"We Even Borrowed Money From Our Neighbor": Understanding Mobile-based Fraud Through Victims' Experiences

LUBNA RAZAQ, HCDE, University of Washington, USA & Information Technology University, Pakistan
TALLAL AHMAD, Lahore University of Management Sciences (LUMS), Pakistan
SAMIA IBTASAM, Paul G. Allen School of Computer Science & Engineering, University of Washington
UMER RAMZAN, Information Technology University, Pakistan
SHRIRANG MARE, Western Washington University, USA

Mobile-based scams are on the rise in emerging markets. However, the awareness about these scams and ways to avoid them remains limited among mobile users. We present a qualitative analysis of the dynamics of mobile-based fraud (specifically, SMS and call-based fraud) in Pakistan. We interviewed 96 participants, including different stakeholders in the mobile financial ecosystem: 71 victims of mobile-based scams, seven non-victims, 15 mobile money agents, and three officials from regulatory agencies that investigate mobile-based fraud. Leveraging the perspectives from these stakeholders and analyzing mobile-based fraud with a four-step social-engineering attack framework, we make four concrete contributions: First, we identify the nuances as well as specific tactics, methods, and resources that fraudsters use to scam mobile users. Second, we look at other actors, beyond the victim and the adversary, involved or affected by fraud and their roles at each step of the fraud process. Third, we discuss victims' understanding of mobile fraud, their behavior post-realization, and their attitudes toward reporting fraud. Finally, we discuss possible points of intervention and offer design recommendations to thwart mobile fraud, including addressing the vulnerabilities discovered in the ecosystem, utilizing existing actors to mitigate the consequences of these attacks, and realigning the design of fraud reporting mechanisms with the sociocultural practices.

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

Additional Key Words and Phrases: Phishing; Vishing; SMS-based Fraud; Financial Services; Smartphone; Fraud; Security; Social Engineering; Qualitative Interviews

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

Authors' addresses: Lubna Razaq, lubnar@uw.edu, HCDE, University of Washington, USA, & Information Technology University, Pakistan; Tallal Ahmad, tallal.ahmad@lums.edu.pk, Lahore University of Management Sciences (LUMS), Lahore, Pakistan; Samia Ibtasam, samiai@cs.washington.edu, Paul G. Allen School of Computer Science & Engineering, University of Washington; Umer Ramzan, umer.ramzan@itu.edu.pk, Information Technology University, Lahore, Pakistan; Shrirang Mare, shri.mare@wwu.edu, Western Washington University, USA.

2573-0142/2021/4-ART41 $15.00
https://doi.org/10.1145/3449115

1 INTRODUCTION

The Global System for Mobile Communication Association (GSMA) predicts that the world's mobile subscribers will increase from 5.2 billion in the year 2019 (accounting for 67% of the global population) to 5.8 billion (70% of the world's population) in 2025. Most of these 600+ million new subscribers will be in the emerging economies with most of the new users predicted to be in India, China, Pakistan, and Nigeria [29]. Leveraging this growing mobile-phone infrastructure, governments and organizations throughout the developing world are seeking to provide affordable services over mobile phones. This includes Digital Financial Services (DFS) which are designed to deliver financial services at lower costs over the digital medium to overcome the limitations posed by the high costs of physical networks [42].

However, as the adoption of mobile phones and DFS increases, the issue of fraud follows alongside. Fraud both contributes to the loss of users' money and undermines trust in these systems as a whole. This issue is particularly important in the developing world, where poor populations with lower financial cushion may be affected dramatically by small monetary losses, and they may lose trust in digital technologies.

Mobile-based fraud (or simply called mobile fraud) is a growing concern, as documented by industry reports (e.g., [24]) as well as by academic literature (e.g., [1, 6, 14, 53]). Fraudsters leverage the increased mobile connectivity to target and scam mobile users, particularly the less technologically-literate users who might be unaware of mobile fraud. Due to the prevalence of feature phones in the developing world and the low-technical and infrastructure requirements, SMS is a popular choice for communication (e.g., financial transaction alerts, confirmation) for mobile money operators, banks, and government organizations. Thus, it is easy for users to confuse fake SMSes (*smishing* or fraud initiated by an SMS) and calls (*vishing* or frauds initiated by a phone call) from real ones. We collectively denote both smishing and vishing as mobile-based frauds.

Our Work

Our work continues the recent focus of CHI and CSCW communities on understanding and addressing the security and privacy challenges around the use of mobile phones in emerging markets [5, 14, 40, 73]. Around 78% of Pakistanis own or have access to a mobile phone [8] and 23% are financially *included*, i.e., they own a transaction account with a bank or mobile money operator [72]. To understand SMS and call-based fraud in Pakistan, we interviewed three key stakeholders in the mobile financial ecosystem: users, agents, and regulatory agency officials. Users are generally the target in mobile-based frauds; we interviewed users who had lost money through mobile fraud (henceforth referred to as *victims*) as well as users who engaged with fraudsters but did not lose money (*non-victims*). Agents provide Over-The-Counter (OTC) mobile money services to users. They are key players in users' engagement and use of mobile money services and are also affected by fraud in the ecosystem. Regulatory and law enforcement agencies handle complaints and investigations about mobile-based fraud and officials in these agencies offer the law enforcement perspective about mobile-based frauds. Using the perspectives provided by these stakeholders, we examined mobile fraud from different lenses and identified the issues in the existing mobile and mobile-based financial services that are leveraged by fraudsters.

Our work sheds light on the specific tactics and mechanisms that fraudsters use to scam mobile users in Pakistan. Specifically, we focus on the following research questions:

(1) What are the types of frauds that people encounter and what are their mental models of fraud? (Section 5)

(2) How do fraudsters scam mobile phone users and what are the different fraud schemes [1] used by fraudsters? (Section 6)
(3) What roles do friends, family, and mobile money agents play in these frauds? (Section 7)
(4) What are the repercussions of fraud? What are the participants' attitudes and perceptions toward reporting fraud? (Sections 8-9)
(5) How can we design better systems or social interventions to help mitigate mobile fraud? (Section 10)

To answer these questions we conducted semi-structured interviews with 71 victims, 7 non-victims, 15 mobile money agents, and informal conversations with 3 officials from regulatory and law enforcement agencies. We utilize a four-step social-engineering attack framework [48] to identify the methods that fraudsters use to gain victims' trust, deteriorate their decision-making ability, and to ensure compliance from the victims. We find that fraudsters exploit the less technologically literate mobile phone users and Computerize National Identify Card (CNIC) holders to gather resources to carry out attacks. In the absence of formal warning systems, the warnings and realization triggers are largely social and vary across victims. We demonstrate that agents, friends, family, and colleagues are human assets that can act as points of intervention to mitigate fraud. We show how the socio-cultural stigmas around fraud prevent women victims from reporting or sharing their experiences and thereby leaving gaps in their mental models. We chronicle points of exploitation used by fraudsters and recommend intervention at the user and regulatory levels.

Our work contributes to a growing body of literature on security, privacy, and social engineering attacks in developing regions by mapping experiences and perspectives of victims and stakeholders on the social engineering framework. We explore the roles of stakeholders other than the victim and the adversary in the social-engineering attack life cycle. We also study the attack life cycle from victims' and non-victims' perspectives and explain their understanding, realization triggers, reactions, and changes in behavior, including reporting behavior after frauds.

The rest of the paper is organized as follows. We explain the necessary background about the mobile money ecosystem in Pakistan in Section 2. In Section 3, we situate our work in the existing literature on SMS and call-based frauds in mobile money systems. Section 4 describes our methodology, followed by findings in Sections 5-9. In Section 10, we discuss the implications of our findings and provide recommendations for different stakeholders in the mobile money ecosystem.

2 BACKGROUND

Before defining and describing the mobile-fraud process, we explain the various actors involved in the process as identified in our study. These actors play diverse roles in (aiding or hindering) the fraud process; we discuss these roles in later sections.

Fraud Victim. *Fraud victims*, in the context of this paper, are mobile users who have lost money to a scam initiated and carried out over a phone call or message.

Non-victim. Non-victims are mobile users who responded to a fraudulent call or message, engaged with a fraudster but did not lose money.

Fraudster. Fraudsters are adversaries that perpetrate social engineering frauds acting alone or working in groups. They can have varying levels of sophistication and organization.

Family/Friends of Victims. Pakistani society has close-knit and highly gendered family structures with family members affecting women's technological interactions [33]. We, therefore, observe family members and friends playing different roles in the fraud-related experiences. Depending on

[1] We define a **Fraud Scheme** as any prevailing trend or program that fraudsters use when targeting mobile users; for example, a hit television game show, a recent census drive, government schemes or cash transfer programs.

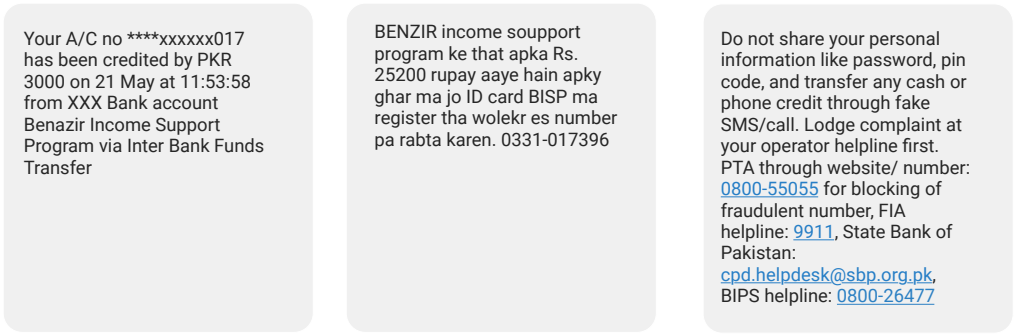

Fig. 1. Example SMSes about mobile frauds. Sample BISP money-transfer SMS sent by the Government of Pakistan to individuals receiving financial support under the BISP scheme (left); Spam message mimicking a BISP message program. (Translation: You have received Rs. 25200 under the BENZIR income soupport (spelling mistakes from original message kept intact which are an indicator of fraudulent messages.) Contact this number 0331-017396 along with the ID card in your home which is registered on BISP) (middle); SMS warnings sent by the Pakistan Telecommunication Authority (PTA) to mobile users (right)

the information-level of the friends or family members, they either encourage the victim to follow fraudster's instructions or limit the victim's compliance to the fraudster by warning them.

Banks. Victims of bank-related fraud typically interface with the bank either through the bank branch where they have an account or through the bank's central helpline.

Mobile Money Agents and Top-Up corner shops. Mobile Money networks were created to financially include the lower-income unbanked customers in emerging markets who have access to mobile phones. They capitalize on the extensive telecommunication and retailer network to provide financial services through either handheld devices using a mobile wallet account or via Over-The-Counter (OTC) transactions through mobile money agents. OTC services utilize the Computerized National Identity Cards (CNICs) to identify sender and recipient in a transaction.

Mobile-money agents are small-shop owners, mostly men [36], who run corner mom and pop shops for local community needs along with providing mobile financial services like Over-The-Counter (OTC) transactions for remitting money using their cash pool. Whereas some corner shops only sell top-up cards without OTC services. All of them are usually familiar with the neighborhood, its residents, and their financial and social dealings. Victims often send money or mobile credit in the form of mobile top-up cards' serial numbers to the fraudsters by visiting either 1) *mobile money agents* - who sell both airtime and provide OTC services; or 2) *the corner shops* - which only sell top-up cards, making interactions with agents and shopkeepers as possible points of intervention.

3 RELATED WORK

In many ways, mobile-based frauds are an extension of online social engineering scams, targeting mobile users (e.g., using calls and SMS instead of emails), by leveraging the processes and norms around mobile-based services, such as mobile payments, mobile banking, and mobile recharge. In this section, we first discuss prior works about online scams and social engineering attacks, which we use as a framework to analyze and present our findings on mobile fraud. We then discuss the use of mobile phones in the Global South and prior works on understanding and addressing the unique security and privacy challenges faced by mobile users in the Global South. Finally, we share recent work on mobile fraud and how our study extends that work.

