Kashf Journal of Multidisciplinary Research
Vol: 02 - Issue 09 (2025)
P-ISSN: 3007-1992 E-ISSN: 3007-200X
https://kjmr.com.pk

A NOVEL APPROACH FOR MOBILE WALLET SECURITY AND MONEY ASSOCIATE'S SECURITY

Fauzia Talpur[1], Hina Memon[2], Ghazala Bibi[3], Hina Shafi[4], Ramesh Kumar[5], Mir Sajjad Hussain Talpur[6]

[1] *Department of Computer Science, University of Sindh Laar Campus*

[2,4,5,6] *Information Technology Centre, Sindh Agriculture University, Tandojam, Pakistan*

[3] *Computer Science Dep, National University of Modern Languages (NUML), Islamabad*

Article Info

Abstract

Mobile money refers to performing monetary transactions using telecommunications networks. This activity is intended to be referred to as "mobile money." The rapid use of mobile money across Asia has the potential to destabilize the overall cash-based economies throughout the area. There is a chance that mobile money will have a significant effect on the economy. This is a possibility. Customers no longer need to physically go to a bank location to make deposits, withdrawals, or perform other banking-related tasks because mobile banking has made this capability available. The introduction of mobile cash paves the way for the development of further applications of mobile technology. Electronic monetary exchanges are now viable for various business and personal dealings. Cash-based economies in Asia will undergo a profound transformation due to mobile money. This shift will have significant repercussions for economies in every region of the planet. Mobile money security needs to be comprehensive since increasing numbers of consumers use mobile money services, and new business use cases are generated regularly. Continued efforts are being made to establish additional use cases for commercial applications. Because of their potential for loss, mobile money providers have incurred losses amounting to millions of dollars. They use qualitative research methods, such as interviewing participants, to obtain information. As part of the scope of this research project, we investigate how mobile network service providers safeguard their customers against the fraudulent use of mobile money. In addition, we analyse the dynamics of mobile based fraud currently taking place in Pakistan to identify potential locations of intervention and affordances for developing necessary technical interventions to defend against such attacks. This measure was implemented to combat the widespread use of mobile-based fraud in Pakistan. Customers are questioned about the safety of their mobile devices and the monetary services that they make use of. One of the most essential focuses of the current research is ensuring that mobile devices and online payment systems are secure.

Keywords:

Mobile Money, Cashless Economy, Mobile Banking Security, Fraud Prevention in Pakistan

1. INTRODUCTION

Mobile money is a digital financial service that allows users to send, receive, and store money on mobile devices. This has revolutionized how people access financial services, particularly in regions where traditional banking services are not widely available. With mobile money, users can carry out financial transactions anytime and anywhere, provided they can access a mobile device and a reliable Internet connection (Mudiri 2012). Internet transactions are now needed for many things, such as shopping, paying bills, sending money to someone else, and many more. People still use the Internet, but most do not buy things online because they fear their personal and financial information will be stolen. More steps must be taken to protect personal information and ensure it does not fall into the wrong hands. When you pay for things online, you should consider a few things regarding the safety of your financial transactions. (Taga et al., 2014). Because security is important, a way must be found to stop people who are not supposed to be there from getting in. You can take many steps to ensure that your financial transactions are safe. This group includes e-wallets, cryptographic protocols, and several others. The cash-based economy that currently dominates this continent may undergo a major transformation as the use of mobile money to undertake financial transactions increases globally (Solin & Zerzan, 2010).

Mobile money needs to be developed with a thorough strategy in mind to ensure that it is free from vulnerabilities that could lead to fraudulent conduct and security breaches. Losses in the multi- million dollar range have been incurred by several companies that help facilitate mobile money transactions as a direct result of the ever-present risk posed by cybercriminals. The first is the ever- increasing demand for mobile money services among consumers, and the second is the ever-increasing production of creative apps within the business world (Au and Kauffman, 2007). Both trends are predicted to continue in the coming years. When it comes to protecting their customers against scams when they make use of mobile money services, mobile network operators have a responsibility to take whatever steps are necessary, and the goal of this study is to investigate those steps. In addition, as a part of the investigation, we carried out a survey in which we asked users of mobile money their opinions on the question of whether they believe there is a connection between the safety of the mobile money services that they use from their own mobile devices and the safety of the mobile money services that are accessible from the same devices. (Mudiri 2012).

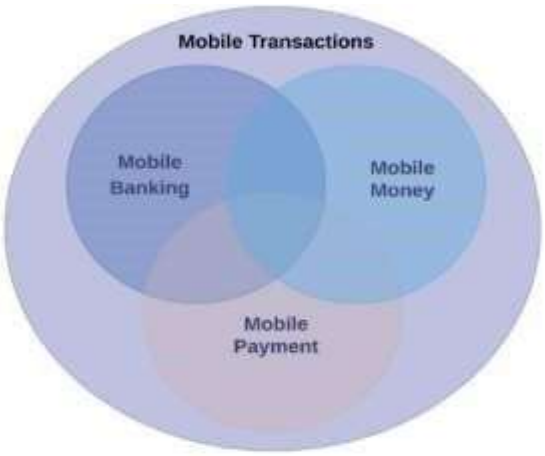

Figure 1: Mobile Transactions

One of the most significant findings was that people generally do not associate the safety of their mobile phones with that of mobile money. One of the main causes of customer fraud was found to be the sharing of PINs. The service provider should send SMS messages to its customers at least twice a year, with tips on better securing their mobile devices (H Joshi & D Chawla, 2023). Users can pay bills, such as utility and mobile phone bills, using their mobile money accounts. This eliminates the need to queue at payment centres or travel long distances to make payments. Mobile money payments are also more secure than traditional payment methods, requiring two-factor authentication, such as PIN or biometric verification, to complete the transaction(Amoah (Amoah et al., 2020).

