck a different code over the original one. The merchant immediately took the QR code down and stopped using the app.

Factors that made merchants vulnerable to fraud. Customers and fraudsters took advantage of merchants by leveraging their vulnerable practices and identity, which made screenshot fraud very effective. Merchants' lack of training by the agents combined with limited understanding of the payment app in the pre-transaction activities pushed them to rely on limited technological cues to verify customer transactions. Even though the payment apps provided several in-app cues, such as transaction ID, date and time of transfer, sender's UPI ID, phone number, and a visual tick mark to indicate the transaction success (see Figure 2.A), most merchants (n=21) relied only on the *successful transfer* SMS sent by the bank or the app. It was also common for merchants to adopt and use multiple payment apps on a single phone. For instance, Merchant 14, who owned a juice shop, used five apps, namely Paytm, Bhim Pay, Amazon Pay, Phone Pe and Google Pay apps on his one phone and displayed those QR codes on the wall of his shop (see Figure 2.B). This meant that he received several SMSs from different apps on one smartphone for every customer purchase. This problem was exacerbated when SMS confirmations were delayed due to network issues. Vashistha's at al. alluded to similar issues [80]. Such practices and the resultant situations made merchants financially vulnerable. Financial vulnerability has been defined as the inability of an individual to protect themselves from harmful actions that contribute to the direct and indirect loss of their income [4, 59].

Merchants verification practices combined with delayed confirmations created opportunities for customers to shift the blame onto the merchant. They blamed merchants' lack of technological skills and inability to use the app, even publicly humiliating them in front of other customers. Participants like Merchant 16 explained how they ended up accepting the customer's word to avoid further embarrassment and not lose their other loyal customers:

> *"Another issue is that the customer says that the money has been deducted from his account. But most of the time the money does not reach me. . . . They [customers] shout at me in front of everyone, calling me a liar. I don't want to lose my business for one transaction and close my shop. I am left with no choice but to trust the customer. . . . Customers are educated, unlike us. It is a pity they find ways to avoid payment and make us suffer!"*

To make the situation worse, we observed customers using these strategies to commit fraud during the busiest business hours. Larger crowds made it easier for them to shift the blame onto merchants when they were less likely to check their devices for verification or cause an altercation that might cost them other customers' business.

Techniques to safeguard against fraud. Merchants did demonstrate resistance against the fraudulent techniques through a range of socio-technical strategies. A few merchants who owned mobile top-up and smartphone repair shops repurposed cheap webcams to capture customers they felt committed fraud and did not transfer money. They printed out the photos and stuck them in front of their shops to humiliate the customers. Merchants felt that these paper-based artifacts also deterred other customers from committing similar fraud. As Merchant 14 explained:

> *"We have been fed up with the customers who do not pay for what they purchased. Whenever a customer did not pay a big amount, we printed their photo and pasted it in front of our shop. . . . Mostly in our shop young boys and girls come. Irrespective of whether the fraud customer will come back or not, their friends will come and they will see their friend's photo. We will tell that the person in the photo has cheated and not paid. This way even if the customer ran away from us it will bring embarrassment to him, if his friends ask from him about the photo."*

A few merchants followed a more conservative approach by only accepting digital payments from regular or trusted customers:

> *"Whenever someone does Paytm to me, I am worried whether the money has come to me or not. I constantly check whether the money had been transferred to my account or not. I do not allow strangers to transfer through Paytm. You never know what trick the other person can do and take away all your money or fool you. I only allow those whom I know, otherwise I ask them to pay me cash. It is okay for me to not earn money but it is not okay for me to lose the money which I earned by working hard."*

Merchant 9 described how he maintained a log of what regular customers bought from his electronic repair shop. Once the expenditure reached a certain amount, he requested his customers to pay through the digital payment app. This method not only reduced the number of transactions but allowed easier tracking of the amount. Merchant 10 mentioned how he was especially wary of new customers and did not allow them to use the digital payment system, sometimes by saying that there were temporary issues with the payment app. A handful of merchants, such as Merchant 21 did not allow customers to walk away with purchased items until they confirmed that the money has been transferred, even if it meant longer wait times for customers at the cost of embarrassment to merchants. Lastly, a few merchants leveraged shared usage of the smartphones with their family members and co-workers—a common practice in Global South [2, 74, 79]—to manage transaction verifications during busy hours. Merchant 11, who helped her husband run a soda counter, shared how she kept an eye on the SMS they received for the transactions, while her husband prepared and served the

Figure 2: (A) Payment confirmation screen shown by the customer to merchant; (B) A merchant displaying five QR codes in his small shop. One QR code is hidden by the merchant (outlined in red); (C) A screenshot of a scammer's fake WhatsApp profile to trick merchants into believing they are a PhonePe Agent; (D) An example of an intimidating scam SMS received by a merchant.

soda. Her husband asked the customer to wait until he received approval from his wife.

4.3 Post-transaction: Beyond Customer Purchases

The post-transaction stage comprises activities beyond face-to-face purchases, including maintenance work and preparing for the next day's business [57, 66]. We now focus on the vulnerabilities merchants faced while seeking support, troubleshooting, and maintaining digital payment apps. We also describe challenges they experience using digital money to prepare the next day's business.