3.1 Online Scams and Social Engineering Attacks

Since the early days of the Internet, online scammers have been using social engineering techniques to scam individuals and organizations; a notable example is the Nigerian advance fee scam [51]. Social engineering is defined as *"The Science of using social interaction as a means to persuade an individual or an organization to comply with a specific request from an attacker where either the social interaction, the persuasion or the request involves a computer-related entity."* [47]. To persuade (or manipulate) individuals, attackers use techniques that exploit human cognitive biases [34]. Depending on the underlying technique, social engineering can be classified into five categories: *i)* Social Engineering via telephone communication, which is characteristic of smishing and vishing; *ii)* Dumpster diving (i.e., office or electronic waste); *iii)* Online social engineering (i.e., on the web through browsing); *iv)* Persuasion (face to face communication), and; *v)* Reverse Social engineering [39]. Even though social engineering attacks vary, they follow a common pattern consisting of four phases: *i)* Gather information about the target; *ii)* Build rapport with the target; *iii)* Exploit the available information and execute the attack and; *iv)* Exit leaving no evidence [48]. We present our findings (in Section 6) using the social engineering framework proposed by Mouton et al. [48].

With the proliferation of mobile devices and mobile financial services, fraudsters have a larger pool of potential targets, evident by the increase in social engineering attacks on mobile devices [55, 76]. In our work, we focus on social-engineering attacks over calls and SMSes, which are the leading ways of communication and, thus, the leading ways of phishing in the Global South [41]. For example, attackers lure or manipulate mobile users to either disclose their private information (e.g., ATM PIN) or send money as an "advanced fee" for a prize [58].

3.2 Security and Privacy in the Global South

Information Communication Technologies (ICTs), are often considered as a catalyst for socio-economic development for low-resourced communities globally. The availability of affordable mobile phones has provided access to the majority of the previously hard-to-reach populations [43]. This increasing number of mobile users with varying socioeconomic, literacy, and language barriers is vulnerable to privacy and security attacks as the technology usage, information utilization, and sharing practices of the population living in the Global South are notably different from those in the Global North. There have been many efforts to understand and mitigate these threats including password construction [15], deducing preference by social network behavior [27], studying privacy on mobile devices [59, 60] and helping privacy through design [38]. However, these studies focused primarily on Western privacy concepts that do not encapsulate the privacy practices in developing regions. There is a need to study the privacy and security practices in the Global South, understand the technology usage differences and resulting unique security and privacy implications, and address those unique challenges [52, 73].

Some previous works in developing countries have attempted to highlight the unique security and privacy challenges. For example, Ahmed et al. [4] provide a holistic local interpretation of privacy threats users face at mobile repair shops in Bangladesh; their work re-validates Nissenbaum's notion of privacy as contextual integrity [52]. They highlight mobile phone users' lack of awareness regarding the loss of privacy in the repair process and suggest designing solutions for preserving privacy in repair by leveraging the cultural and religious values of society [61–63]. To that end, [3, 69] explored the interactions and privacy perceptions of users with identity infrastructures in the Global South. Another study [5] noted that broad conceptualization of privacy influences the design of devices used in the Global South context but their privacy features only tend to work in stable environments (e.g., stable democracies). So privacy not only needs to be studied in different social and cultural contexts but also in a diverse political environments and settings.

Besides differences of perceptions around security and privacy between the developed world and the Global South, gender also impacts the semantics of security [66] as women tend to have a stronger perception about security of a particular method than men [20]. Apart from gender, prior works suggest that individuals from low socioeconomic status have differing privacy norms, and variations in socioeconomic status are associated with differences in users' security and privacy beliefs and behaviors [17, 30, 45, 57]. We continue this line of work to understand and describe user perception and understanding of security and privacy in the Global South. Engaging with diverse users, we identify the various actors at play in the life cycle of mobile-based frauds in the Global South and map their experiences on this life cycle.

3.3 Mobile Fraud

The chances of users falling prey to mobile fraud is increasing with the growing number of mobile phone users in the Global South [10, 28]. Growing number of transactions on mobile devices, as compared to desktops, makes mobile users an attractive target for fraudsters. According to a recent industry report, mobile users have lost millions of USD to mobile frauds [16]. Mobile fraud attempts grew 50% in 2018 and one common type of fraud is account takeover wherein fraudsters trick users into giving sensitive account details like PIN. Other techniques (or attacks) that fraudsters use include malware, fake mobile app, smishing, vishing, Man-In-The-Middle (MITM) attacks, SIM cloning, using Thin SIMs, and SMS spoofing [14, 21, 54].

Bowers et al. performed a comprehensive security analysis of emerging digital credit applications to identify security and privacy issues [12]. Phipps et al. showed the vulnerabilities in SIM cards by employing a mock attack using thin SIMs on SIM-based mobile money systems, which reliant on SMSes [54]. Although mobile fraud attacks happen online, they highlight how our online and offline worlds are interconnected. Offline trust such as trust in social institutions and individuals is coupled with online trust [44]. From a security point of view, physical and digital space are also interrelated [19], and it is this trust that fraudster exploit in their scams. Therefore, it is significant to study users' reactions offline to understand online threats. Information required to commit crimes such as phishing and identity theft usually comes from phone conversations with the victims (10.5%). This suggests that in identity theft and fraud incidents, information was given voluntarily by the victims and was provided during direct contact instead of online contact [68]. In our work, we focus on phishing attacks in Pakistan (smishing and vishing), and identify the social-engineering tactics utilized by the fraudsters.

4 METHODOLOGY

To examine the dynamics of mobile-based fraud in Pakistan, we conducted an IRB approved year-long study. We interviewed a total of 78 mobile users who had engaged with fraudulent calls or messages (including 71 fraud victims and 7 non-victims) in addition to 15 mobile money agents from urban, peri-urban, and rural areas of Punjab during 2019. We also conducted informal open-ended interviews with 3 officials from two different organizations: Pakistan Telecommunication Authority (PTA), which is the national regulatory agency for telecommunications in Pakistan [26]; and Federal Investigation Agency (FIA), which is the national intelligence agency responsible for undertaking operations against Federal crimes, cybercrimes, smuggling and terrorism [46].

4.1 Sampling and Recruitment

4.1.1 Interviews with Officials. We first reached out to the PTA and FIA officials to gain an understanding of the types and prevalence of various mobile-based frauds. Our motivation was to acquire reporting statistics on fraud types and their geographical distribution to guide our sampling. Interviews with officials were conducted by three authors and captured in the form of extensive

meeting notes. Due to the sensitive nature of their roles, interviews were not recorded. We also collected published Press Releases by FIA to support the information provided during interviews.

After meetings with officials, we conducted qualitative fieldwork to understand the differences in the types and execution of frauds, participants' experiences and reporting of frauds. We conducted semi-structured interviews with mobile phone users and mobile money agents (explained below). Interviews with users and agents were conducted by the authors and a group of undergraduate RAs; the undergraduate RAs were trained to conduct interviews (e.g., questioning and probing) and were provided with a formal interview guide in Urdu prepared by the first author. Interviews were conducted in Urdu or Punjabi, depending upon participants' preference, and were audio-recorded with participants' consent; recordings were transcribed in Roman Urdu. Participants were interviewed by researchers of the same gender to reduce the impact of gender, especially when communicating with female participants [50]. None of the participants were compensated.

4.1.2 Interviews with users. We recruited mobile phone users who had engaged with fraudsters (e.g., by responding to a phishing SMS or call), focusing our efforts on recruiting *victims*. To recruit participants, we inquired if they had been a victim of mobile fraud. All participants who replied affirmatively to being a fraud victim were recruited. During the semi-structured interviews, we discovered that some participants did not lose money. Even though they disengaged upon realizing that the interaction was fraudulent before incurring any monetary loss, they considered themselves victims merely by interacting with fraudsters. These interviews with non-victims provided unique perspectives about potential points of intervention and were thus included in our analysis.

We aimed for a diverse sample and recruited participants from different localities (urban, peri-urban, and rural), genders, age groups (18-25, 26-45, 46+) and education levels; with respect to age, our sample is representative of Pakistani population [49]. Participants were recruited from the districts of Lahore, Okara, and Gujranwala in Punjab. Due to the lack of literature on mobile frauds in Pakistan, we talked to participants who had experienced fraud at different points in time ranging between one month to 5 years.

We conducted in-depth semi-structured interviews to explore the dynamics and user motivations around these fraudulent interactions. We reached out to victims through someone in their close social circle because money is a sensitive topic especially when associated with a crime and people tend to be uncomfortable discussing it with strangers. Participants concealed being fraud victims for various reasons and only disclosed it in close circles (we discuss this further in Section 9). Keeping their experiences private was particularly prevalent among women and additional effort was required to find and recruit women participants. The social contacts helped develop participants' trust in researchers. At the end of every interview, we inquired if the participants knew any other victim of mobile fraud. Most victims did not know anyone else who was defrauded. Some victims shared their experiences in detail in the hopes that we will help them in recovering their lost amount. We clarified that we are researchers and could not help with recovering financial losses. It was a sensitive subject for participants, so we did not suspect any misreporting. We did not have access to calls, message logs or complaints filed (limited representation due to non-reporting by the majority as shown in findings) which could be used to validate participants' claims. We, therefore, relied on self-reporting.

4.1.3 Interviews with Mobile-Money Agents. We conducted semi-structured interviews with 15 mobile-money agents. Initially, the agents were unwilling to participate in interviews as they suspected the researchers to be from the taxation department. The undergraduate RAs used their university ID cards to establish an identity as students and gain the trust of mobile money agents. In peri-urban and rural localities, RAs sought help from local contacts, acquainted with the mobile money agents, to recruit them. Table 1 shows the demographic information of all participants.

Table 1. Victims, Non-victims and Agents Demographics.

	Victims		Non-victims		Agents	
	(n=71)	(%)	(n=7)	(%)	(n=15)	(%)
Male	52	73.2	4	57.1	15	100
Female	19	26.7	3	42.8	-	-
Age 18-25	42	59.1	4	57.1	5	33.3
Age 26-45	20	28.1	2	28.5	8	53.3
Age 46+	9	12.6	1	14.2	2	13.3
Less than High School	15	21.1	1	14.2	1	6.7
High School	21	29.5	2	28.5	4	26.7
College	35	49.2	4	57.1	10	66.6
Urban	56	78.8	4	57.1	12	16
Peri-urban	4	5.6	1	14.2	-	-
Rural	11	15.4	2	28.5	3	4

4.2 Interview Guides

We developed two different interview guides; one for users and another one for mobile money agents. We created a list of discussion points for officials.

Mobile phone Users (victims and non-victims). Mobile phone users were asked about their technology use, details about the fraud incident(s) beginning with the receiving of phishing call or SMS up to their last contact with the fraudster, factors that made them trust the fraudster, when and how did they realize that they were (or are being) defrauded, their reaction after that realization; and, finally, their attitude towards reporting fraud.

Mobile Money Agents. We asked mobile money agents about their day-to-day interactions with customers, behaviors and actions that raise suspicion of the customer being defrauded, customers' reactions towards agents' fraud warnings, and, the agents' information about and perception of effectiveness of fraud reporting procedures.

Regulatory Officials. The conversation topics included most common fraud types and population segments most affected by each type, extent of pre-planning in frauds, fraudsters' access to verified SIM cards, the sophistication of fraudsters, existence and availability of statistics on fraud complaints filed by victims. The interview data from officials was incorporated using in-vivo codes.

4.3 Data Analysis

All the interviews were analyzed, using inductive thematic analysis [13]. Two codebooks were developed, one for user (victim and non-victim) interviews and a second one for mobile money agent interviews. For each category, one author coded a few transcripts using inductive coding on NVivo. The resultant codebooks were discussed among the first two authors to add some new codes, sub-codes and rearrange data between codes. The finalized codebooks were used to complete the coding of data. The coded data were analyzed by three authors.