Mobile wallet fraud has become a growing concern in the digital age as more people rely on mobile wallets for financial transactions. According to a Federal Reserve Bank of Atlanta report, the number of mobile wallet users in the United States is projected to reach 64 million by 2020 (Korolova 2014). As mobile wallet usage increases, providers must take steps to prevent fraud and protect their users. Strong authentication measures are among the most effective ways to prevent mobile wallet fraud. Mobile wallet providers should encourage users to use strong passwords and avoid using the same password on multiple accounts. They should also implement two-factor authentication, which requires users to provide two forms of identification, such as a password and fingerprint or facial recognition, before accessing their account. Two-factor authentication has been shown to reduce the risk of mobile wallet fraud by up to 80% (Juniper Research 2019). Mobile wallet providers should also educate users about the risks of mobile wallet fraud and provide tips to protect their accounts. Users should be informed of the latest fraud trends and techniques used by fraudsters. They should also be provided with clear and easy-to-understand instructions on reporting suspicious activity and what to do if their account is compromised. According to a report by Juniper Research, user education is one of the most effective ways to prevent mobile wallet fraud (Khan et al., 2017). Another important step that mobile wallet providers can take to prevent fraud is monitoring accounts for suspicious activities. This can include monitoring for multiple failed login attempts, unusual transaction patterns, or other signs of fraudulent activity. Providers should also have fraud detection and prevention systems to identify and prevent fraudulent transactions. According to a Javelin Strategy and Research report, mobile wallet providers that invest in fraud detection and prevention systems can reduce fraud losses by up to 80% ((Yao et al., 2018). Mobile wallet providers should also set transaction limits to reduce the risk of large-scale fraud and limit the financial impact of any fraudulent activity. Transaction limits can be set based on the amount of money transferred or spent using the platform. According to a report by the Aite Group, setting transaction limits is one of the most effective ways to prevent mobile wallet fraud (Aite Group 2017).

2. Literature Review

2.1 Mobile payments, M-Commerce, or E-Commerce

M-payment, or mobile payment, is when money is exchanged for goods or services using a mobile device to start, authorize, and confirm the transaction. This payment is sometimes called "m-payment" (Karnouskos, 2004). "Mobile devices" in this discussion means any phone, tablet, or device that can connect to a mobile network and accept payments. Cellular networks and Wi-Fi networks are both part of mobile networks. Depending on the ways the MNO makes the service available, customers may only be

able to use mobile phones, or they may be able to use any mobile device. When people use M-Payments, they can pay for goods and services with what is called "e-money" or "m-money." (Herzberg 2003).

Mobile money services are growing increasingly popular across the bulk of Africa, partly because most African nations do not have traditional banking services. More than a billion people live in developing nations, but they have access to mobile phones but do not have formal bank accounts (GSMA 2012). In Africa, there is a sizable population that makes use of mobile phones. Because of this, it is now feasible for financial services to be provided to persons living in rural poverty who do not have bank accounts.

2.2 General uses of mobile money

As mobile money services become increasingly common in people's daily lives, it is safe to say that they are making money transfers much easier and less expensive. In Ghana, for example, a person can put money in their mobile money wallet and send it to other mobile money users or to people who don't have mobile money. This saves time that would have been spent travelling long distances, waiting in line at banks to deposit money, or using risky methods like sending money by bus to people in nearby cities and towns. By clicking a few buttons on their phone, the person who gets a mobile money transfer can get it immediately. The m-payment market seems to be growing quickly, which can be explained by the fact that most users like how easy and convenient the service is for making transactions and payments with their phones (Au & Kauffman 2007). Mobile money has much potential to improve mobile payments and the cashless society many African countries are moving toward. Here are the main ways that mobile money can be used.

2.2.1 Transfer – domestic and international

Two individuals in the same country can send one another money (Solin & Zerzan, 2010). All three mobile money service providers in Ghana MTN Ghana, Tigo (Millicom Ghana), and Airtel offer this service so consumers can send money to others anytime. A registered or unregistered user can send money to either party using their mobile device. A registered user can transmit money to another user by withdrawing funds from the recipient's mobile money wallet or providing an unregistered user with a token and secret withdrawal code. A 9 user who is not registered can transmit or receive mobile money at a retailer or MNO service center. It is illegal in Ghana to transfer funds between networks. A user cannot, for example, transfer funds from MTN Ghana mobile money to Airtel mobile money. This causes people to be concerned about the ability to transfer money between networks, known as MNO interoperability (IFC 2011) and is something that rival mobile money service providers must recognize as a component of the value they provide to customers(H Joshi & D Chawla 2023).

Conversely, migrant workers often send money back to their families who still live in their home countries (Solin & Zerzan 2010). This service is usually provided by combining mobile money services with money transfer services like Western Union. Ghana does not yet offer international money transfers through mobile money, but this will change as the market becomes more competitive and new mobile money applications are made.