Lack of support from customer care and agents. In situations when coping strategies did not work to prevent fraud, merchants actively sought support from companies' customer care after their business hours. However, merchants struggled to follow the remote instructions provided by the customer care to diagnose and/or resolve the problem. For instance, Merchant 24 described how he called customer care because he was seeing his balance on the app but could not figure out why the money was not getting transferred to his bank account. When the customer care representative asked him to navigate to the settings to verify the bank address, Merchant 24 was unable to replicate the instructions even on the third try. His added fear of pressing the *"wrong button"* that might lead to financial loss further hindered his ability to follow the steps suggested by customer care. A few participants also described how the long conversation times frustrated customer care representatives, who promised to call back and follow up, but never did.

Consequently, merchants also sought assistance from the agents who originally onboarded them, but the agents often did not pick up the call because they were busy onboarding new merchants. Even if the agents answered the merchants' calls, they preferred trying to solve the issue remotely over a call that resulted in similar problems as customer care. A few agents who agreed to a physical visit came very late, with an average of two days delay. Merchant 9 explained his frustration in getting support from customer care and the agent:

"I stopped receiving confirmation SMSs last week. I should be getting the SMS whenever the transaction happens. I called the customer care number and told them my issue. But they did not clarify my issue; instead they told me that SMS might not be coming due to network issues. I told them my network is fine. Then they asked me to check some feature [notification permissions] in my settings. I did not know where that was. I struggled for 20 minutes. The customer care person clearly was frustrated. What is the need for me to take their app then experience anguish with some random guy whom I have never met? ... He eventually disconnected my call... I tried calling the agent who made my QR code but that number was not working. I tried many times, but the number was switched off. My neighboring shop owner told me that had stopped working and gave another contact. This agent also told me that he will not be able to come and help me as he is not working in that area... It took me two weeks to do all this during my business hours ... nothing came out of it. Finally a long-term customer of mine sorted the issue."

When we probed agents on this topic, they shared several issues that hindered them from supporting merchants. Agents often covered areas in clusters. After they covered an area and onboarded merchants, they moved to a new area. Most companies only incentivized agents to onboard merchants, not to support or sustain them, so agents were reluctant to travel back to older locations and provide support at their own expense. When the agents that we observed realized they were getting a call from a merchant they had already onboarded, they either ignored the call or promised to help at a later date that they did not intend to fulfill. Such practices deprived merchants of critical information to troubleshoot issues and protect themselves from scams. Multiple prior studies have indicated how such information asymmetry due to unequal possession and use of information contributes to *information vulnerability*, opening up opportunities for fraud [8, 15].

A few merchants created a workaround to force agents to visit their shops by hiding (or removing) the QR code stickers (see Figure 2B) or uninstalling the app. They felt that physically removing the sticker from the shop would push the agent to come to the neighborhood. Merchant 24 described how he managed to get his

agent's attention by removing the QR code from display and using other companies' payment apps instead.

Challenges preparing for next day's business using digital money. Merchants also experienced challenges in using their digital money to prepare for the next day's business. Most low-income merchants we interviewed sustained their businesses by reinvesting a significant portion of their daily earnings in procuring materials for the next day's business. For instance, the vegetable seller used his revenue from that day to visit the wholesale market to get more vegetables for the next day. However, the upstream wholesale traders from whom merchants bought their goods only accepted cash. This created problems when the merchant's prior day earnings were primarily digital. Merchant 23 described:

> *"My income through these digital apps is constantly increasing. I have two working men's hostels in front of my shop. They only pay through the app. Soon, I will have more digital money then cash in my hand .... This money in the app is totally wasted with my vegetable suppliers. They only take cash. The app money will be tax. But cash they can hide. I am the one who is stuck between the customers and these suppliers. I have no option but to listen to both. Otherwise I will have to close my business. I have asked my supplier several times to make an account on the app. He refuses to my face ...I sometimes take cash from my good friend and transfer him digital money. But how many times can I ask? It is embarrassing."*

Moreover, when their earnings were low or non-existent, merchants who were desperate also took micro-loans (known as *Udhaar*) from loan sharks to procure their daily merchandise. These contractors provided cash, but with high interest rates that had to be returned at the end of the day, and did not accept digital money in return as it was officially accountable and traceable. Consequently, most merchants (n=18) described how they felt trapped and restricted as they struggled to use their digitally earned money.

Merchants were also skeptical and afraid to spend their digital money on other services offered via digital apps, such as smartphone recharge, electricity and gas bill payments, buying public transportation tickets, and booking travel tickets. Most merchants (n=20) were reluctant to spend money on a service that they could easily pay for with cash or lacked the knowledge to conduct such transactions on their own. For instance, Merchant 19 described how he preferred adding a top-up to his phone from his neighboring shop and paying him at his convenience, instead of using the app. This overall lack of ease to use digital money for activities in their work and personal lives made merchants financially vulnerable.