4.4 Limitations

Although we report the mobile-based frauds in Pakistan from a few months to a few years preceding 2019, the fraud mechanisms and schemes might have evolved since then. The respondents were

recruited through social contacts in the field that could pose self-selection bias as only those willing to discuss mobile-based fraud incidents participated in the study. The data collected is based on retrospective questioning and dependent upon the participants' ability to recall incidents accurately. It could suffer from recall bias and self-serving distortions in memories. Similarly, the data can be impacted by social desirability bias, as the participants could report instances to show innocence or hide their lapse in judgment. We report the incidences as reported by the participants and did not try to validate or authenticate the factual or technological feasibility of these attacks and claims.

4.5 Positionality and Reflexivity

The first four authors are born and raised in Pakistan. After receiving their undergraduate engineering degrees from Pakistan, the first three authors worked as ICTD and HCI researchers for multiple years. The authors, their friends and families have received numerous fraudulent messages and phone calls over years. Besides hearing stories of individuals losing money to fraudsters, two authors also interacted with fraudsters over call to determine nature of interaction with the victims and information sought. Fraudsters wanted the authors to share Whatsapp One-Time-Pin (OTP) and bank account information. The authors have also witnessed fraud schemes evolving from one cash transfer scheme name (BISP) to another (EHSAAS) over a decade. The motivation for this project, therefore, comes from personal knowledge of the problem and desire to contribute towards the understanding and solution of a problem that has gotten worse over the years.

5 FINDINGS: PARTICIPANTS' UNDERSTANDING OF FRAUD

We first present (in this Section) participants' mental models of fraud and types of frauds faced by them. In Section 6, we describe, using a social-engineering attack framework, the strategies fraudsters used to target our participants. In Section 7, we discuss the roles different actors play in the context of mobile frauds. Finally, in Sections 8 and 9, we share participants' attitudes towards mobile fraud and changes in their behavior upon witnessing or falling victim to mobile fraud.

5.1 Participants' Mental Models of Fraud

Before inquiring users and agents about their experience and interactions with fraudsters, we ascertained their understanding of mobile frauds. We asked them *"what constitutes a mobile fraud in your opinion?"* All users and agents associated mobile fraud with "stealing money". When probed further *"who are the fraudsters?"* and *"how do they carry out the fraud?"*, they described fraudsters as *prank callers*, *cybercriminals*, and *hackers* who can easily "get into their phone and take money out." Victims who reported fraudsters having prior information about them were asked from where did they think the fraudsters got their information. Victims had varying suspicions including data leak from NADRA (Pakistan's National Database and Registration Authority) but weren't clear about the mechanics, or an employee at their service provider (bank or telco) colluding with the fraudsters. Some suspected that the fraudsters got their information from the victim's social contacts who had ill intentions towards the victim and were aware of their details including the fact that their parents or husband were away from home leaving the victim vulnerable. Some victims believed that fraudsters randomly dialed numbers because, in their interactions with the fraudsters, the fraudsters did not have any information about them. Some respondents referred to friends and YouTube videos for answers which suggested the fraudsters to be hackers using software to steal people's information. One victim suspected that fraudsters got her information from the voucher she had filled at a mall to participate in a lucky draw. Another victim believed it might have been leaked through the social media apps she used.

Commenting on fraudsters' sophistication, the officials shared that it varied with some of them being highly organized while others being unsophisticated and just trying to make hay while the

sun shines (referred to as copycats). As per arrests made by FIA officials, fraudsters operate as individuals (a hawker making fraudulent calls) as well as in gangs (an elaborate and organized setup for making illegal VOIP and fraudulent phone calls). According to the PTA, once a victim responds to one of these fraudsters, they share the victim's contact information with other members of the gang and continue defrauding them. Multiple members of the gang pretend to be members of an organization passing calls from one member to another.

Among our participants, we found that men elaborated more than women on the topic of mobile fraud, sharing their own experiences as well as those of others in their social circle. For example, a male participant (Victim 61) shared: "*One type of fraud is the one which happens over messages that say 'You are getting money under this scheme'... there are frauds on calls too. Other than that, there is one bank-related fraud prevalent these days about which I have heard from one or two people that they have received calls.*" On the other hand, women, especially low-literate women, shared only their own experiences of fraud. A female participant (Victim 12) said: " *Yes there are many different types of frauds. I can only think of the one (type) that happened to me – through mobile – [the kind of fraud] that people do these days mostly.*" These differences reflect the inequity in access to information for women [33].

5.2 Types of Frauds Reported by Participants

Participants reported four main types of mobile fraud: lucky draw, BISP fraud [2], bank fraud, and damsel in distress. Parenthesis indicate the number of participants that were victims of these frauds.

Lucky Draw (n=39; 55%). In this type of fraud, fraudsters text or call their targets congratulating them on winning a prize (usually a car, jewelry, or cash). After convincing them of the prize, fraudsters coerce them to share their bank account number (so that the prize money can be sent) or to pay a processing fee (necessary to receive the prize). The fraudsters pretend to represent a telecommunication company or a popular game show that is known to give lucky draw awards.

This fraud was reported by participants of varying income, education, and literacy levels, suggesting that a broad demographics is targeted. Officials reported that victims of lucky draw frauds ranged across socioeconomic segments with rich and poor equally falling victim to them.

BISP Fraud (n=6; 9%). In this fraud, fraudsters send text messages similar to the ones sent by the Government of Pakistan to individuals eligible for the Benazir Income Support Program (BISP). Figure 1 shows a sample BISP message sent by the government and a sample BISP fraud message. BISP is aimed towards low-income families; thus BISP fraud targets low-literate low-income groups.

As per officials, most of the BISP frauds were reported by victims from lower socio-economic segments. In our sample, four (out of the six) victims of BISP fraud had education less than or equal to high school. BISP fraud victims reported calling the number in the fraudulent SMS in the hopes that they got qualified for the BISP program and would receive financial assistance.

Bank Fraud (n=9; 13%). In this type of fraud, fraudsters impersonate bank officials, military, or other government personnel and trick or coerce victims into sharing their banking credentials, used by fraudsters to steal money. Bank fraud victims reported that the fraudster tricked them into sharing information over the brief interaction of *one* phone call. Reflecting on why they fell for the scam, some of these victims said that they were unable to reflect on the situation and adopt a more thoughtful course of action in such short duration. Creating urgency to impair victim's decision making is a common strategy among fraudsters [70]

[2]BISP is an unconditional cash transfer program for reducing poverty and is disbursed to eligible families below the poverty line based on a poverty scorecard formed after a national survey each year. https://bisp.gov.pk

Damsel in Distress (n=5; 7%). In this fraud type, fraudsters pose as a girl in need of help (e.g. stuck at the hospital and out of money) and ask for money as support promising to payback. This fraud is generally targeted towards men. In our data, all five victims to this fraud were men.

The above four types of fraud were the most prevalent in our sample. However, participants also reported becoming victims to other scams, such as pyramid schemes, investment scams, and blackmailing and coercion through impersonation of law enforcement officers.

6 FINDINGS: REPORTED MOBILE FRAUD STRATEGIES IN PAKISTAN

Mobile fraud, like any other social engineering attack, typically follows four phases: *planning*, *engaging with victims*, *attacking*, and *ending the attack*. Although the general attack pattern may be the same, depending on the context, attackers use different mechanisms and strategies, and knowing these is important to develop appropriate context-specific defenses. We present the strategies fraudsters used to scam participants in our study.

6.1 Phase 1: Planning and Gathering Resources

We found that fraudsters used three main strategies to appear legitimate to their victims.

Masking phone number. Soliciting calls and messages from an unidentified number are likely to arouse suspicion or get ignored. To make fraud calls and messages look legitimate, fraudsters trick victims into saving a phone number as a contact on their phone, so that future calls or messages from that phone number would appear legitimate. One lucky-draw victim reported that they were tricked by a fraudster into saving a number as a 3-digit telco shortcode, which looks like a legitimate 3-digit shortcode that Telecom operators typically use. The victim shared their experience:

> " *...the call was from a regular mobile number, not a shortcode. They sounded like typical telco operators and said that 'You have won a prize and you have to follow my instructions to get this prize'. First, they asked what is your mobile model so we told them our mobile model. Then one of them asked us to press some buttons two or three times on our phone. I don't clearly remember what were those buttons now but they told us by doing so you will forward a number to us. We followed their instructions and what we eventually ended up doing was saving their number as short code 333, they also told us not to disconnect call. We figured out these things after being scammed.*" (Victim 16)

Obtaining difficult-to-trace SIM cards. Pakistani regulations require every SIM Card to be verified against the National Database and Registration Authority (NADRA) using Biometric Verification System (BVS) machines. More than 90% of the Pakistani adult population have NADRA issued CNICs [64]. FIA official reported that the SIMs used by fraudsters are verified but fraudulently. They said *"Fraudsters scam low-income and low-literate individuals in rural parts of Pakistan to give thumb impressions on the BVS machines in exchange of a few hundred rupees"*. Due to low-literacy, these men and women are unaware of the ramifications of providing their thumb impressions such as the use of these SIMs in illegal activities. They believed that the penetration of BVS machines to small stores and franchises across the country by telecom operators (to increase subscriptions) was being exploited by fraudsters. They claimed that *"customers visiting to buy SIM cards are misled into providing fingerprints multiple times, under the false pretense of network unavailability and having to retry the fingerprint registration process. But instead, they secretly verify another SIM card that is hidden from the customer."* A press release from FIA validated these responses by FIA officials [18]. Although PTA warns customers against such schemes [7] and provides a service for subscribers to check for SIMs associated with their identities, the defrauded low-income and low-literate users from rural areas who don't have a mobile phone might never consider using such a service.

6.2 Phase 2: Engaging With Victims

After establishing initial contact with the victim, fraudsters employ various tactics to establish their legitimacy or authority with the victims and gain their trust, which they exploit later to make the victims comply with their instructions. Here we explain the hooks they used to engage victims.

Using designated number and leveraging personal information. In some instances, victims mentioned receiving a text or call from either a bank helpline number or telco shortcode. For bank fraud, most participants reported that they believed the scammer was a bank representative because they had information about victim (e.g., name, identity card number) and called from a helpline number. Exploiting that trust, scammers asked victims for their debit card number or ATM PIN.

> "*... I received a call from XYZ bank's helpline, and it sounded like it was a representative. They knew my name and repeated some basic information about me. They said "Our link is down, so we are facing some issues with the ATMs. Kindly share your account number and PIN so that you don't face any issue." I gave them the information because their helpline number was showing so I did not suspect anything.*" (Victim 2)

Another victim shared that the scammer had detailed information about his phone usage.

> "*Once I got a call and they told me that I have won a PKR 30,000 lottery type. At first, I did not believe it then the person told me all my details ...Information like this SIM is on my name, my ID card number, and all other SIMs on my name and what are my activities [on the phone]. So that is why I was sure [they were trustworthy].*" (Victim 4)

Participants mentioned that they believed the scammer because of fraudsters' professional manner like a banker or government official speaking in English. People's trust in banking organizations and their employees is established through in-person (offline) interactions, and scammers exploit victim's offline trust by impersonating bank employees.

Portraying authority. Respondents reported fraudsters impersonating military officials and central bank officials claiming to run a verification process for bank accounts in connection with the latest census in Pakistan which was carried out in assistance with the Pakistan Army [71]. Fraudsters use their supposed authority to threaten victims of the consequences like the closure of bank accounts in case of non-compliance to their instructions. One participant shared:

> "*Some soldiers came for census. So I got a call from them that they wanted to confirm some data. They asked my mother's name and address and it seemed like they are military officers or government officers. After this, the call ended. After two hours I got another call and asked me which banks do you have accounts at. We need data to confirm because a lot of frauds are happening these days. At first, I got afraid. But from their voice, it seemed like they are government officials. They were speaking English too. Then I told them my account number and they ended the call.*" (Victim 41)

In three instances of lucky draw frauds where the scammer is trying to prove association with a telecom operator, they asked victims to share serial number written on the back of their SIM to receive a prize or told the victim the number on the back of their SIM [3] and asked the victim to confirm it. Since the first few digits of this number are public knowledge and easy to predict, a fact unknown to victims, fraudsters exploited it to prove association with the telecom company. We hypothesize that the fraudster already had information about the victim. One respondent

[3] The number printed on the back of a SIM card is the Integrated Circuit Card Identifier (ICCID) number and is unique for every SIM (Subscriber Identity Module) card internationally. Its length is between 19 to 22 characters. The first two digits refer to the industry code, the next two digits refer to the country code and the next two digits refer to the telecom operator code. The first four digits are, therefore, common across all SIM cards used in the telecom industry and publicly known. The next two digits, although unique to every telecom service provider, are also public knowledge.

mentioned, "*I received a call in which I was told that they are calling on behalf of Zong (telecom). When I did not believe them they said "Your SIM has a 3-digit code on the backside. Send that to us". When I sent them the code, they told me all my information after which I started believing what they were saying.* " (Victim 43)

Participants also reported fraudsters impersonating call center employees and replicating call center interactions by e.g. pretending to transfer calls among call center employees and playing on-hold music. Participants claimed these tactics were convincing and made them trust the fraudster.