2.2.2 Payments for goods and services

You can use mobile payments to purchase items in stores and from vendors. Payment is made at the time of transaction by instantly depositing funds into the mobile money accounts of the store owners. These types of transactions are only possible in Ghana, where the buyer and vendor must use the same mobile money service to process the transaction. Also, basic utility services like power, water, and DSTV subscriptions can be paid for using mobile money services, which offers customers better ease and efficiency (Solin & Zerzan, 2010). In Ghana, one of the features offered by all mobile service providers is the ability to pay for utilities with mobile money. Utility payments using mobile money can be made at bank branches, utility company offices, outlets of specialist payment networks, or retail stores with agency agreements with these utility companies (Amrik & Mas, 2009). Consumers can conveniently pay utility bills with mobile money and skip the hassle of conventional payment methods. You could pay for public transportation with mobile money (IFC, 2011).

2.3 Security of Mobile phones, mobile money, m-payment services

Many emerging technologies, which are still maturing, enable mobile payment (Eze et.al 2008). These technologies are required to meet the diverse needs of the payment industry, including secure authentication infrastructure on mobile devices, secure transmission infrastructure for wireless payment, trust/validation directories, and virtual "wallets" stored on a mobile device or accessible via a network (I khan et.al 2017). Despite advances in mobile technology, M-payment security is still paramount. A "Manin-the-middle" assault can steal data from NFC devices when they contact the reader, usually within 10 centimeters. SMS and USSD are included in entry-level mobile money phones that use the GSM network (World Bank, 2012). GSM and UMTS networks provide end-to-end security. USSD, like SMS, uses the GSM/UMTS signalling plane's security and lacks its own. Authentication, message integrity, replay detection, sequence integrity, proof of receipt and execution, message secrecy, and security procedures are also claimed. Applications decide whether to employ them and whether their cryptographic strength is sufficient (Schwiderski-Grosche & Knospe, 2002).

2.3.1 Mobile money fraud and scams

Fraud in mobile money can be defined as purposeful actions by people in the mobile financial services ecosystem to make money for themselves, take money away from other people in the ecosystem, or hurt the reputation of other stakeholders. Fraud depends on how many people use the mobile money service and how often it happens. So, the different types of fraud also change when deployment does. (Mudiri 2012). Key factors that make mobile money fraud possible are the age of the mobile money services, weak or non-standard processes, cultural issues, lack of compliance monitoring (Mudiri 2012), and poorly thought-out new value-added services, like the post-paid scheme, in which the transaction is added to the user's phone bill and paid later (Merritt 2010). Fraud with mobile money can be put into the following groups, according to (Bahrini et,al 2019). Fraud is caused by the consumer, the merchant or agent, the business partner, the system administrator, or the mobile network operator (MNO).

Most research on information system security focuses on implementation and technical issues. According to (Taga et.al 2004) most consumers only consider security from their perspective, typically influenced

by marketing and public information (Karnouskos 2004). Trust is one of the most crucial factors when utilising M-Payment systems. A concentrated group study (Mallat 2007) on the use of mobile payments revealed, for instance, that a lack of perceived security is one factor that discourages their use. If this discourages using electronic payment systems in general and mobile payment solutions in particular, security must be considered seriously. But should security be viewed from the perspective of the service provider or the user?

Objective and subjective security are the two categories into which researchers have divided the security concept. "Objective security" refers to platform or application security based on certain technical characteristics (Kreyer et.al 2002). These security characteristics are mostly of interest to security professionals, system owners, and backend IT staff. According to some, not all clients can comprehend or evaluate the technical components of objective security (Egger & Abrazhevich 2001). On the other hand, it is claimed that personal security, or the felt perception of the procedures' security from the customer's perspective, is a more significant indicator of how mobile payment security promotes consumer acceptance.

For businesses to maximize their business opportunities and build customer confidence in the security of their services, they must adopt a security strategy that encompasses both objective security (security with technological characteristics) and subjective security (mostly procedural and from the customer's perspective). To be both subjectively and objectively secure, mobile payments must satisfy requirements for authentication, authorization, non-repudiation, and confidentiality (Egger &Abrazhevich 2001).

(Miduiri 2013) researched mobile money services in Argentina, Kenya, Papua New Guinea, Uganda, India, Indonesia, and the Philippines. As part of the exploratory research method that was used to do the study, interviews were done. The results convince the researchers that the problem needs a comprehensive solution, focusing on building people's skills and teaching them about money. (Z Rieke et.al 2018) Analyzed the part of the economy that deals with services that help people make transactions using electronic or mobile money services. To be more specific, they used a method for doing predictive security analysis in real-time. This tool tracks how processes act about transactions within a money transfer service. The goal is to compare how processes act to what a process model predicts they will do. They looked for strange behaviour different from what was expected, which could be a sign that the service was being used to launder money.

They tested how well the Predictive Security Analyzer instrument could do calculations and recognize patterns. It was made using real and fake records. The goal of the experiments was to find abuse patterns that matched a certain way of laundering money in a simulated process by pulling out attributes from real transaction events. (Adedoyin & Kapetanakis, 2017) It proposed an improved Case-Based Reasoning (CBR) technique to find mobile money service fraud.