Social engineering fraud via SMS and WhatsApp. Information and financial vulnerabilities due to lack of support and stagnant digital money provided further opportunities for serious fraud. One such fraud exploited merchants' inefficient support system and their over reliance on SMS for verification by sending an intimidating SMS message (see Figure 2.C) that claimed there were critical issues with their payment account, such as a hold on the account due to lack of accurate ID documents. These SMSs were designed to closely resemble an official message with a similar sender ID and message syntax. However, unlike an official SMS, the scammer appended their personal number as the contact information for customer care. When merchants dialed the number the scammer pretended to be a customer care agent and pressured them to resolve the account issue immediately, with failure to do so resulting in account suspension.

Razaq et al. [71] and Pervaiz et. al [67] categorized such tactics as *intimidation* frauds that leveraged individuals' information vulnerability to pressurize and force critical information out of them. Razaq et al. described how fraudsters used top-up cards as a major way to steal money [71]. Victims had to physically go to a top-up recharge broker, who at times warned the victim. Fraudsters in our study leveraged digital payments to trick payments out of the merchants. They shared a payment request link over the app, thereby eliminating the middle-person, like brokers, who might act as a last line of defense for the victim.

A variation of this fraud used WhatsApp calls from fake agent profiles to entice merchants, claiming they had a fake cashback amount pending in their account (see Figure 2.C). To establish trust with the merchant, the scammer initiated a small transfer request of money from their phone to the merchant's phone. The successful transfer of the small amount, which scammers cited as a transfer to validate the account, convinced merchants of the cashback and encouraged them to follow subsequent steps. Scammers then sent a transfer request for the fictitious cashback promised. However, instead of sending a request link to *send money to the merchant*, they shared a link to *request money from the merchant*. Merchants did not realize this subtle difference in the link and fell prey to it because the notifications and steps to request payment and send payment are quite similar. By the time merchants received an SMS notification for the deducted amount, instead of a refund, it was too late and the scammers were inaccessible. Merchant 9, who fell for such a trap and lost money, described:

> *"A person posing as a Paytm representative called and said I am eligible for the ₹1200 cashback but my cashback was stuck. He even knew my name. So, I thought he must be from customer care. He sent me an SMS with the request and I accepted the payment. But in the night I realized that money was deducted! ...It was two days of earnings that they stole from me. Next day, a regular customer told me that I should never accept such calls. I just studied till 10th grade. How will I know all this?...I tried calling the company's customer care. They said they can't help. What is the point? Who is protecting us? No one!"*

In our study, four merchants mentioned receiving such calls at least once, losing amounts ranging from ₹1,200 to ₹20,000 (US$15-300). Even though agents we interacted with were aware of these frauds, none provided any training to merchants on how to protect themselves. A few merchants tried to minimize their exposure to such fraud by opening and linking to a bank account used only for their digital payment apps. They transferred their daily earnings to this account, and then subsequently transferred it from that account to their main bank account, which was not connected to any payment apps. Merchant 6 described how this strategy ensured his losses were limited to just one or two days of earnings.

These findings corroborate Razaq et al. [71], who found mobile users in Pakistan were susceptible to SMS fraud. They saw how fraudsters used socially engineered messages to do call-based fraud, arguing that both urban and rural populations were vulnerable to the loss of personal information and experienced financial fraud.

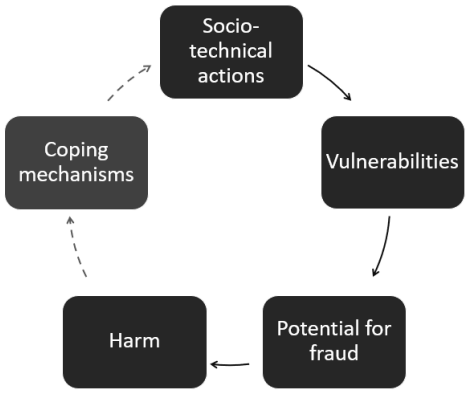

Figure 3: Cyclic vulnerability model. Dashed lines show optional coping mechanisms implemented by some merchants.

5 DISCUSSION

Vulnerability frameworks in HCI4D contexts. Our findings paint a concerning picture of merchants' business lives and show how they encounter at least four different types of vulnerabilities as they use digital payment systems: access-based, identity-based, financial, and informational vulnerabilities. Although these vulnerabilities are not exhaustive, we observed how merchants frequently experience them across all three stages of the Moneywork lifecycle.

McDonald & Forte emphasize the need to articulate such vulnerabilities to recognize the unequal harms inflicted on marginalized populations by different systems of oppression [51]. Doing so can help to give voice to these communities and create more equitable designs. Calo [15] adds depth to McDonald and Forte's argument by indicating how specific socio-technical situations can also contribute to an individual's vulnerability, which we saw when agents were coerced into adopting digital payment systems they did not understand. Both McDonald & Forte [51] and Calo [14] argue that failure to uncover and prevent such vulnerabilities can contribute to opportunities for fraud, thereby putting marginalized individuals in harm's way. Both McDonald & Forte's [51] and Calo's work [15] suggest a *linear* relationship: socio-technical actions lead to vulnerabilities, creating the potential for fraud, which leads to harm.