Being persistent. We found incidents of young, educated, banked women initially resisting sharing of information with the fraudsters who then coerce them by repeated calls and insist that they share the information.

> "*When they started asking for my personal information, my e-banking account like which email address do I have set as user name, something like that, I disconnected the call. I would end a call and get another, one after the other, They were, without a pause, continuous. I got 3 calls from the bank because I was not sharing information.*" (Victim 71)

Victims reported that the fraudsters often do not let them disconnect until they have transferred money to maintain their control over victims' reactions and to prevent them getting a warning from an intermediary or agent. One victim shared their interaction:

> "*They said you have won 3.5 Tola gold (37.5 grams). After that they said 'Do not disconnect our call. Stay on the line with us'. I said "OK". This time when I disconnected the call, they would call me back immediately...They told gave me two CNIC numbers to send 7000 rupees on each [using OTC]. [They told me] 'Do not send 14000 rupees on one. Instead send 7000 rupees on each.*" (Victim 18)

Increasing incentive. In three incidents, fraudsters were successful in baiting a participant by increasing the promised amount, utilizing weakness in human psychology – increase in incentive deteriorates judgement and hence decision making ability [22]. Relative importance of promised amount varies depending on the socioeconomic status of the targeted individual. One participant recounted his lapse in judgment as:

> "*Initially when I started getting the messages, I asked my mother if she had registered [for BISP]. She said that she has not registered anywhere. I have a friend who has a mobile shop. He told me that this is fraud and do not fall for it. The first message I got said that I could receive PKR 32,000. During the first month, I ignored it. But next month, I got another message that said that I was due to receive PKR 64,000 from Benazir Income Support Program. So then I started trusting that I was really due to receive money as they had doubled this month. I got greedy.*" (Victim 59)

6.3 Phase 3: Stealing Money

After fraudsters collect resources to attack victims (Section 6.1) and deploy tactics to seek victims' compliance and establish legitimacy (Section 6.2), they execute their attack to steal money.

Through over-the-counter (OTC). We found that fraudsters leveraged the loopholes in social norms around the interactions and OTC transactions at mobile money agents' shops. Several victims reported that fraudsters convinced them to visit agents and to send them money. The typical amount they sent through OTC was higher compared to mobile top-ups (discussed below). Agents explained that fraud through OTC was frequent in areas with low mobile wallet penetration.

Based on fraud instances reported by victims, we identified how fraudsters execute this phase: Fraudsters tell the victim that they have won a prize but discourage them from disclosing this information to their local mobile money agent. Instead, the victim is instructed to hand over the

phone to the agent. (Handing over phone calls to agents by low-literate users is common in contexts where the caller wants to explain the transaction which might be complex for low-literate users to explain or understand themselves; the agent makes note of what is required and return the phones.) To avoid suspicion, the fraudster lies to the agent that they are related to the victim, and they explain that customer (victim) will give cash and that amount is to be deposited into their (fraudster's) accounts. The agent deposits the money in the account using his mobile money account float and asks the customer for money. The customer, then, discloses that they weren't there to pay but rather to collect money that they had won. Sometimes the customer accepts responsibility and pays the agent; sometimes they don't and the agent (like Agent 14) loses money.

> "*They were a man and a woman, they parked their motorbike here and asked us to deposit PKR 36,000. My brother asked them about the receiver's name, phone number and the man confirmed that the receiver was his brother. After sending money when we asked for PKR 36,000 cash payment, they said that they were about to receive PKR 80,0000 and also showed us a text message 'Benazir income support'. I saw the message and told them this message is fraudulent. The man said 'I did not tell you to send money'. [Then] I called One-Five [police helpline], police came, people gathered here at my shop. Police said to us 'Why did you send money before taking cash, first take cash then send money' and our PKR 36,000 was never recovered.* " (Agent 14)

Through mobile top-up. Besides OTC, fraudsters also ask victims to send serial numbers of mobile top-up cards. Three victims reported that fraudsters asked them to burn the scratch cards afterward and that fraudsters could see their movements. When we probed if the fraudster told them they could see their movements, all three victims said that the fraudster did not explicitly say it, but they all felt (based on how the fraudster was speaking) that they were being monitored.

It is important to distinguish top-ups from larger value frauds as they are more prevalent in rural areas where cards are bought from corner shops. In one instance, a shopkeeper in a rural area after exhausting his shop's scratch cards, accompanied the victim to another shop to get more cards. The shop ran out of the cards because the amount demanded by the fraudster was larger than the typical demand for top-up cards and the victim ended up buying all available cards. However, this abnormal demand did not raise suspicion with the shopkeeper. We hypothesize that, unlike mobile money shops, small shops have less experience in the identification of such fraud victims and do not have any financial risks, (mobile money agents use float to conduct these transactions). Therefore, rather than warning customers, these shops sometimes facilitate victims.

From bank account. In bank frauds, fraudsters target ATM PINs, mobile banking usernames and OTPs, debit card numbers, etc. The aim is to eventually take control of and empty the victims' mobile banking accounts. The amounts lost in bank frauds are generally higher than other frauds except when victim's account balance is low. Educated banked victims initially try to resist the fraudsters who then coerce them into sharing ATM or mobile banking PIN Codes, login or last 4 digits of the Debit/ATM card etc. But sometimes victims underestimate information's sensitivity and share it like Victim 7 who refused to share the ATM PIN but shared the last four digits of the ATM card number and lost money.

> "*They were asking for ATM PIN. I said 'I won't share it'. They said 'Ok then, share the last four digits of your account number'. I told them. After some time, I received a message from the bank about PKR 11,000 transactions from my account.I called my bank immediately. They said 11,000 has been debited from your account.* " (Victim 7)

Tactic: Adjusting demands based on customer profile. Sometimes victims informed the fraudsters about the shortage of amount in hand and in turn, fraudsters adjusted their demand to get

hold of whatever the victim had. One victim explained this adjustment conversation as "*So there wasn't as much money at home [as demanded by fraudster] so I told them the truth that I do not have PKR 50,000. They said 'Fine, you can pay whatever you have'.* " (Victim 12)

Tactic: Demanding money in installments. Victims reported that fraudsters asked for repeated payments in lieu of various fees such as shipment charges, duty to be paid at the port, etc. Agents and victims both reported that the victims conduct multiple transactions and are instructed by fraudsters to send money from a different shop every time to avoid suspicion, identification, and warning. The agents shared that with the increase in OTC transaction limits, the fraudster can steal more money in fewer transactions, exploiting improvements in the ecosystem. One participant shared sending PKR 13,000 through OTC in various transactions.

> "*[We sent] PKR 13,000 in portions... I think first we sent PKR 2000 through Easypaisa, then PKR 5000 and PKR 6,000. We did not feel good about it [getting defrauded] at that time either but later we both regretted it and also laughed at how we were tricked by someone into sending them PKR 13,000. It was not just our money but also money at home, we sent those. We even borrowed money from our neighbor to complete 13,000 and we sent that money through Easypaisa too.*" (Victim 16)

6.4 Phase 4: Ending Attack and Realization by the Victims

In this section, we report how fraudsters cease communication without creating suspicion. We also explain the triggers and information sources that lead the victims' realization about fraud.

Ending attack: Delaying realization. Fraudsters avoid suspicion by mentioning processes *"We are creating lists"* and timelines *"It will be there by morning"* to delay the victim's reaction. Meanwhile, fraudsters switch off their phones, use received scratch card numbers, or remove traces by cashing out the money from OTC which ends the trail. One participant recounted the interaction prolonging their wait for the prize.

> "*They said we are almost there [at your house]. We thought it would take them an hour or two hours maximum. We kept waiting and when it was almost midnight we thought time is over and concluded that it was nothing but a fraud. Then we thought that maybe they will reach our house in the morning. We kept waiting till morning. The next day went by and nothing happened.*" (Victim 14)

Each fraud type prompts different responses and different stages of realization. The most common realization stage was when the scammer's phone number was turned off. However, in some instances, a social contact or a mobile money agent had to intervene and confirm that the victim had been defrauded. We detail such ways of realizations and reactions below.

Ending attack: Ceasing communication. In lucky draw frauds, after the transactions, scammers tell victims to wait a few days for their prize to be delivered to their homes. After the specified time elapses, victims reach out to scammer's by then unresponsive phone numbers. That is when victims realize that they have been defrauded. Unresponsiveness of scammers' mobile phones is the most common realization point for victims. One victim waited for a whole day for the fraudsters to deliver her prize car as they had told her that they were hours away. "*So they disconnected the call after that. I called them again but their number was off. The number stayed off after that.*" (Victim 18)

Realization: After failed attempts to reach the fraudster. Another point of realization is when participants call fraudster's number and hear a pre-recorded audio. One participant shared,

> "*When I called the number was off. Then after a month, I called the number mentioned in the message. Then I figured that it was a recording [on the other end]. Nobody is actually talking to us. But it seems almost as if someone is talking to you. One almost believes it if*

he is like us. When I am quiet, he is speaking. It seems almost as if I am talking to him but they are clever people. They give proper replies. But I was quiet and they were replying. Then I checked with some people around. One or two of them had also faced this. Then I figured that it is a fraud. I had topped up for PKR 500." (Victim 8)

Realization: On follow-up demands for more money. In some instances victims realize that the caller is a fraudster due to the continued insistence on money, and thus do not share anything. "As soon as I gave him [topup card serial] numbers, I said 'Where is my prize?'. He replied 'Brother, we asked for cards worth 500 rupees not 300. Then I felt like he was taking me for a ride. And then I said goodbye to him and ended [the communication]." (Victim 31)

Realization: After notification from their bank. In the case of bank frauds, the fraudsters called from the bank's helpline [4] or short-codes and/or had basic information, therefore, the victims did not suspect anything until very late. Once the victim received a message from their bank regarding transactions that they had not conducted, they would call their bank to check what had happened. The bank representative would then explain to them that the bank does not conduct any such verification asking for a customer's PIN and that they had been defrauded.

One victim immediately realized her mistake of sharing PIN and called her bank asking them to stop the transactions. She called the bank branch instead of helpline to seek help. Since someone was already asking her to share information over the helpline, which evaded her trust in the helpline. Others victims who realized late would close their accounts: "I closed my account so that no further transactions take place because I had shared my PIN." (Victim 2)

Some victims even confronted the bank officials regarding the use of bank helpline for calls "*And when I went to the bank, I showed them my mobile screen and said "This is your (bank's) number, right?" They said that "Yeah, the number is ours". I said "If your number is so easily showing how can anyone be sure (of anything). Anybody would think that this is the bank's number". "* (Victim 71)

Although most respondents learned from their experiences and grew skeptical of further fraudulent messages with some even deleting them, the same was not true for all participants. One participant, belonging to a rural community and having education till 5th grade, was unable to extrapolate the warning to a previously unknown fraudulent scheme. She repeatedly engaged with the fraudsters despite being warned by her social circle about frauds of particular types but was saved from becoming a victim by intervening agents, colleagues and neighbour.

7 FINDINGS: ROLE OF DIFFERENT ACTORS

In this section, we describe the various direct interactions victims have with mobile money agents and people in their social circle (e.g., family, friends, colleagues) and the roles these actors play in mobile fraud.