They said that basic CBR capacity is improved by using machine learning to evaluate the sample size of instances that lead to the discovery of strange and fraudulent actions. Instead of employing the conventional dimensions of time and transaction amounts, they divided subscriber behaviour into five contexts and then combined them into one dimension. They also suggested that the CBR strategy might

work better if simulation data were used. Their findings demonstrated that weighted and combined dimensions outperform those measured independently(H Joshi & D Chawla 2023).

According to (Kanobe & Bwalya 2017), the emergence of mobile money services has helped the unbanked in emerging economies access formal financial services. This is one of the conclusions drawn from their research. They claimed that this problem was caused by a permissive regulatory climate, which encouraged the expansion of fraudulent transactions and contributed to their prevalence. They used a qualitative interpretive approach that was based on Activity Theory (AT), concentrating on information security regulations, regulatory papers, and processes when they were conducting the evaluation of the administration of the mobile money service. Their investigation revealed the reasons for the information security management flaws that are prevalent among mobile money service providers in underdeveloped countries. In addition to this, they discussed the roles that employees of mobile money operators play in ensuring the confidentiality of the service's customer information.

3. Materials and Methods

This research used a qualitative method to determine the social and economic factors behind mobile money theft. Using the research method, the memories of the people who participated in this study could be carefully examined from their point of view. So, it was easier to understand what the highlighted worries meant and how to interpret them. In qualitative research, context and meaning help people and groups reach their social and personal goals. A qualitative research method (Myers 2009) says that social constructs like relationships and behaviours play a part in the growth of social life and help us understand social and personal problems. So, the facts and parts of life are shaped and explained through the lens of the event in which they happen. We had brief talks with 71 victims, 7 people who weren't victims, 15 mobile money agents, and 3 people from regulatory and law enforcement groups to find answers to these questions. Using a four-step social engineering attack model, we can see how con artists try to get their victims to trust them, weaken their ability to make decisions and make them think they must follow their rules. Based on our study, fraudsters can use people with CNICs (Computerized National Identifier Cards) and mobile phones to gather information for network attacks. When no clear warning systems exist, most warnings and realization triggers come from social interactions. These are different for each victim(Yin 2011) We show that agents, friends, family, and coworkers can help stop theft by serving as intervention points.

3.1 Backgrounds

First, we will discuss the numerous individuals involved in mobile fraud before defining and explaining the process of mobile fraud. Because this research, we were able to learn about them. During the deception, they engage in various beneficial and detrimental activities to the target. In the next sections, Lets discuss these responsibilities in further detail.

Fraud Suspect. Participants in this study are those who own mobile phones and have experienced financial loss due to fraud conceived of and carried out during a phone call or text message.

Non-suspects. Those who answered a bogus call or received a fraudulent message but were able to avoid losing any money are non-victims.

Fraudsters. are bad people who use social engineering to trick people into giving them money. They can vary in how complex and well they are put together.

Family/Friends of Victims. In Pakistan, families are close and strongly based on gender. This means that family members can affect how women use technology. Because of this, we see friends and family members acting in different roles when fraud is involved.

Figure 3.1 Sample SMSs regarding cellphone fraud

On the left is an example of a BISP money-transfer SMS that the Pakistani government sends to people who get money through the BISP program. On the right is an example of spam that looks like a BISP message program. (The BENZIR income support program has awarded you Rs (spelling problems from the original message were kept intact, which is a red flag for bogus mail.) Call the Pakistan Telecommunication Authority (PTA) at this number: 0331-017396 and bring your BISP-registered ID card with you (right)

3.2 Sampling and recruitment

3.2.1 Official talk shows

First, we talked to PTA and FIA officials to learn more about the many mobile-based scams and how common they are. So that our sampling could be more accurate, we were motivated to collect reporting statistics on the different types of fraud and where they were happening. Three authors talked to government officials and wrote detailed meeting notes about what they said. Because of their jobs' importance, there are no recordings of the interviews. We also looked at Press Releases that the FIA had put out in the past to back up what people told us in interviews. After talking with the authorities, we did some qualitative research to learn more about the different types of fraud, how they were carried out, how participants felt about it, and how the fraud was reported. In semi-structured interviews, we talked to people who use mobile phones and handle mobile money (explained below). The first author and a group of undergraduate RAs interviewed users and agents. The undergraduate RAs were trained in interviewing techniques (like asking questions and probing) and given interviewing someone formally guides written in Sindhi by the first author. With the people's permission, interviews were done in Urdu or Sindhi, and their voices were recorded. After that, the recordings were written down in Roman Urdu. So that gender

didn't matter as much, especially when talking to women, researchers of the same gender interviewed the participants. No one who helped put on the event got paid.

3.2.2 Discussions with customers and users

We searched for mobile phone users who have interacted with scammers to identify victims (such as by answering a phishing SMS or call). We asked them about their experiences with mobile fraud to get people interested. All the people who answered "fraud victim" were picked for recruitment. We learned that some participants did not lose money through the semi-structured interviews. They considered themselves victims because they talked to fraudsters, even though they stopped talking to them when they realized the relationship was fake and didn't lose any money. These interviews with people who were not victims gave us different perspectives on possible intervention points, so we used them in our analysis. So that the sample would be as diverse as possible, we sought out individuals from various backgrounds, including urban and rural areas, genders, age ranges (18 to 25, 26 to 45, and 46+), and educational attainment. Our sample is similar in age to the Pakistani population. In Sindh, people were discovered in Hyderabad, Tandojam, and Arazi. We spoke to individuals who had fallen victim to fraud at various intervals, ranging from one month to five years, because there isn't much research on cellphone fraud in Pakistan.