Our findings, by contrast, suggest a cyclic relationship between vulnerability, potential for fraud, and consequent harm (see Figure 3). We see how participants' vulnerabilities expose them to fraud and harm that further contribute to new vulnerabilities, leading to exacerbated consequences when compared to previous perspectives that treat vulnerability as part of a linear process. This cyclic behavior was evident across all stages of the Moneywork lifecycle.

For example, in the pre-transaction phase, agents used coercion and fear-instilling techniques to take control of the merchant's smartphone. Loss of control of their own device contributed to access-based vulnerability, which opened up opportunities for agents to commit fraud. Agents utilized this chance to not only peek into merchants' personal information, but also steal their money by entering their own financial details. As a result, merchants experienced privacy harm when their information was openly shared by agents outside the legal structures set by companies (i.e., on WhatsApp). They also experienced livelihood harm due to financial theft. Calo defined such instances as *objective* harm, where individuals experience measurable negative consequences due to fraud [14]. In addition to objective harm, Calo also discusses *subjective* harm as an unwanted perception of observation, such as anxiety, embarrassment, and fear that stem from the belief that one is being monitored. Our findings show merchants experienced subjective harm in the form of helplessness and loss of agency when they lost control of their device and were unable to do anything once agents controlled their phones.

Such harms in the pre-transaction phase further motivated socio-technical practices that led to vulnerabilities in the at-transaction phase. For instance, merchants' loss of agency and lack of training led to a problematic reliance on only a small set of features, like SMS, to safeguard their finances. This enabled fraudsters to take advantage of merchants' vulnerability by showing screenshots of old transactions, or physically manipulating the QR code stickers in merchants' shops. These frauds resulted in both the objective harm of livelihood loss, as well as subjective harm as merchants felt humiliated when customers blamed their lack of technical know-how and publicly embarrassed them.

The livelihood harm pushed merchants, in the post-transaction phase, to seek support from both companies' customer support and from agents. The ineffectiveness or lack of such support then further contributed to information vulnerability, opening up opportunities for SMS-based financial fraud when fraudsters posed as customer care agents. Significant financial losses through these frauds led to stress and anxiety for merchants, and further exacerbated livelihood and privacy harms. These findings are particularly concerning as digital payment systems expand to account for larger portions of merchants' overall financial transactions. A 2019 study of autorickshaw drivers who adopted digital payment systems showed that they used digital payments sparingly, preferring cash payment [57]. Autorickshaw drivers considered digital payment systems as a *money-guard*, primarily for saving secondary income [57]. In our study, we saw that this is not the case. Companies use lucrative features, such as cashback and microloans, to push adoption of digital payments for customers and merchants alike. This has increased the portion of merchants' overall income that flows through digital payment systems, with larger amounts of money in their digital wallets making merchants more financially vulnerable.

We saw how merchants tried to minimize the harms they experienced by adopting creative coping strategies, such as displaying the photos of culprits to warn other customers or restricting who could pay via digital payment services. Calo argues that such coping mechanisms are defense strategies exhibited by the victims to minimize the extent of harm in their lives [14]. We observed that merchants did a substantial amount of work devising and implementing such coping strategies. They also spent a large amount of time and energy trying to obtain support from companies' customer support and agents, all of which resulted in increased burdens and more labor for these low-income merchants. Previous studies have reflected on the additional labor marginalized populations had to perform in the form of *articulation* and *mobility* work to make

digital money work [57, 69]. For instance, rideshare drivers had to perform additional mobility work to convert digital money to cash because they did not use digital money for other things [57].

In our study, merchants' experiences of fraud pushed them to perform additional articulation and mobility work. We saw several instances where merchants had to argue against the fraudulent activities that customers conducted during transactions. When that did not work, they had to perform mobility work to repurpose technology to capture customers' photos, print it out, and stick it on their shops. Such actions required additional work and increased the burdens on these low-income workers.

Implications for digital payment systems. Our findings suggest that companies' current models for recruiting, onboarding, training, and supporting low-income merchants are not sufficient. The agents who are employed to recruit merchants are paid only according to the number of merchants that they onboard. This incentivizes agents to rapidly onboard as many merchants as possible, leading to coercive and fear-instilling practices. In addition, although agents are supposed to deliver essential training to merchants and help them to install the app and create an account themselves, we saw that in practice agents do not follow these steps because they do not receive compensation for these activities. Instead, agents' current practices often nullified the safeguards that companies' policies outlined to protect merchants' interests (e.g., that agents are prohibited from handling merchants' phones). We argue that companies' fixation on onboarding and subsequent failure to ensure proper training and support for merchants is detrimental to companies' in the long run, since merchants who experienced fraud or other harms frequently reduced or stopped accepting payments via the app.

Better onboarding practices could be achieved, for example, by changing agents' current incentive structures to reward agents who take the time to properly train merchants and ensure they have agency in the onboarding process. Agents can also make merchants aware of possible vulnerabilities and common frauds, and help merchants to develop bottom-up strategies to protect themselves. Reflection of these merchant-sustaining activities in agents' incentive models would encourage agents to spend more time with merchants and develop deeper relationships.