7.1 Agents

Agents as predictors of unusual customer behavior. Agents have information about transaction and top-up patterns of regular customers, and can thus identify abnormalities in customer behavior. Upon suspicion, they can warn customers against transferring money to fraudsters. We inquired from agents about the daily footfall in their shops and the proportion of regular customers. All agents reported that majority of their customers are men and they recognized more than 50% of their customers. For frequent customers, agents rely on customers' transaction behavior and history to identify peculiarities in transactions and identify frauds. Agents know customers' routine top-up amounts, connection types (prepaid, post-paid) and mobile money networks used to send money

[4] Victims reported receiving calls from banks' helplines. While we can hypothesize rogue actors or spoof etc, we report our analysis as described by the participants.

to customers' friends and family. At times, agents suspect that the customers are sending money to fraudsters but are uncertain. If they feel that the customer is being defrauded, then they warn them against sharing their top-up card number as their money will be lost. But because fraudsters forbid the customers from sharing any information with the mobile money agent, the customers hide the identity of the actual recipient. With familiar customers, agents inquire about the sudden need for a higher than usual top-up amount and warn them against fraudulent prize schemes.

Victims' Reaction towards Agent Warnings. Agents reported that customers have varied reactions towards the agent's warnings. To discourage fraud, agents refuse to conduct any suspicious transactions. Agents say that when large amounts are promised by the fraudsters, attempts to stop customers are useless as the customers strongly believe in fraudsters' promise. Customers keep sending money hoping that this might be the last transaction and they may finally get the money fraudster is promising. The victims are instructed to go to different shops for each transaction so that the mobile money agent may not recognize the fraud and intervene. Agents familiar with most of their customers reported that the customers listened to their warning and did not send money. It indicates that the trust between customers and the agents serves positively to protect customers. This is why fraudsters insist that customers do not go to the same shop to conduct multiple transactions. One shopkeeper explained this dynamic "*Those who are acquainted with you, they trust you. But those who are not, you can warn them and they can decide on what they want to do.* " (Agent 4)

Another agent shared his experience about warning customers: "*People don't stop [sending money], they leave my shop and go to other shops [if I stop them from sending money]. They have to send money at any cost.*" (Agent 16)

One victim shared that an agent warned her against sending money but she sent it anyway in the hopes of receiving a much larger amount in return.

> "*Then I went to the mobile agent shop and I asked him to conduct a transaction. Then he [agent] warned me that if I am doing it [for a prize] then it is wrong. It could be a fraud. To which I replied that it's ok. Please conduct the transaction. [I thought to myself that] I have savings, so what if I send PKR 14,000. I will get a lot more in return too.*" (Victim 18)

7.2 Family and Friends

Participants refer to friends, family members, and colleagues to make sense of the fraudulent communication or simply share what they consider as the exciting news of winning a prize. Sometimes these confidants are equally unaware of scams and tend to participate in the compliance process by accompanying, supporting, and encouraging the victim in the money transfer process. At other times, they warn the participants about the fraud and protect them from falling prey.

Enablers in Scam Compliance. Both agents and victims reported that victims sometimes travel to the mobile money agent's shop in pairs to conduct transactions indicating the inability of those close to the victims to recognize frauds. One agent reported about a couple asking him to send money in the hopes of a prize. The agent warned that they should not send money, but they still insisted on sending the money. They later returned and asked if the transaction can be reversed.

Multiple women reported accompanying other women to the market for buying top-up cards or buying the cards for them or lending money for sending to fraudsters. One woman shared how she agreed to help her colleague in sending money to fraudster.

> " *Fraud happened with my colleague once. She said "Sister, I have got this [message] that I have won PKR 5 lac prize. I have to send PKR 3000 then the process will be completed." I replied, "So what do you want to do?" She said, "We have to send them 3000 rupees mobile load [credit]." I said "OK. I am with you ... I will support you [in getting it]". She said, "Can*

you please send them the mobile top-up? It is not available here in the village." I called a boy and told him to bring his bike. During recess, he took me to the shop where mobile top-up was available. When I came back, I brought top-up cards worth PKR 1000. They only had this many available. She kept sending the balance to them." (Non-Victim 6)

Another participant consulted a neighbor about a fraudulent message and was encouraged to reply. "*At first I could not understand it. I could neither read it properly nor could I believe it. A brother lived near my house. I told him and he congratulated me that I give it a try. Then I called them [the fraudsters].*" (Victim 51)

Limiters in Scam Compliance. Participants who were saved from falling for a scam or replying to a fraudulent communication, had mostly referred to a colleague, a shopkeeper or someone with higher literacy than the participant. One woman recalled receiving a call that she has won a prize and she can visit a certain location to collect the prize. She and her uneducated sister-in-law decided to consult a university student who saved them from being defrauded by warning them against it.

"*Once I got a call that this is so and so speaking. You have won a prize of 5 lac rupees and gold through your (mobile) number. My sister-in-law and I then thought that we had won without making any effort and decided to collect the prize. My sister-in-law is not educated. They told us to collect the prize from so and so location. We left home. On our way, it crossed our mind that it might be a scam and what if we get defrauded. There was a girl sitting who looked like she was a university student. We talked to her and told her that this is what happened. She replied "Aunty, please do not mind but you should not do this. These days there are a lot of scams happening. You might run into some sort of trouble." So we came back.*" (Non-Victim 1)

Another woman was warned by her colleagues about a BISP message being fraudulent.

"*I got a message from Benazir Income Support. It was from 25 to 30 thousand rupees. I was very happy that I will get the money. I did not think about how or why I got it or what will happen next. I discussed it with my colleagues the next morning that neither am I a widow nor do I qualify for it then how could this happen? These people are asking me to collect the money and contact on this number. Everyone said 'Sister, do not do this. This is a scam. This has become very common. They defraud people out of money. They cheat them. We are clueless as to what should be done. This is a high-tech time and these are high-tech frauds.' Then I forgot about it. I thought 4 to 5 women can't be wrong.*" (Non-Victim 6)

Participants reported borrowing money to send to fraudsters and the lender warning them.

"*They told me to send money through Easypaisa. I only had PKR 5000. I thought let's borrow 3000 from a friend & send it. I said to a friend "Your brother has won a prize. I need 3000." My friend said "Are you crazy? There are no prizes like this." [Then what did you do?] I confirmed with two or three more people who also said it's a fraud.*" (Non-Victim 7)

8 FINDINGS: REPERCUSSIONS OF FRAUD

Our findings show that the negative repercussions of frauds are not limited to the direct victims or the duration of the fraud. These fraudulent interactions impact the perceptions of victims towards services in the long run, result in financial losses for agents and create potential threats for CNIC holders whose SIMs are illegally used by the fraudsters. We discuss these below.

8.1 On Victims

We observed two types of behavior change among victims.

Avoidance. Some victims reported ignoring all doubtful communication. Unable to differentiate fraudulent messages from service messages, some participants reported deleting messages they receive from their service providers. "*Now we do not trust [these messages] anymore (laughs). These messages you get from Zong... we have lost trust in them because these are fraud and nothing else. Now even if we see the text or even if we get a call, we disconnect it and delete the message.*" (Victim 14)

Loss of trust in services. Others shared how they had lost trust in their telecom, mobile money operator, or bank through which fraud occurred and avoided using the service altogether out of the fear of losing more money. "*I have started fearing using the bank to the extent that I hardly transfer money even though I have my account. I do not trust it anymore. I feel like something will go wrong because a small transaction and a small mistake led to so much.* " (Victim 71)

One victim created a mobile money account but avoided cashing in any funds into wallet or installing the wallet application out of fear of being hacked and losing his money.

> "*I have opened an Easypaisa account but have not installed an app. I have Telenor. I had put two or three thousand rupees (in my wallet) but later took them out because (I was afraid) it might be a duplicate app and turn out to be fake. Because I have been defrauded so now I have lost trust. And I feel like if I will put money (in my wallet) I am afraid that someone might hack it and take my money.*" (Victim 24)

8.2 On Agents

Agents are the indirect victims of these scams as they suffer financial losses when the customer refuses to pay for the transaction or their shops are sealed out of vengeance misdirected at them as the victims cannot get hold of the fraudsters. One agent shared an incident where a customer asked him to transfer money to an account. Upon realizing that he has been defrauded, the customer consulted his employer, a government officer. The employer told the customer that the agent had defrauded him. Using his clout, the government officer had the agent's shop sealed by a magistrate.

Agents were apprehensive of complying with instructions received on phone. One agent shared that he refuses to talk to anyone on the customer's phone because fraudsters often mislead customers that their prize can be received through a mobile money agent's shop and ask customers to give their phones to agents to let them (fraudsters) explain the process of receiving the prize to the agent. The fraudsters also warn customers of fabricated taxes associated with prizes and convince customers to lie to the mobile money agents that the call is from a relative to avoid such tax deductions. Also, low literate customers do not understand the term 'Deposit' and the fraudster fools them into thinking it means they will receive money.

> "*Some people come to us and say 'Please Deposit'. They [customers] being illiterate don't know the meaning of deposit and withdrawal. They say 'I want to deposit' and make us talk on the phone with someone. After depositing when we ask for cash they say 'We are here to receive [money]', then they have to give cash to us.*" (Agent 15)

8.3 On Bystanders

As reported by FIA officials, the SIM cards used for mobile frauds are verified fraudulently and cannot be traced back to the fraudsters. Since the customers are unaware of this fact, some victims reported finding out about the CNIC associated with the SIMs used to make fraudulent phone calls. They learned about the identification details of the apparent fraudsters including their home addresses in an attempt to seek vengeance. Ability of an average customer to find out the identity and address of a SIM owner is a breach of customers' privacy. This privacy breach also poses a potential physical threat to the CNIC holder as the victim wrongly considers that the fraud has been perpetrated by them and might take any action they think is suitable for vengeance. However, in

most cases, the amounts are small and do not warrant a visit to another city. FIA officials reported that in their investigations, the phone number is first traced to the associated verified CNIC and then last active location which reveals the existence of drastic distances between the addresses of the CNIC holders and location of SIM activity pointing to a fraudulent use.

9 FINDINGS: TRENDS AND ATTITUDES TOWARDS (NON) REPORTING

According to the PTA officials, no database is maintained for complaints besides a list of mobile phones blocked as a result of customer complaints. One official commented: *"Even if such a database existed, access to it could not have been granted due to the Consumer Protection Laws"*. Reports from FIA grouped social media harassment, financial frauds, and other crimes into a single category, *cybercrime*, and did not yield any insights into the demographic or geographic profile of the most affected segments.

We, therefore, studied the attitudes and perception of fraud victims towards reporting and found various issues related to information and understanding about reporting mechanisms, hesitation in reporting driven by socio-cultural reasons, and expectations after reporting.

9.1 Lack of Awareness about Relevant Authority for Reporting

The most commonly cited challenge in reporting frauds in Pakistan was lack of information about the relevant authority and mechanism for reporting among phone subscribers. In Pakistan, financial frauds carried out over the phone and SMS have to be reported to the Pakistan Telecommunication Authority (PTA), regulator of telecommunication industry, which then refers these cases to the Federal Investigation Agency's (FIA) National Response Center for Cyber Crime (NR3C). The NR3C has the national jurisdiction to track and catch criminals involved in carrying out crimes over ICTs (among other things). PTA has designated helpline numbers and email addresses where users can call and report about any fraudulent calls and SMS. During our qualitative exploration, we found that 35 (29 men and 6 women) out of the 72 victims (49%) did not report frauds at all. Only 16 (22%) victims, 11 men and 5 women all belonging to urban areas, reported the frauds to their telecom operators, their banks, police stations, and the FIA. Majority of the victims, whether they had reported a fraud or not, were unaware of PTA's existence making the lack of knowledge of reporting to PTA a peripheral issue.