We conducted in-depth semi-structured interviews to understand how and why users were involved in these fraudulent exchanges. We contacted the victims via someone they knew since talking to strangers about money can be uncomfortable, especially when it's connected to a crime. People didn't disclose their scams to anyone outside their social group for various reasons (covered in more detail in Section 9). Finding women to participate took longer since they tended to keep their experiences to themselves more than males. Their connections to researchers increased the public's confidence in researchers. We questioned each participant regarding their knowledge of others who had experienced phone scams after the session. Most people who were scammed didn't know of others who had been scammed. Some people who lost money told us about their situations hoping we could help them get their money back. As researchers, we clarified that we couldn't help them recover their money. We didn't find any false reports because it was a sensitive topic for the participants. We didn't have access to call logs, complaints, or message logs, which could have been used to back up what the participants said. Most of them didn't report, as the findings show. So, we relied on what people said them.

3.2.3 Recruiting for mobile money agents

15 mobile money industry employees took part in semi-structured interviews. Because they initially believed the researchers to be from the Department of Revenue, the police initially refused to speak with them. The undergraduate RAs demonstrated their student status to the mobile money vendors by using their school ID cards. RAs asked people in the area who knew them if they could help them find mobile money dealers in rural and peri-urban areas. The table shows the basic information for everyone who took part.

Table 3.2 Demographics of victim, non-victim, and agents

	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

3.3 Conducting interviews with guidelines

Users and mobile money agents each got their own set of interview guidelines. We made a list of things that the officials should talk about.

3.3.1 Victims and non-victims who use mobile gadgets

Mobile phone users' technology use, how and when they recognized they had been (or were being) deceived, how they reacted to that revelation, and how they felt about reporting fraud were all examined.

Details of the fraud incident(s), from when they initially got a phishing call or SMS to when they last spoke to the scammer, were also included.

3.3.2 Money agents on the go

We probed mobile money agents about their daily interactions with customers, the signs that a user is being scammed, the effectiveness of the agents' fraud warnings, and the level of customer comprehension and confidence in the reporting processes.

3.3.3 Regulatory agents

The most typical types of fraud and the demographics they affect were discussed, along with the degree to which they are planned, whether fraudsters can obtain verified SIM cards, how cunning they are, and whether there are statistics on complaints of fraud made by victims. Using "in-vivo" coding, the interview data from the officials was incorporated.

3.4 Analysis of data

Every interview was looked at through the lens of an inductive theme analysis. One codebook was made for interviews with users (victims and people who were not victims), and another was made for interviews

with mobile money agents. One author used the inductive coding feature in NVivo to code a few transcripts for each category. The first two writers talked about the codebooks made so that new codes and subcodes could be added and the order of data between codes could be changed. Coding the data was finished with the help of the completed codebooks. Three writers looked at the coded data. Three writers looked at the coded data.

3.5 Findings: participants understanding of fraud

This section discusses how people feel about fraud and the different kinds of fraud they have seen. Section 6 of the paper discusses how fraudsters set up a plan for a social engineering attack on our subjects. Section 7 discusses the many roles different people play in mobile scams. Sections 8 and 9 discuss how the subjects felt about mobile fraud and how their behavior changed after learning about it or becoming victims.

3.5.1 Participants' mental models of fraud

First, we asked people and agents what they knew about cell scams. Then, we asked them how they had dealt with scammers. We asked, "From your point of view, what makes a mobile scam?" Mobile fraud has always been connected to users and workers "stealing money. When asked, "Who are the fraudsters?" individuals mentioned prank calls, criminals, and hackers who could "steal money from their phone." In addition, "How do they commit fraud?" We asked those who claimed that fraudsters were already aware of them where they believed the information came from. People who fell for the hoax believed that a telco employee, a bank employee, or a representative of Pakistan's National Database and Registration Authority (NADRA) had provided information to the hackers. Some people thought that the scams got the information they needed from the victim's friends and family, who may have had bad feelings toward the victim and knew things about them that made them vulnerable, like the victim's parents or husband were away. Some scam victims thought the scammers just randomly picked numbers because they didn't know anything about them when they talked to them. Some people said in their answers that the scammers were hackers who stole people's personal information from their friends and YouTube videos using the software. One person who fell for a scam thought the ticket she filled out at a mall to enter a lucky draw gave scammers information about her. One of the people who was hurt thought it might have been spread through her social media sites.

The cops said that the level of intelligence of scammers was different. Some were well-organized and tried to make money while things were going well. Others, called "copycats," were not as smart. Based on the people the FIA has caught, fraudsters work alone (like a street vendor making fake calls) and in groups (like a complicated plan to make illegal VOIP and fake phone calls). The PTA asserts that when a victim responds to one of these con artists, the con artists share the victim's contact information with other gang members and then spread false information. When they pass calls from one member to another, gang members pretend to be other gang members.

In conversations, more guys than women talked about mobile fraud. They talked about their and people's lives in their social networks. "There are also phone scams," a man (Victim 61) said as an example. Fraud can happen when someone sends you a message that says something like, "You will get money through this scheme." Also, a few people have told me that they have gotten calls about a common bank scam that

is going on right now. Women who couldn't read or write well were more likely to only talk about their experiences with scams. A member named "Victim 12" said there are different kinds of scams. I can only remember falling for one kind of smartphone scam. These differences show that women don't have the same access to information as men.