Beyond merchant onboarding, companies could employ agents to act as *merchant care agents* who are trained in supporting and sustaining merchants through empathy in all the stages of the Moneywork framework. Ensuring that agents are available in an area to visit merchants' shops and help them troubleshoot issues and challenges with digital payment systems could help to reduce merchants' vulnerabilities and subsequent fraud. Previous studies in HCI4D, especially in financial and health settings, have shown that agents can be reliable entities to oversee care-based socio-technical strategies that aid vulnerable populations [40, 55]. For instance Morawczynski et al. show that agents played a key role by providing vital financial education to rural populations [55]. Providing support to merchants at all stages of the Moneywork framework could help to break the cycle of vulnerabilities, frauds, and harms we encountered and reduce instances of merchants abandoning digital payments.

Finally, companies can further strengthen their merchant safeguard policies by better integrating them with existing government and non-profit efforts. For instance, the Indian government has developed and executed the Ombudsman Scheme for Digital Transactions to protect the interests of merchants by enabling them to share their challenges and concerns [61]. However, the initiative lacks systematic integration with the policies of digital payment companies, resulting in large quantities of unresolved issues. Companies have opportunities to integrate their internal policy efforts with such external initiatives to further minimize the harms experienced by merchants who use their payment systems. We argue that providing better support and protections for merchants is in-line with the companies commercial interests, since these efforts can reduce the number of merchants who abandon and/or refuse to adopt digital payment apps, while also improving merchants' wellbeing.

6 CONCLUSION AND LIMITATIONS

Our qualitative study examined the socio-technical interactions that low-income merchants engage in as they use digital payment systems. Informed by vulnerability literature and the Moneywork framework, we show how merchants experience four different types of vulnerabilities (access, identity, financial, and informational) when they interact with the agents and adopt and use digital payments. These vulnerabilities in turn contributed to fraud by agents, customers, and external fraudsters, leading to both subjective and objective harms. We show how merchants devise coping mechanisms to mitigate these harms, which adds to their burden and creates more work for them. We end by proposing a cyclic model of vulnerabilities and discuss practical implications for minimizing these vulnerabilities and improving merchants' experiences with digital payments.

Our study has several limitations. In addition to the inherent limitations of qualitative research, such as a small sample size and limited generalizability, we acknowledge that our findings capture predominantly male experiences, since all but one of our participants were men. We did not encounter any women agents in any of our fieldwork, finding this profession to be entirely male dominated. Although there are a few women merchants who run makeshift shops, they are still a minority. In addition, the author who conducted the fieldwork is a man, and women merchants may have been uncomfortable to be observed and interviewed by a man that they did not know. We would expect that women merchants might have different experiences that our findings do not cover and we plan to conduct future studies that explicitly engage women. We note also that future work should also engage with companies to elicit their perspectives on the digital payment ecosystems they create and support.

ACKNOWLEDGMENTS

This work was funded by a National Science Foundation CAREER Grant #1748903 and a gift from Mozilla. We thank all our study participants and the anonymous reviewers.

REFERENCES

[1] Shilpa Aggarwal and Leora Klapper. 2013. Designing government policies to expand financial inclusion: Evidence from around the world. *The Journal of Finance* 56, 3 (2013), 1029–51.

[2] Syed Ishtiaque Ahmed, Md Romael Haque, Irtaza Haider, Jay Chen, and Nicola Dell. 2019. " Everyone Has Some Personal Stuff" Designing to Support Digital Privacy with Shared Mobile Phone Use in Bangladesh. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–13.

[3] Irwin Altman. 1975. The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding. (1975).

[4] Luisa Anderloni, Emanuele Bacchiocchi, and Daniela Vandone. 2012. Household financial vulnerability: An empirical analysis. *Research in Economics* 66, 3 (2012), 284–296.

[5] Susan Athey, Christian Catalini, and Catherine Tucker. 2017. *The digital privacy paradox: Small money, small costs, small talk*. Technical Report. National Bureau of Economic Research.

[6] Yoris A Au and Robert J Kauffman. 2008. The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application. *Electronic Commerce Research and Applications* 7, 2 (2008), 141–164.

[7] Rajesh Krishna Balan, Narayan Ramasubbu, Komsit Prakobphol, Nicolas Christin, and Jason Hong. 2009. mFerio: the design and evaluation of a peer-to-peer mobile payment system. In *Proceedings of the 7th international conference on Mobile systems, applications, and services*. 291–304.

[8] Masooda Bashir, Carol Hayes, April D Lambert, and Jay P Kesan. 2015. Online privacy and informed consent: The dilemma of information asymmetry. *Proceedings of the Association for Information Science and Technology* 52, 1 (2015), 1–10.

[9] 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*. 39–44.

[10] Sharit K Bhowmik. 2007. Street vending in urban India: the struggle for recognition. In *Street Entrepreneurs*. Routledge, 114–129.