9.2 Reasons for Not Reporting Frauds

Participants cited many reasons for not reporting frauds. These include:

Hassle in reporting. In most cases, the victims turned to police stations where they were asked by police officials for bribes "to go and catch the criminals from other cities." This led victims to do a cost-benefit analysis and a general trend towards not reporting incidents involving financial losses below a certain value, typically PKR 5000. This leads to high under reporting of mobile-based financial frauds and results in a lack of estimation of the scale of such frauds and the collective financial losses caused by them. "*Who reports a fraud of PKR. 2500? There is no need to report. It is not a big amount. PKR. 2500 is the bribe police asks for [laughs].*" (Victim 1)

Unsatisfactory outcomes of reporting. Victims expect that after reporting a fraud, the money they lost will be recovered. As per our conversation with the FIA officials, frauds are carried out by criminals operating in gangs and the likelihood of recovery of money is very low. A misalignment of expectations and the actual outcome leads to lack of reporting by the victims. One participant shared his reason: "*[I:Why didn't you report it?] Firstly, the amount was very small, only 3000 [rupees]. Secondly, if I had this surety that I will get some good outcome by visiting the police station then I would have reported it. But you know our [police] stations' situation. I felt like I will be wasting my*

time so I did not report it." (Victim 2) Thus, FIA officials urged that users need to (a) understand the low likelihood of recovery of funds and risk involved when making dubious transactions; and (b) consider reporting as a means to prevent future crimes and more people falling victims to frauds.

Someone else as the SIM Owner. As mentioned earlier, Pakistan mandates SIM verification using biometrics. However, previous research [32] has noted that many times the phone users are not the SIM owners. Thus, when victims faced mobile-based financial fraud, and the SIM was not registered on their name, they assumed that they cannot report the fraud. "*The one who has the number [registered] on his name, only he can go and ask for an action against this. I did not have a CNIC back then. The number was on my father's name.*" (Victim 15)

Lack of evidence of fraud or Feeling responsible for Fraud. Many victims believed that falling for fraud was their own fault and therefore there was nothing to report. Some victims cited lack of evidence as a reason for not reporting. One victim of voice phishing said that he did not have a proof as everything happened over a call so he did not report. Another victim was of the opinion that it was her own fault to have been fooled and therefore, she could not have reported it. "*No, because we were fooled because of our own fault so did not consider it suitable to report. Meaning, there was no benefit of reporting. What should we report? What would we explain to someone about what happened? Then we did not [report] because the number that we had called [earlier] when we called back on it, it was unresponsive. Nobody was picking it up.*" (Victim 14)

Embarrassment among Educated Victim. We came across educated respondents who did not report such scams or if they lacked knowledge about reporting, they would not ask anyone in their social circle out of the fear of being socially embarrassed, also reported by [56]. "*No [I did not report]. Like I told you, I told a friend and all she did was scold me. So I was afraid that if I would tell anyone else, they would have said that I am so educated and I still did something like this. I felt embarrassed because i thought what use is this education if one falls for such scams.*" (Victim 62)

9.3 Gendered Trends in Non-Reporting

We observed gendered trends in reporting behavior. Women reported concerns about tarnishing their own or their family's reputation, mobility constraints and the fear of criticism upon disclosure to male family members as reasons for not reporting or even disclosing incidents of frauds. Women tend to not report because of dependency on male family members for reporting to relevant authorities and also driven by the misconception that frauds need to be reported at Police Stations where women find it difficult to go alone because of fears of harassment and security. Women are seen visiting FIA office or a police station along with male family members to report cyber-harassment and blackmailing. This ofcourse requires first disclosing any incident, that needs to be reported, to the family members who may criticize women on their poor judgment. Some of our female respondents shared that they have never shared these incidents with their family as men already think that women are gullible and more likely to fall for such scams, as also reported by previous research [32]. One participant shared, "*No, men think women are stupid anyway and can be easily scammed. That is why I did not mention it to my husband. When I mentioned it to my relatives they said that such things are a scam and you should not trust them.*" (Non-Victim 1)

Mobility & Reporting. Another female respondent was influenced by lack of information around reporting and mobility constraints and decided not to report. "*Report?! I don't know. Actually, there is no male in our household. Therefore, we used to be wary of doing the running around and so avoided reporting. We were like what should we report? Like where would ladies go for reporting? So we did not go [for reporting].*" (Victim 14). Another female respondent was of the opinion that reporting would only result in losing more money and indignity.

"*No I did not file a report. I thought it was no use. Where would a woman go (for reporting)? When you go for reporting to police station, half of the money [of the amount lost] is consumed by the police station people [in bribes] then there is the added indignity and no benefit.* " (Victim 29)

Fear of Negative consequences. One woman shared that she did not share the incident of fraud with her husband out of the fear of being beaten and her phone being snatched from her for talking to strangers and loosing the money.

> "*No I did not think of reporting and I did not tell these things to anyone. To be honest, I am telling you in the hopes that you would do something for us. That vile person took all my savings and vanished. Its been 2, 2.5 years but I have not told my husband. If I had told him, he would have broken my legs that I gave the fraudster so much money. Money aside, he would have said why I trusted him [the fraudster], why did I talk to him, why do you talk on phone. He would have snatched my phone. That is why I did not report it. If I would have told then one thing would have led to another that is why I did not tell anyone. To this day, I get goosebumps. I did not tell anyone. I said to myself that now the money has gone to hell.*" (Victim 22)

Reaction from Social Circle. Woman feel comfortable and trust their female friends and other women in their social circle to disclose these incidences. One woman shared how she discussed such an incident with her friends but not her family. Her friends then shared incidents of frauds known to them to explain to her not to trust such calls.

> "*No, I told my friends. After they berated me a lot, then how could I have told anyone at home. They started quoting instances [of frauds]. But the thing is, I knew Benazir Support's scams are happening but I did not know that Jeeto Pakistan scams are also happening. I did not know that someone would call me from a short number [short code] and would know my name too and would say that we can talk when you are free from your class. That makes it look like an official call.*" (Victim 62)

Shame for the Family. One woman shared how going to a police station is a source of shame for her family therefore they avoided reporting.

> "*Sister, where should a poor man go and how should they. We hardly make both ends meet. In any case, going to a Police Station is considered an insult [in our social circle]. The envious relatives and extended family start talking that is why we did not report. They would not have said that we were victims of fraud. They would have said that there is something suspicious going on that is why they are going to police station.* " (Victim 33)

10 DISCUSSION

Researchers in HCI and CSCW [23, 25, 74] are increasingly pursuing agendas that aim to address security and privacy concerns within users' contexts. Our study aimed to explore the dynamics around the prevalent mobile-based frauds in Pakistan with the goal to identify points of intervention and affordances for designing appropriate technological interventions to thwart such attacks. We conducted qualitative interviews with 71 victims, 7 non-victims, 15 mobile money agents, and 3 regulatory officials. Through a thematic analysis of these interviews, we identified the common fraud types reported in our data, the relevant actors in the fraud cycle and their role in limiting or (unknowingly) supporting the fraudsters' agenda, and attitudes of victims towards reporting of frauds. Inspired from the social engineering fraud cycle, we analyzed the methods employed by the fraudsters to gain victims' trust, deteriorate their decision making ability, and ensure compliance from the victims. We also explored victims' triggers for realization, immediate reaction, and long-term change in victims' behaviors. Appreciating the context of a *collectivist culture*, during all these

steps, we do not limit our analysis to the actions of the victim and the fraudsters only but also include other actors—law enforcement agencies, mobile money agents, top-up shops, the victims' social circle—to identify *human assets* and interactions that could be leveraged for increasing awareness about mobile-frauds.

Exploitation of digital infrastructure. Low-income users negotiate their privacy practices by comparing what they are being offered in exchange for the data that they are providing and if the reason for data collection resonates with them [69]. Our findings indicate that fraudsters are exploiting the practice of privacy negotiation and the lack of awareness among technologically excluded or those with limited inclusion (e.g., individuals with a feature phone but not a smartphone) to collect resources for carrying out attacks. These include fraudulently verifying SIMs against the biometrics of citizens who do not own or use a phone; these citizens may never check if any SIMs are registered on their name. This also includes feature phone users who might end up sharing Whatsapp OTP with fraudsters unaware of the consequences. This creates a false trail to these marginalized individuals and protects the identity of the fraudsters. Similarly, Over-The-Counter (OTC) transactions are being used to defraud people without leaving a trail. Ironically, the same ICT and mobile money infrastructure created to benefit the marginalized population is being used to exploit them. As the mobile phone penetration increases across the globe, with the highest increase predicted in emerging markets, the risk of exploitation of the uninformed users also increases. Possible leakages of customers' personal data like phone numbers and addresses from franchises and customer support call centers further indicates the potential of exploitation of the digital infrastructures and underscores the need for data security and privacy policies for service providers to ensure customer privacy [11].

10.1 Technological, Procedural and Infrastructural Vulnerabilities

ICT infrastructures like universal identities have been championed as enablers of financial inclusion and development. As Singh et al. highlight, inclusion in ICT is an ongoing and fragile process and there is a need to attend to the design and use of ICT infrastructures at the seams where various interconnected systems merge and there is uneven inclusion and possibilities of exploitation at these spaces [67]. We extend the discussion on *imbrication* in ICT infrastructures to show that in addition to the technological and human vulnerabilities, political, procedural, infrastructural unevenness at the seams impact users in developing countries and these seams are exploited by scammers to carry out mobile-based financial frauds.

10.1.1 Regulatory Jurisdiction, Technological and Awareness issues around Biometric Verification System (BVS). A verified SIM establishes trust in any interaction and provides a mechanism for the governments to track and report activities for development, financial inclusion, and preventing illegal activities such as grey trafficking, mobile-based frauds, and even terrorism. Ahmed et al. [4] highlighted various concerns of citizens in the Global South against biometric SIM verification such as lack of trust in the entity carrying out such verification, the technical prowess required to ensure the requisite security [2] and hence the privacy of citizens' data in the biometric surveillance systems. Our study indicates that in contexts where such biometric identification has been normalized, trust of the marginalized population on entities that help create, maintain, and consume these identities [35] can be exploited [9] by adversaries to bypass such surveillance. There are three contributing factors: *i)* manipulating technologically unaware citizens, whose fingerprints are part of the biometric database, into providing their biometrics, *ii)* technical security of the verification devices that enable authentication, and *iii)* insufficient due-diligence in the distribution of BVS machines, resulting in a large scale access including to less trustworthy actors, which magnifies any risk arising due to security vulnerabilities. State Bank of Pakistan, the financial regulator, has

mandated every financial institution to provide BVS machine to their respective mobile-money agents who should then perform biometric verification for the sender and receiver of each OTC transaction [36]. Installation of BVS machines to small shops will increase the risk associated with the vulnerabilities in BVS and further enable fraudulent SIM verification. However, last mile availability of BVS machines could also prevent use of OTC by fraudsters as it would require establishing identity of the recipient.

Clear delineation of roles and responsibilities between the Law Enforcing Agencies (LEAs) and regulators [18] is required to eliminate vulnerabilities and prevent fraudulent verification. Criminology's broken window theory [75] states that general lawlessness and lack of punishment gives rise to serious crimes in the future and such prevalence of disorder creates an illusion of unsafe environment among the citizens. Lack of ownership of an issue by agencies and regulators creates room for new fraudulent actors to capitalize on the opportunity because the probability of being caught as well as the consequences once caught are minimal, if not non-existent.

10.2 Social Warning Systems

Prior work suggests that low-literate and rural populations are more affected by mobile-based financial frauds [53]. Our study indicates that fraud affects mobile users from varied educational backgrounds, from non-literates to college graduates. Mental models are created and updated based on experiences and information. In our study, while educated individuals sometimes actively resisted fraudsters, participants with high school or lesser education usually required some assistance in identifying a fraud attempt, had limited understanding of the types of frauds, were unable to extrapolate experiences from one type of fraud to another, and took longer to realize after being defrauded. In cases of suspicion, they relied on their social network for verification. Our study confirms that in a collectivist culture, and in the absence of system based warnings, social actors like friends, family and colleagues [56] act as information sources at various stages of fraud.