3.5.2 Types of fraud that people reported

The participants discussed four fundamental categories of mobile fraud: lucky draw, BISP fraud 2, bank fraud, and damsel in distress.

Lucky Draw (n=39; 55%). Con artists use texts or phone calls to tell their victims they have won a prize, usually a car, gold, or money. Scammers trick people into thinking they've won so they can send them the money they need to claim the win. Then, they ask for a fee or information about their bank account. The con artists pretend to be from a phone company or a well-known game show that gives out prizes by drawing names.

People who reported this scam had a wide range of income, education, and reading skills, which shows that it is meant for a wide range of people. Officials say that people who fell for lucky draw scams came from all walks of life, including the rich and the poor.

Fraud BISP (n=6; 9%). Fraudsters are going after people who get money from the Benazir Income Support Program (BISP). They do this by giving them SMS messages that look like they came from the Pakistani government. Figure 1 shows both an example of a real BISP message from the government and an example of a BISP scam message. Con artists often target low-income people because BISP programs are meant to help people with low salaries. Officials say that lower-income people were more likely to report BISP scams. From our study, we found that four of the six people who fell for the BISP scam had not even finished high school. The other two contestants had some college experience. The people who fell for the BISP scam say they called the number given to them in the fake SMS because they wanted to join the BISP plan and make money from it.

Bank Fraud (n=9; 13%). To trick or coerce victims into providing their financial information so that fraudsters can use it to steal money, this type of fraud involves impersonating bank personnel, members of the military, or other government employees. Victims of bank fraud alleged that the con artist tricked them into providing information over a single phone call. Some of these victims responded that they couldn't take the time to stop and consider their options and choose a more thoughtful course of action when asked why they fell for the con. The strategy of establishing urgency is one that fraudsters frequently use to sway their victims' judgment.

Damsel in Need (n = 5; 7%). In this type of scam, con artists pretend to be a woman who needs help (like a girl in the hospital who doesn't have any money) and ask for money in exchange, promising to pay it back. Most of the time, this trick is played on men. Based on the numbers we have; five men fell for this scam. Most of the frauds in our sample were the four types we just talked about. Participants said they had also been fooled by other types of fraud, such as financial fraud, pyramid schemes, extortion, and other forms of pressure, such as fake police officers.

3.6 Findings: fraud strategies reported on mobile devices in Pakistan

Mobile fraud assaults adhere to the same four steps as any other social engineering attack: planning, getting to know the victims, attacking, and bringing the attack to a close. Even while the basic pattern of attack remains the same, attackers have various strategies and methods at their disposal depending on the situation. It is essential to have this level of understanding to devise suitable defence strategies for the situation. We provide an overview of con artists' methods to manipulate individuals into giving them money through deception.

3.6.1 Step 1: Plan and gather resources.

We found that scammers used three ways to make their victims think they were real.

Masking phone number. Calls or texts from people you don't know that try to sell you something are more likely to be misunderstood or ignored. Fraudsters can make fake calls and texts look real in the future if they can get their victims to add a phone number to their phone's contacts list. One lucky person reported being duped into saving a number resembling a common 3-digit telco short code. The injured party revealed what had transpired.

Instead of a short code, the call was made from a standard mobile number. The person received a message that said, " You have won a prize, and to claim it, you must adhere to my instructions.," in a manner that sounded typical of a phone operator. They first asked about your phone model, so we gave them information about ours. Then one told us to push a few buttons on our phones repeatedly. They told us that if we pressed one of those buttons, a phone number would be sent to us, but I can't remember what they were. We finally did what they said and saved their number as the short code 333. Also, they told us not to cut off the connection. We didn't know these things until we fell for a trick. (Victim 1)

Getting SIM cards that are hard to track down. [. "Con artists in rural Pakistan get people with low incomes and no education to leave their thumbprints on BVS devices in exchange for a few hundred rupees," they said. Because they can't read or write, these men and women don't know what could happen if they give their thumbprints, like their SIM cards being used for illegal things. They thought that con artists were taking advantage of the fact that telecom companies were putting BVS devices in small shops and franchises all over the country (to boost subscriptions). Customers are tricked into giving their fingerprints more than once when they buy SIM cards. They are told that the network is down and that they must repeat the fingerprint registration process. Instead, they check the SIM card so the customer can't see it. What these FIA officials said was supported by a news release from the FIA. Even though PTA warns users about these scams and gives members a way to check for SIMs linked to their names, low- income, illiterate people from rural areas who don't have cell phones may never think to use this service.

3.6.2 Step 2: The next step is to talk to the victims. After the first contact, scammers use various methods to prove their authority or legitimacy and gain the victim's trust. They then use this to force the victim to do what they want. We will now talk about the lures they used to get people to come to them.

- **Using personal information and unique phone numbers.** Some victims said they got a text message or phone call from a short code or a bank number. Most people who participated in bank fraud thought the scammer was a bank employee because they called from a helpline number and knew the victim's name and ID card number. Scammers use people's trust to get their ATM PINs or debit card numbers.