[11] Muhammad Bilal and Ganesh Sankar. 2011. Trust & Security issues in Mobile banking and its effect on Customers.

[12] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.

[13] ET Bureau. 2017. *Paytm Mall to hire 3000 agents to help local stores sell on its platform*. Retrieved January 1, 2021 from https://economictimes.indiatimes.com/small-biz/startups/paytm-mall-to-hire-3000-agents-to-help-local-stores-sell-on-its-platform/articleshow/59212571.cms?from=mdr

[14] Ryan Calo. 2011. The boundaries of privacy harm. *Ind. LJ* 86 (2011), 1131.

[15] Ryan Calo. 2018. Privacy, Vulnerability, and Affordance. In *The Cambridge Handbook of Consumer Privacy* (first ed.), Evan Selinger, Jules Polonetsky, and Omer Tene (Eds.). Cambridge University Press, 198–206. https://doi.org/10.1017/9781316831960.011

[16] Stevie Chancellor, Jessica Annette Pater, Trustin Clear, Eric Gilbert, and Munmun De Choudhury. 2016. #thyghgapp: Instagram Content Moderation and Lexical Variation in Pro-Eating Disorder Communities. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing* (San Francisco, California, USA) *(CSCW '16)*. Association for Computing Machinery, New York, NY, USA, 1201–1213. https://doi.org/10.1145/2818048.2819963

[17] Priyank Chandra and Joyojeet Pal. 2019. Rumors and Collective Sensemaking: Managing Ambiguity in an Informal Marketplace. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–12.

[18] Sumedha Chauhan. 2015. Acceptance of mobile money by poor citizens of India: Integrating trust into the technology acceptance model. *info* (2015).

[19] Apala Lahiri Chavan, Sarit Arora, Anand Kumar, and Praneet Koppula. 2009. How mobile money can drive financial inclusion for women at the Bottom of the Pyramid (BOP) in Indian urban centers. In *International Conference on Internationalization, Design and Global Development*. Springer, 475–484.

[20] Dai-Yon Cho, Hyun Jung Kwon, and Hyoung-Yong Lee. 2007. Analysis of trust in internet and mobile commerce adoption. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*. IEEE, 50–50.

[21] Frank Rudy Cooper. 2014. Always Already Suspect: Revising Vulnerability Theory. *North Carolina Law Review* 93 (2014), 1339.

[22] John W Creswell and Dana L Miller. 2000. Determining validity in qualitative inquiry. *Theory into practice* 39, 3 (2000), 124–130.

[23] Kevin Donovan. 2012. Mobile money for financial inclusion. *Information and Communications for development* 61, 1 (2012), 61–73.

[24] Brianna Dym and Casey Fiesler. 2018. Vulnerable and online: Fandom's case for stronger privacy norms and tools. In *Companion of the 2018 ACM Conference on Computer Supported Cooperative Work and Social Computing*. 329–332.

[25] Jennifer Ferreira, Mark Perry, and Sriram Subramanian. 2015. Spending Time with Money: From Shared Values to Social Connectivity. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (Vancouver, BC, Canada) *(CSCW '15)*. Association for Computing Machinery, New York, NY, USA, 1222–1234. https://doi.org/10.1145/2675133.2675230

[26] Finara. 2021. *Digital Payments to Hit $6.6T Value in 2021, a 40% Jump in Two Years*. Retrieved March 1, 2021 from https://www.finaria.it/pr/digital-payments-to-hit-6-6t-value-in-2021-a-40-jump-in-two-years/

[27] Martha Albertson Fineman. 2010. The Vulnerable Subject and the Responsive State. *Emory Law Journal* 60 (2010), 251.

[28] J. Foelste and A Khairy. 2019. *Leveraging Technologies to Improve the Quality and Maximize the Productivity of Agent Models*. Technical Report. Washington, DC, USA.

[29] Cyril Fouillet, Isabelle Guérin, and Jean-Michel Servet. 2021. Demonetization and digitalization: The Indian government's hidden agenda. *Telecommunications Policy* 45, 2 (2021), 102079. https://doi.org/10.1016/j.telpol.2020.102079

[30] Daniela Gabor and Sally Brooks. 2017. The digital revolution in financial inclusion: international development in the fintech era. *New Political Economy* 22, 4 (2017), 423–436.

[31] Arunava Ghosh. 2017. Turning India into a Cashless Economy: The Challenges to Overcome. *Available at SSRN 2989290* (2017).

[32] Ishita Ghosh. 2012. The mobile phone as a link to formal financial services: Findings from Uganda. In *Proceedings of the Fifth International Conference on Information and Communication Technologies and Development*. 140–148.

[33] Ishita Ghosh and Jacki O'Neill. 2020. The Unbearable Modernity of Mobile Money. *Computer Supported Cooperative Work (CSCW)* (2020), 1–35.

[34] Leo A Goodman. 1961. Snowball sampling. *The annals of mathematical statistics* (1961), 148–170.

[35] 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.

[36] Serena Hillman, Carman Neustaedter, Erick Oduor, and Carolyn Pang. 2014. User challenges and successes with mobile payment services in North America. In *Proceedings of the 16th international conference on Human-computer interaction with mobile devices & services*. 253–262.