However, there are several drawbacks of social warning systems and we highlight four of them here. 1) In cases where the friends, family, colleagues and agents are also unaware about frauds, they participate and support the victim in compliance. Since there is no formal warning, the need to decipher the incident does not arise until very late. 2) Due to a collectivist culture, the need to consult is overcome by the need to protect one's reputation and impression. Socio-cultural factors impede information seeking and hence development of mental models around mobile-based frauds. We see this particularly among women who hesitate in seeking support or information and hence their mental models are limited to their own experiences as opposed to men who have more elaborate mental models. 3) The perceived credibility of warnings given by a social actor like an agent remains limited. 4) The social diffusion process is slower compared to the pace of evolution of threat model - the speed with which fraudsters update cues, moving on to more serious frauds over time, which we refer to as fraud schemes. Hence users' mental models also evolve slowly. Mobile users cannot detect a fraud by its general characteristics if it has been packaged into a different scheme. Changing schemes erodes any collective experiential learning of the masses in identifying frauds, providing an avenue for fraudsters to scam low-income users under a new scheme. [5]

10.3 Recommendations

We suggest formal education to overcome the limitations or drawbacks of social warning systems and capitalize on the benefits of the collectivist culture.

[5] A recent example is the Pakistan Government's announcement to provide funds to low-income households with no income due to the COVID-19 lockdown. Fraudsters have already started exploiting this scheme [65] impersonating State Bank officials and claiming to open victims' accounts for cash transfers.

10.3.1 Empowering Agents through Information. Educating users can include increasing awareness about the typical characteristics of a social engineering attack, new fraudulent schemes, concepts about what constitutes personal information and the possible negative consequences of sharing this information. The medium of education needs to be updated to address all citizens, particularly those in rural areas and should not be limited to mobile subscribers and banked populations. Internet based media is unlikely to reach users without internet access. We recommend taking an assets-based approach to reach these users. We identify family, friends, colleagues, and shop-agents as the *human assets* in the social engineering cycle. Mobile money agents constitute an inevitable point of contact for many victims during the fraud cycle and are in a unique capacity to intervene in the fraud process. Although the efficacy of warnings by agents relies currently on the social capital between agents and their customers, technological tools that identify or verify agents' suspicion of fraudulent communication and inform about typical characteristics of prevalent scams and fraudulent numbers, can increase the credibility of agents' warnings where customer-agent social capital is lacking. We suggest equipping agents with applications which lend credibility or legitimacy to their warnings and enable them to help customers identify a fraudulent number or SMS and also report it. Mobile subscribers can be educated to consult agents before sending money to a stranger and take agent warnings seriously.

Since the fraud schemes are constantly evolving, the authorities need to collect updated information about the prevalent fraud types, schemes, and tactics. This updated information should be utilized to educate (and warn) mobile users about the latest trends in mobile fraud.

10.3.2 Educational campaigns by authority figures. Literature [37] suggests that victims' trust in scammers is a factor in scam compliance leading to shift of victims' focus on the interaction rather than the plausibility of the message. This leads to peripheral—instead of logical— processing of information, deteriorating victim's decision making ability [22]. Our study identifies the various sources of authority fraudsters impersonate in order to exploit victims' offline trust in these authorities, which include military and bank officials, game show staff, and government officials representing cash transfer schemes. They use tactics like mimicking call center interaction, creating the illusion of sharing information only accessible to telecom operators, banks or government, and calling from designated helpline numbers or shortcodes.

The ideal leverage points to break this association are the offline trusts whose credibility is being utilized by fraudsters. This can be in the form of game show hosts informing at the end of their TV show or government-backed ad campaign as the Government of Pakistan already utilizes ads for health and other campaigns. Another asset available to reach the last mile is through caller tunes. During COVID-19, telecom operators in various developing countries including Pakistan are mandated by the government to play awareness messages on caller tunes [6] to raise awareness. Similar approach can be used to raise awareness against fraudulent schemes particularly focusing on the remote rural parts not accessible through other media, such as social media, newspapers.

10.3.3 Redesigning Reporting for Social Influences. Vashitha et al. suggest that the design of security and privacy measures in the developing world should be embedded in the sociocultural practices, needs and behaviors [73]. In developing world and Islamic contexts, women's technology engagement including ownership and use is affected, both enabled and limited, by the family members [33]. Their financial and technological agency depends on men's perception of their gullibility [31]. Gender is also a factor in shaping the security and privacy practices of individuals in Global South [62]. We contribute to this research by demonstrating that gender also shapes

[6]Caller tunes, also known as Caller Ring back Tunes, are sounds heard by the caller when the call is made before the receiver picks up the phone. Operators also allow it to be changed to message or songs.

reporting behaviors around mobile frauds. Women avoid reporting out of the fear of negative reactions and criticism by family, friends, and particularly spouses. Women also fear losing agency of mobile use due to family's reactions to interactions with unrelated men over phone along with the financial loss. The misconception that frauds need to be reported at police stations also leads women to avoid reporting due to lack of mobility and dependency on men to visit police stations. The cultural factors at play in our study around reporting behaviors indicate a need to redesign reporting such that it ensures privacy of individuals and offers a convenient friction-less reporting process. *Reporting channels and mechanisms* need to be redesigned to allow women to report without leaving home or needing assistance of a man, facing harassment or compromising her privacy. A convenient reporting mechanism (e.g. a smartphone-based application) could significantly reduce the required effort for reporting and could possibly increase the frequency of reporting. This can be seen in the significant increase in reports filed by women since the creation of FIA's website for reporting cybercrimes.

Currently, reporting is associated with negative social outcomes. However, reporting behaviors need to be encouraged, incentivized, and associated with society's collective good. We recommend associating reporting and helping fellow citizens in filing reports with being a good and responsible citizen. Perceptions around the benefits of reporting should be updated to include altruistic reasons like protection of others beyond ties to one's own benefits of financial recovery. Existence of clear reporting authorities and precise protocols (e.g. providing screenshots, SMS, or timestamps), acknowledgement of citizens' fraud reports and separation of reporting mechanisms for digital and relatively low-value crimes from other in-person and serious criminal incidents will reduce friction to reach out to law enforcement agencies and might provide positive incentives to report.

Reporting parameters can include the fraudsters' number, content of text messages from fraudsters. The serial number of top-up cards sent to fraudsters can be reported and used by telecom operators to detect subscriber IDs where such cards have been consumed to detect and block further fraudulent numbers. Existing crowdsourced spam blocking applications remain ineffective at blocking such fraudulent calls and SMS as fraudsters keep on changing their numbers. Reporting can work towards restricting activities of fraudsters by limiting their resources such as access to fraudulently verified SIMs, which are used to make multiple fraudulent messages and calls. The sooner each fraudulent SIM is detected and blocked, the fewer fraudulent activities can be done by fraudsters.

11 CONCLUSION

In this paper, we report a one-year study to understand and describe the mobile-based frauds occurring in Pakistan. Using qualitative interviews with 78 participants (victims and non-victims) including 56 men and 22 women, 18 stakeholders (regulatory officials and mobile money agents), we report the various actors and types of mobile-based frauds in Pakistan. We present our findings using the conceptual framework of social engineering to explore the human aspect of these frauds in detail. We describe the victims' interaction with the fraudsters, victims' social circle, and financial institution representatives in various fraud types. We showcase how these interactions and the social perceptions form victim's reactions, responses, and reporting behavior. We also identify various points of intervention and human assets during the social engineering life-cycle.

Our findings show that fraudsters are rapidly updating schemes (stories concocted to gain trust) to hook an increasing number of potential victims. However, the general efforts to curtail the losses and increase awareness are all lagging behind. We also report the various reasons for non-reporting by victims, including trust issues with reporting authorities, embarrassment, the hectic process of reporting, and perception of unfavorable outcomes after reporting. We also discuss a lack of discourse, discussion, and reporting by women, due to embarrassment to family or threats to their agency, and how that leads to a lack of collective learning among women when compared to men.

12 ACKNOWLEDGMENTS

We would like to thank all participants for their time and detailed responses, Khansa Sanabal and the students of ITU BSCS Class of 2020 for their assistance in data collection, Dr. Agha Ali Raza (Lahore University of Management Sciences), and Dr. Umer Janjua (Information Technology University) in Lahore, Pakistan for their guidance at the early stages of this study. We would also like to thank Sudheesh Singanamalla from ICTD Lab for rereading the paper and helping us improve it along with Dr. Richard Anderson and Sam Castle of Paul G. Allen School of Computer Science and Engineering at the University of Washington who initiated the research on SMS frauds in Pakistan which formed the basis for this study.

REFERENCES

[1] Adeyinka Adedoyin, Stelios Kapetanakis, Georgios Samakovitis, and Miltos Petridis. 2017. Predicting fraud in mobile money transfer using case-based reasoning. In *International Conference on Innovative Techniques and Applications of Artificial Intelligence*. Springer, 13 pages.

[2] Adhaar Leak [n.d.]. *Personal data of a billion Indians sold online for £6*. Retrieved Jan 2018 2020 from https://www.theguardian.com/world/2018/jan/04/india-national-id-database-data-leak-bought-online-aadhaar

[3] Nova Ahmed, Farlina Barik, Zareen Tasnim, and Jasmine Jones. 2019. Development Through Digital Family Stories in Bangladesh. In *Proceedings of the Tenth International Conference on Information and Communication Technologies and Development (ICTD '19)*. ACM, New York, NY, USA, 40:1–40:5. https://doi.org/10.1145/3287098.3287136 event-place: Ahmedabad, India.

[4] Syed Ishtiaque Ahmed, Shion Guha, Md Rashidujjaman Rifat, Faysal Hossain Shezan, and Nicola Dell. 2016. Privacy in Repair: An Analysis of the Privacy Challenges Surrounding Broken Digital Artifacts in Bangladesh. In *Proceedings of the Eighth International Conference on Information and Communication Technologies and Development*. 10 pages.

[5] Syed Ishtiaque Ahmed, Md Romael Haque, Shion Guha, Md Rashidujjaman Rifat, and Nicola Dell. 2017. Privacy, security, and surveillance in the Global South: A study of biometric mobile SIM registration in Bangladesh. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 13 pages.

[6] Isaac Akomea-Frimpong, Charles Andoh, Agnes Akomea-Frimpong, and Yvonne Dwomoh-Okudzeto. 2019. Control of fraud on mobile money services in Ghana: an exploratory study. *Journal of Money Laundering Control* (2019).

[7] Pakistan Telecommunication Authority. [n.d.]. *Biometric Verification*. https://www.pta.gov.pk/en/consumer-support/complaints/biometric-verifications

[8] Pakistan Telecommunication Authority. [n.d.]. *Telecom Indicators*. https://www.pta.gov.pk/en/telecom-indicators

[9] Geoffrey Barbier and Huan Liu. 2011. Data Mining in Social Media. In *Social Network Data Analytics*, Charu C. Aggarwal (Ed.). Springer US. https://doi.org/10.1007/978-1-4419-8462-3_12

[10] Anurag Bhatia. [n.d.]. *Decline of landline in India*. https://telecomtalk.info/decline-of-landline-in-india/66093/

[11] Jasmine Bowers, Bradley Reaves, Imani N Sherman, Patrick Traynor, and Kevin Butler. 2017. Regulators, mount up! Analysis of privacy policies for mobile money services. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*. 18 pages.

[12] Jasmine Bowers, Imani N Sherman, Kevin RB Butler, and Patrick Traynor. 2019. Characterizing security and privacy practices in emerging digital credit applications. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*. 14 pages.

[13] V. Braun, V. Clarke, V. Braun, and V. Clarke. 2006. Using Thematic Analysis in Psychology. *Qualitative Research in Psychology* 3, 2 (2006), 25 pages. http://dx.doi.org/10.1191/1478088706qp063oa

[14] Sam Castle, Fahad Pervaiz, Galen Weld, Franziska Roesner, and Richard Anderson. 2016. Let's Talk Money: Evaluating the Security Challenges of Mobile Money in the Developing World. In *Proceedings of the 7th Annual Symposium on Computing for Development*. ACM, 10 pages. https://doi.org/10.1145/3001913.3001919

[15] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle, and Paul C Van Oorschot. 2011. Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism. *IEEE Transactions on Dependable and Secure Computing* 9, 2 (2011), 14 pages.