When I picked up the phone, it seemed like someone from XYZ Bank was on the other end. They told me my name and went over some of the most important facts about me again. They said, "Our connection is down, so we are having trouble with the ATMs." Please give me your personal identification number (PIN) and the number for your bank account. I had no reason to think there was a problem, and it was easy to get their phone number, so I gave it to them. (Victim 2)

Another victim revealed that the con artist thoroughly knew his phone activities.

I remember getting a phone call that told me I had won 30,000 PKR in a raffle at one point. I didn't believe it at first, but when the person told me everything, I had no choice but to agree. This SIM card, the number on my ID card, and all my other SIM cards have information about who I am, what I do on the phone, and other things. Because of this, I was sure that the company would be reliable (Victim 3)

Some people fell for the scammers because they acted like bankers or government officials speaking English. People trust banks and their workers more when they talk to them in person. Scammers take advantage of the fact that their victims believe them when they say they are from a bank.

3.6.3 Step 3: Stealing Money Fraudsters steal money by attacking their victims after gathering the tools they need to do so and using techniques to get the victims to help them and prove their legitimacy.

Through over the counter (OTC). We discovered that scammers took advantage of social norms and over-the-counter transactions at shops where mobile money agents worked. Many scammed people said they were tricked into sending money to agents. In general, they sent more money through OTC than phone top-ups, which will be discussed below. Agents said that over the counter (OTC) fraud was popular, and people didn't use mobile wallets often. From what scam victims told us, we figured out how con artists do these stepCon artists tell their victims that they have won a prize for them, but they are told not to tell their local mobile money company. The person is told to hand the phone to the agent instead. People who can't read or write often call an agent to explain a deal that might be hard for them to understand or explain. After noting what is needed, the agent returns the phones. To avoid getting caught, the con artist tells the agent they know the target. They also say they will give the victim money, which will be sent to their accounts. When a customer offers to pay, the salesman uses his mobile money account float to put the money in the customer's account. The customer then says that they came to get their prizes, not to pay. When the client doesn't take responsibility and pay the agency, the agent, like Agent 14, may lose money.

Two people parked their motorbikes here and asked the owner for PKR 36,000. When his brother asked who was on the other end of the line, the man said it was his brother and gave the person's name and phone number. They asked for PKR 36,000 in cash, and when we gave it to them, they said they would give us PKR 80,000 and showed us a text message that said, "Benazir income support." They also showed us the text message. As soon as I read the message, I told them it was a fake. He told her, "I didn't tell you to

send money." After calling 1-5, the police came, and soon after, people started gathering in front of my business. When our PKR 36,000 wasn't returned, the cops asked us, "Why would you send money before getting cash?" First, you should get money, and then you can send money. (Victim 4)

By topping up a cell phone. Fraudsters frequently request mobile phone and over-the-countertop-up card serial numbers. Three victims of the fraud have reported being instructed to destroy the scratch cards and told that the con artists were watching their every move. When we asked the three victims if the con artist had told them explicitly that they could see their movements, they all said that even though the con artist hadn't said it, they could tell by the way the con artist spoke that they were being watched. Since top-ups occur more frequently in rural areas where cards can be purchased at convenience stores, it is essential to distinguish them from schemes involving larger amounts of money. When the victim exhausted all the scratch cards at a rural store, the proprietor accompanied them to another location to purchase more. The con artist demanded more than most individuals were prepared to pay for top-up cards. Ultimately, the victim purchased all remaining playing cards, causing the store to run out. However, the merchant showed no concern for this peculiar request. Since mobile money stores use float to handle these transactions, we don't think small businesses are as good at finding fraud victims and keeping their money safe. Because of this, these places may help victims instead of telling customers.

From bank account. Fraudsters use debit card numbers, usernames, and one-time passwords (OTPs) for mobile banking, ATM PINs, and more to steal money from banks. The goal is to finally get into the mobile bank accounts of the victims and empty them. Unless the victim has a small amount of money in their account, bank fraud usually causes more money to be lost than other scams. When fraudsters force educated bank customers to give up their PIN codes for ATMs or mobile banking, login information, or the last four digits of their debit or ATM cards, etc., the customers try to fight back at first. But sometimes, victims get the importance of a piece of information wrong and give it out. For example, Victim 7 lost money because she didn't give out her ATM PIN, but she did give out the last four digits of her ATM card number.

They asked for the PIN for the ATM. I made a promise not to tell anyone. "Okay, let's just switch the last four numbers of your account number," they said. I explained what had happened. After a while, the bank told me they had taken 11,000 Pakistani rupees from my account. I called my bank as soon as I could. Someone took $11,000 from your account and told your bank about it. (Victim 6)

Strategy: Changing what's needed based on who the customer is when the victim told the con artist that they didn't have enough money, the con artist would sometimes change their demands to take what the victim did have. One victim said, "I didn't have as much money at home as the scammer asked for, So I told them I didn't have PKR 50,000, which is the truth. "Okay, you can pay what you can," they said. " (Victim 7)

Demanding payments in installments is a tactic fraudsters are said to have asked victims for multiple payments to cover different costs, like shipping fees and duties at the port to be paid. Fraudsters tell their victims to pay money to a different store each time to avoid getting caught, recognized, or warned. Both the agents and the scammed people said this was the case. The agents said that fraudsters could steal more

money in fewer transactions if they take advantage of ecosystem improvements and raise the limits on OTC transactions. Someone said that they sent 13,000 PKR in several over-the-counter trades.