[37] Srihari Hulikal Muralidhar, Claus Bossen, Apurv Mehra, and Jacki O'Neill. 2018. Digitizing Monetary Ecologies: Intended and Unintended Consequences of Introducing a Financial Management App in a Low-Resource Setting. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–17.

[38] 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*. 1–11.

[39] Badar Alam Iqbal and Shaista Sami. 2017. Role of banks in financial inclusion in India. *Contaduría y administración* 62, 2 (2017), 644–656.

[40] Azra Ismail and Neha Kumar. 2019. Empowerment on the margins: The online experiences of community health workers. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–15.

[41] Tanmay Joshi, Sharmistha Swasti Gupta, and Nimmi Rangaswamy. 2019. Digital Wallets 'Turning a Corner'for Financial Inclusion: A study of Everyday PayTM Practices in India. In *International Conference on Social Implications of Computers in Developing Countries*. Springer, 280–293.

[42] Deepa Krishnan and Stephan Siegel. 2017. Effects of demonetization: Evidence from 28 slum neighborhoods in mumbai. *Available at SSRN 2896026* (2017).

[43] K.Hema Divya K.Suma vally. 2018. A study on Digital payments in India with perspective of consumers adoption. *International Journal of Pure and Applied Mathematics* 118, 24 (2018).

[44] Deepti Kumar, David Martin, and Jacki O'Neill. 2011. The times they are a-changin' mobile payments in india. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 1413–1422.

[45] Neetu Kumari and Jhanvi Khanna. 2017. Cashless payment: A behaviourial change to economic growth. *Qualitative and Quantitative Research Review* 2, 2 (2017).

[46] Roy J Lewicki, Edward C Tomlinson, and Nicole Gillespie. 2006. Models of interpersonal trust development: Theoretical approaches, empirical evidence, and future directions. *Journal of management* 32, 6 (2006), 991–1022.

[47] 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*. 1–14.

[48] Scott Mainwaring, Wendy March, and Bill Maurer. 2008. From meiwaku to tokushita! Lessons for digital money design from Japan. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 21–24.

[49] Niina Mallat. 2007. Exploring consumer adoption of mobile payments–A qualitative study. *The Journal of Strategic Information Systems* 16, 4 (2007), 413–432.

[50] Diogo Marques, Tiago Guerreiro, Luís Carriço, Ivan Beschastnikh, and Konstantin Beznosov. 2019. Vulnerability & Blame: Making Sense of Unauthorized Access to Smartphones. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–13.

[51] Nora McDonald and Andrea Forte. 2020. The Politics of Privacy Theories: Moving from Norms to Vulnerabilities. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–14.

[52] Indrani Medhi, Aishwarya Ratan, and Kentaro Toyama. 2009. Mobile-banking adoption and usage by low-literate, low-income users in the developing world. In *International conference on internationalization, design and global development*. Springer, 485–494.

[53] Hamid Mehmood, Tallal Ahmad, Lubna Razaq, Shrirang Mare, Maryem Zafar Usmani, Richard Anderson, and Agha Ali Raza. 2019. Towards Digitization of Collaborative Savings Among Low-Income Groups. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–30.

[54] Aakash Mehrotra, Akhand Tiwari, MP Karthick, Mimansa Khanna, Vivek Khanna, Bhavana Srivastava, Manoj Sharma, and Sidra Butt-Mughal. 2018. State of the agent network, India 2017.

[55] Olga Morawczynski, David Hutchful, Edward Cutrell, and Nimmi Rangaswamy. 2010. The bank account is not enough: Examining strategies for financial inclusion in India. In *Proceedings of the 4th ACM/IEEE international conference on information and communication technologies and development*. 1–11.

[56] Francisco Munoz-Leiva, S Climent-Climent, and Francisco Liébana-Cabanillas. 2017. Determinants of intention to use the mobile banking apps: An extension of the classic TAM model. *Spanish Journal of Marketing-ESIC* 21, 1 (2017), 25–38.

[57] Srihari Hulikal Muralidhar. 2019. Making Digital Money "Work" for Low-Income Users: Critical Reflections for HCI. *International Journal of Mobile Human Computer Interaction (IJMHCI)* 11, 4 (2019), 49–65.

[58] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.

[59] Genevieve E. O'Connor, Casey E. Newmeyer, Nancy Yee Ching Wong, Julia B. Bayuk, Laurel A. Cook, Yuliya Komarova, Cazilla Loibl, L. Lin Ong, and Dee Warmath. 2019. Conceptualizing the multiple dimensions of consumer financial vulnerability. *Journal of Business Research* 100 (2019), 421–430. https://doi.org/10.1016/j.jbusres.2018.12.033

[60] Raphael Odoom and John Paul Kosiba. 2020. Mobile money usage and continuance intention among micro enterprises in an emerging market–the mediating role of agent credibility. *Journal of Systems and Information Technology* (2020).