[16] Kwan Choi, Ju-lak Lee, and Yong-tae Chun. 2017. Voice phishing fraud and its modus operandi. *Security Journal* 30, 2 (2017), 13 pages.

[17] Mark Ciampa. 2013. A comparison of password feedback mechanisms and their impact on password entropy. *Information Management & Computer Security* (2013).

[18] DAWN. [n.d.]. *FRADULENT ACTIVITIES: FIA recovers 2000 SIMS from eight suspecrs*. http://www.fia.gov.pk/en/images/2018/nov/full_news/21-11-2018%201.jpg

[19] Trajce Dimkov. 2012. Alignment of organizational security policies–theory and practice. *University of Twente* (2012).

[20] Jie Du and Gregory Schymik. 2018. Gender Difference on Studentsâ€™ Email Security Behaviors. (2018).
[21] William Enck, Patrick Traynor, Patrick McDaniel, and Thomas La Porta. 2005. Exploiting open functionality in SMS-capable cellular networks. In *Proceedings of the 12th ACM conference on Computer and communications security*. 12 pages.
[22] Peter Fischer, Stephen EG Lea, and Kath M Evans. 2013. Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. *Journal of Applied Social Psychology* 43, 10 (2013), 13 pages.
[23] Diana Freed, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. 2019. " Is my phone hacked?" Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 24 pages.
[24] Lara Gilman and Michael Joyce. 2012. Managing the risk of fraud in mobile money. *GSMA: Mobile Money for Unbanked (MMU)* (2012).
[25] Ricardo Gomez and Elizabeth Gould. 2010. The" cool factor" of public access to ICT. *Information Technology & People* 23, 3 (2010).
[26] Government of Pakistan. 2020. Pakistan Telecommunication Authority. https://pta.gov.pk/en
[27] Ralph Gross and Alessandro Acquisti. 2005. Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*. 10 pages.
[28] GSM Intelligence. 2019. *The Mobile Economy 2019*. Annual. GSM Association. https://www.gsma.com/mobileeconomy/
[29] GSM Intelligence. 2020. *The Mobile Economy 2020*. Technical Report 2020. GSM Association. https://www.gsma.com/mobileeconomy/
[30] Eszter Hargittai. 2007. Whose space? Differences among users and non-users of social network sites. *Journal of computer-mediated communication* 13, 1 (2007), 22 pages.
[31] 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*. ACM, 11 pages. https://doi.org/10.1145/3136560.3136571 event-place: Lahore, Pakistan.
[32] Samia Ibtasam, Lubna Razaq, Haider W. Anwar, Hamid Mehmood, Kushal Shah, Jennifer Webster, Neha Kumar, and Richard Anderson. 2018. Knowledge, Access, and Decision-Making: Women's Financial Inclusion In Pakistan. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies*. ACM, 12 pages. https://doi.org/10.1145/3209811.3209819
[33] Samia Ibtasam, Lubna Razaq, Maryam Ayub, Jennifer R Webster, Syed Ishtiaque Ahmed, and Richard Anderson. 2019. " My cousin bought the phone for me. I never go to mobile shops." The Role of Family in Women's Technological Inclusion in Islamic Culture. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 33 pages.
[34] Tom N. Jagatic, Nathaniel A. Johnson, Markus Jakobsson, and Filippo Menczer. 2007. Social Phishing. *Communications of the ACM (CACM)* 50, 10 (Oct. 2007), 7 pages. https://doi.org/10.1145/1290958.1290968
[35] Aditya Johri and Janaki Srinivasan. 2014. The role of data in aligning the'unique identity'infrastructure in India. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing*. 13 pages.
[36] Imran Khan, Mimansa Khanna, Sidra Butt, and Vera Bersudskaya. 2017. Agent Network Accelerator Research: Pakistan Country Report September 2017. *Helix Institute of Digital Finance* (Sept. 2017).
[37] Jeff Langenderfer and Terence A Shimp. 2001. Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. *Psychology & Marketing* 18, 7 (2001), 21 pages.
[38] Heather Richter Lipford, Gordon Hull, Celine Latulipe, Andrew Besmer, and Jason Watson. 2009. Visible flows: Contextual integrity and the design of privacy mechanisms on social network sites. In *2009 International Conference on Computational Science and Engineering*, Vol. 4. IEEE, 5 pages.
[39] Johnny Long. 2011. *No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing*. Syngress.
[40] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F. Churchill, and Sunny Consolvo. 2017. Stories from Survivors: Privacy & Security Practices when Coping with Intimate Partner Abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 13 pages. https://doi.org/10.1145/3025453.3025875
[41] Nora McDonald and Andrea Forte. 2020. The Politics of Privacy Theories: Moving from Norms to Vulnerabilities. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. 14 pages. https://doi.org/10.1145/3313831.3376167
[42] McKinsey Global Institute. 2016. *Digital Finance For All: Powering Inclusive Growth In Emerging Economies*. Technical Report. McKinsey&Company. http://www.mckinsey.com/global-themes/employment-and-growth/how-digital-finance-could-boost-growth-in-emerging-economies
[43] Mary Meeker. 2019. *2019 Internet Trends*. Technical Report. KPCB. https://techcrunch.com/2019/06/11/internet-trends-report-2019/

[44] Gustavo S Mesch. 2012. Is online trust and trust in social institutions associated with online disclosure of identifiable information online? *Computers in Human Behavior* 28, 4 (2012), 7 pages.
[45] Marina Micheli. 2016. Social networking sites and low-income teenagers: between opportunity and inequality. *Information, Communication & Society* 19, 5 (2016), 17 pages.
[46] Ministry of Interior Government of Pakistan. 2020. Federal Investigation Agency. http://www.fia.gov.pk/en/index.php
[47] Francois Mouton, Louise Leenen, Mercia M Malan, and HS Venter. 2014. Towards an ontological model defining the social engineering domain. In *IFIP International Conference on Human Choice and Computers*. Springer, 14 pages.
[48] Francois Mouton, Louise Leenen, and Hein S Venter. 2016. Social engineering attack examples, templates and scenarios. *Computers & Security* 59 (2016), 24 pages.
[49] Adil Najam, Faisal Bari, et al. [n.d.]. *Pakistan National Human Development Report 2017*. https://planipolis.iiep.unesco.org/sites/planipolis/files/ressources/pakistan_nhdr_2017.pdf
[50] Soud Nassir and Tuck Wah Leong. 2017. Traversing Boundaries: Understanding the Experiences of Ageing Saudis. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 12 pages. https://doi.org/10.1145/3025453.3025618 event-place: Denver, Colorado, USA.
[51] nigerian scam [n.d.]. *Nigerian Advanced Fee Fraud*. Retrieved May 2020 from http://www.consumerfraudreporting.org/nigerian.php
[52] Helen Nissenbaum. 2004. Privacy as contextual integrity, 79 Wash. *L. Rev* 119, 121 (2004), -98 pages.
[53] 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*. 11 pages. https://doi.org/10.1145/3314344.3332500
[54] Rowan Phipps, Shrirang Mare, Peter Ney, Jennifer Webster, and Kurtis Heimerl. 2018. ThinSIM-based Attacks on Mobile Money Systems. In *Proceedings of the ACM SIGCAS Conference on Computing and Sustainable Societies (COMPASS)*. Article 23, 11 pages. https://doi.org/10.1145/3209811.3209817
[55] Zulfikar Ramzan and Candid Wüest. 2007. Phishing Attacks: Analyzing Trends in 2006.. In *CEAS*. Citeseer.
[56] Elissa M Redmiles. 2019. " Should I Worry?" A Cross-Cultural Examination of Account Security Incident Response. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 15 pages.
[57] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2016. How i learned to be secure: a census-representative survey of security advice sources and behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. 12 pages.
[58] Stuart Ross, Russell G Smith, et al. 2011. Risk factors for advance fee fraud victimisation. *Trends and Issues in Crime and Criminal Justice* 420 (2011).
[59] Kevin A Roundy, Paula Barmaimon Mendelberg, Nicola Dell, Damon McCoy, Daniel Nissani, Thomas Ristenpart, and Acar Tamersoy. [n.d.]. The Many Kinds of Creepware Used for Interpersonal Attacks. ([n. d.]).
[60] Norman Sadeh, Jason Hong, Lorrie Cranor, Ian Fette, Patrick Kelley, Madhu Prabaker, and Jinghai Rao. 2009. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and Ubiquitous Computing* 13, 6 (2009), 12 pages.
[61] Nithya Sambasivan, Amna Batool, Nova Ahmed, Tara Matthews, Kurt Thomas, Laura Sanely Gaytán-Lugo, David Nemer, Elie Bursztein, Elizabeth Churchill, and Sunny Consolvo. 2019. "They Don'T Leave Us Alone Anywhere We Go": Gender and Digital Abuse in South Asia. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, 14 pages. https://doi.org/10.1145/3290605.3300232 event-place: Glasgow, Scotland Uk.
[62] Nithya Sambasivan, Garen Checkley, Nova Ahmed, and Amna Batool. 2017. Gender Equity in Technologies: Considerations for Design in the Global South. *Interactions* 25, 1 (Dec. 2017), 4 pages. https://doi.org/10.1145/3155050
[63] 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)*. 16 pages.
[64] Qasif Shahid, Lubna Razaq, Ahsan Mughal, Mahrukh Imtiaz, Myra Piracha, and Omar Shahid. 2017. *SEEDING INNOVATION A framework for rooting FinTechs in Pakistan*. Technical Report. FinSurgents. http://www.karandaaz.com.pk/wp-content/uploads/2017/01/Seeding-Innovation.pdf
[65] Shehzad Ali. 2020. PTA blocks eight numbers over Ehsaas programme fraud. *SAMAA News* (April 2020). https://www.samaa.tv/news/pakistan/2020/04/pta-blocks-eight-numbers-over-ehsaas-programme-fraud/
[66] Hanul Sieger and Sebastian Möller. 2012. Gender differences in the perception of security of mobile phones. In *Proceedings of the 14th international conference on Human-computer interaction with mobile devices and services companion*. 6 pages.
[67] Ranjit Singh and Steven J. Jackson. 2017. From Margins to Seams: Imbrication, Inclusion, and Torque in the Aadhaar Identification Project. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 49 pages.

[68] Russell G Smith and Alice Hutchings. 2014. Identity crime and misuse in Australia: Results of the 2013 online survey. (2014).
[69] Janaki Srinivasan, Savita Bailur, Emrys Schoemaker, and Sarita Seshagiri. 2018. Privacy at the margins| The poverty of privacy: Understanding privacy trade-offs from identity infrastructure users in India. *International Journal of Communication* 12 (2018).
[70] Frank Stajano and Paul Wilson. 2011. Understanding Scam Victims: Seven Principles for Systems Security. *Commun. ACM* 54, 3 (March 2011), 6 pages. https://doi.org/10.1145/1897852.1897872
[71] Daily Times. [n.d.]. *Census to start from 15th with Pak Army support.* https://dailytimes.com.pk/23621/census-to-start-from-15th-with-pak-army-support/
[72] unbanked [n.d.]. *State Bank of Pakistan.* https://www.sbp.org.pk/Finc/About.asp
[73] Aditya Vashistha, Richard Anderson, and Shrirang Mare. 2018. Examining Security and Privacy Research in Developing Regions. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies*. ACM, 14 pages. https://doi.org/10.1145/3209811.3209818 event-place: Menlo Park and San Jose, CA, USA.
[74] Jessica Vitak, Yuting Liao, Mega Subramaniam, and Priya Kumar. 2018. 'I Knew It Was Too Good to Be True" The Challenges Economically Disadvantaged Internet Users Face in Assessing Trustworthiness, Avoiding Scams, and Developing Self-Efficacy Online. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 25 pages.
[75] James Q Wilson and George L Kelling. 1982. Broken windows. *Atlantic monthly* 249, 3 (1982), 29–38.
[76] Ezer Osei Yeboah-Boateng and Priscilla Mateko Amanor. 2014. Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences* 5, 4 (2014), 11 pages.

Received June 2020; revised October 2020; accepted December 2020