[61] Ministry of Electronics and Information Technology. 2019. *Ombudsman Scheme for Digital Transactions*. Retrieved April 7, 2021 from https://vikaspedia.in/e-governance/digital-payment/policies-and-schemes/ombudsman-scheme-for-digital-transactions

[62] Jan Ondrus and Yves Pigneur. 2006. Towards a holistic analysis of mobile payments: A multiple perspectives approach. *Electronic commerce research and applications* 5, 3 (2006), 246–257.

[63] Jacki O'neill, Anupama Dhareshwar, and Srihari H Muralidhar. 2017. Working digital money into a cash economy: The collaborative work of loan payment. *Computer Supported Cooperative Work (CSCW)* 26, 4-6 (2017), 733–768.

[64] Joyojeet Pal, Priyank Chandra, Vaishnav Kameswaran, Aakanksha Parameshwar, Sneha Joshi, and Aditya Johri. 2018. Digital payment and its discontents: Street shops and the Indian government's push for cashless transactions. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–13.

[65] Saurabh Panjwani and Edward Cutrell. 2010. Usably secure, low-cost authentication for mobile banking. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*. 1–12.

[66] Mark Perry and Jennifer Ferreira. 2018. Moneywork: Practices of use and social interaction around digital and analog money. *ACM Transactions on Computer-Human Interaction (TOCHI)* 24, 6 (2018), 1–32.

[67] 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*. 195–205.

[68] Martin Pirker and Daniel Slamanig. 2012. A framework for privacy-preserving mobile payment on security enhanced arm trustzone platforms. In *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE, 1155–1160.

[69] Gary Pritchard, John Vines, and Patrick Olivier. 2015. Your money's no good here: The elimination of cash payment on London buses. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. 907–916.

[70] Daniel Radcliffe and Rodger Voorhies. 2012. A digital pathway to financial inclusion. *Available at SSRN 2186926* (2012).

[71] Lubna Razaq, Tallal Ahmad, Umer Ramzan, and Shrirang Mare. 2021. "We Even Borrowed Money From Our Neighbor": Understanding Mobile-based Fraud Through Victims' Experiences. *Proceedings of the ACM on Human-Computer Interaction* CSCW (2021).

[72] Bradley Reaves, Jasmine Bowers, Nolen Scaife, Adam Bates, Arnav Bhartiya, Patrick Traynor, and Kevin RB Butler. 2017. Mo (bile) money, mo (bile) problems: Analysis of branchless banking applications. *ACM Transactions on Privacy and Security (TOPS)* 20, 3 (2017), 1–31.

[73] Ms Ratna Sahay, Mr Ulric Eriksson von Allmen, Ms Amina Lahreche, Purva Khera, Ms Sumiko Ogawa, Majid Bazarbash, and Ms Kimberly Beaton. 2020. *The promise of fintech: Financial inclusion in the post COVID-19 era*. International Monetary Fund.

[74] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. 2018. " Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*. 127–142.

[75] Nithya Sambasivan, Ed Cutrell, Kentaro Toyama, and Bonnie Nardi. 2010. Intermediated technology use in developing communities. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2583–2592.

[76] Daniel J Solove. 2002. Identity theft, privacy, and the architecture of vulnerability. *Hastings Lj* 54 (2002), 1227.

[77] Matthew Soursourian, Ariadne Plaitakis, and Emilio Hernandez. 2019. AGENT NETWORKS AT THE LAST MILE. (2019).

[78] Press trust of India. 2016. *Paytm to hire 10,000 agents to expand offline merchant network*. Retrieved January 1, 2021 from https://economictimes.indiatimes.com/small-biz/startups/paytm-to-hire-10000-agents-to-expand-offline-merchant-network/articleshow/55355204.cms

[79] Rama Adithya Varanasi, Aditya Vashistha, Tapan Parikh, and Nicola Dell. 2020. Challenges and Issues Integrating Smartphones into Teacher Support Programs in India *(ICTD2020)*. Association for Computing Machinery, New York, NY, USA, Article 10, 11 pages. https://doi.org/10.1145/3392561.3394638

[80] Aditya Vashistha, Richard Anderson, and Shrirang Mare. 2019. Examining the use and non-use of mobile payment systems for merchant payments in India. In *Proceedings of the 2nd ACM SIGCAS Conference on Computing and Sustainable Societies*. 1–12.

[81] Viswanath Venkatesh, Venkataraman Ramesh, and Anne P Massey. 2003. Understanding usability in mobile commerce. *Commun. ACM* 46, 12 (2003), 53–56.

[82] John Vines, Paul Dunphy, Mark Blythe, Stephen Lindsay, Andrew Monk, and Patrick Olivier. 2012. The Joy of Cheques: Trust, Paper and Eighty Somethings. In *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work* (Seattle, Washington, USA) *(CSCW '12)*. Association for Computing Machinery, New York, NY, USA, 147–156. https://doi.org/10.1145/2145204.2145229

[83] John Vines, Paul Dunphy, and Andrew Monk. 2014. Pay or delay: the role of technology when managing a low income. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 501–510.

[84] Alan F Westin. 1968. Privacy and freedom. *Washington and Lee Law Review* 25, 1 (1968), 166.