We sent in parts PKR 13,000 We probably sent PKR 2,000 through Easypaisa first, then PKR 5,000 and PKR 6,000. We didn't like being scammed at the time, but we felt worse about it afterwards. We joked about how someone else tricked us into sending PKR 13,000 to someone else. We sent both our own money and money from home. We even borrowed $13,000 from a neighbor and sent it through Easypaisa to cover the rest. (Victim 8)

3.6.4 Step 4: The attacks stop, and the victims realize what's going on

We describe how fraudsters cut off connections without raising suspicions in this section. We also describe the events and data sources that caused the victims to become aware of fraud.

Attack cessation: postponing understanding. Scammers use phrases like "We are making lists" and "It will be there by morning" to keep their victims from acting. In the interim, the con artists hide their tracks by withdrawing cash from an OTC, turning off their phones, or using scratch-off numbers provided by the police. Someone said they had to wait longer for the reward after touching the thing.

They claimed that your home was becoming close by. We anticipated they wouldn't need more than one or two hours to complete. When it was approaching midnight, we worried that we had run out of time and that the whole thing was a ruse as we continued to wait. Then we speculated that they might visit us in the morning. We remained there till dawn. Nothing new emerged the following day. (Victim 9)

We were supposedly getting near to your place, they said. They were supposed to be done in over an hour or two. As the clock drew nearer to midnight, we worried that time had run out and the whole affair was a ruse. We then anticipated that they might pay us a dawn visit. We continued to wait till sunrise. The following day, nothing happened.

Attack over: Cut off communication Con artists using the lucky draw scam usually tell their targets to wait a few days before receiving their prizes. When the allotted time is up, the victim tries to phone the con artist but gets a disconnected number. At that point, the victims realize they have been cheated. Victims often figure out what's happening when the scammers' cell phones stop working. One victim was told by the con artists that they would be there in a few hours, but it took them a whole day to bring her prize car. After that, they cut the call short. When I tried to call them again, the number I had was wrong. The number stopped after that. (Victim 18)

Realization of being unable to talk to the person who did the crime. They come to the same conclusion when they call the fraudster's number and hear pre-recorded noises. The people in the group began to talk to each other.

When I called the number, I couldn't get through. I called the number on the message after a month. So I thought that the person on the other end was making a recording. We are not being spoken to. Still, it looks almost like someone is talking to you. If one is like us, one almost believes it. He talks when I don't. These people are funny, but it almost looks like I'm talking directly to him. They answer in the right way.

I didn't say anything, but they did. I then asked some people who lived nearby. Some of them had also been through this. Then I decided it was a trick. I put 500 PKR into my account. (Victim 10)

Realization: When they asked for more money again. Others don't say anything. After all, they think the caller is trying to scam them because they keep asking for money. " The moment I handed him “the numbers on the top-up card, I asked, " What happened to my prize?" Brother demanded a 500-rupee card, not 300. Soon I got the impression that he was riding me. I told him farewell and immediately ended the conversation. (Victim 11)

Realization: Following bank notice. Even if the fraudsters used the bank's hotline or short codes and had basic information, the victims of their schemes didn't recognize anything was wrong until it was too late. The victim would call their bank to inquire about transactions they had not performed after receiving a notice from their bank. The bank staff would then inform the consumer that they had been duped and that the bank does not conduct this check by requesting a customer's PIN. One victim called her bank to request that the transactions cease after realizing she had given her PIN in error. She chose not to dial the helpline. She dialed the local bank branch instead. She no longer believed it because she had already been asked for information via the helpline. Other victims whose accounts were business. Use the discovered the issue too late include: Because I gave out my PIN, my bank stopped my account so that I couldn't do any more business. (Victim 12)

Even some victims called the bank's helpdesk and inquired as to why they did so. Then, when I visited the bank, I asked the staff, "Is this your number?" while displaying the phone's screen to them. They said, "Yes, that's our number." How can anyone be sure when your phone number is so plainly visible? I inquired (about anything). The number would be assumed to be the banks by all. (Victim 13)

Even though most of the people who answered said they had learned from their mistakes and would be more careful with similar messages in the future—some even deleted them—this was not true for everyone. A participant from a rural area who had only finished the fifth grade couldn't figure out how to apply the warning to a scam that hadn't been found yet. Even though people she knew warned her about certain types of fraud, she kept talking to the con artists. However, agents, coworkers, and neighbors stopped her from becoming a victim.

4. Results

This section covers the direct encounters that victims have with mobile money agents and members of their social network (such as family, friends, and coworkers), as well as the roles that these persons play in mobile scams. In addition, we discuss the roles that mobile money agents and members of social networks play in mobile scams. We also talk about the different kinds of mobile scams that can happen. The part of the agents in figuring out what the customers will do. Agents know how often their regular customers make deals and add money to their accounts. Using this data, they can find patterns of unusual customer behavior. If a customer has reason to think that another person is a scammer, they should be told not to give that person any money. We asked the salespeople about the average number of people who visited each business daily. All the workers know well over half of the people who come in, and they all agree that most of the people who come in are men. When working with customers who come back

repeatedly, customer service reps look at the customers' past transactions and how they act to spot scams and other problems. Agents can find out how much money a customer usually adds to their account, what kind of link they have (prepaid or post-paid), and which mobile money networks they use to send money to their loved ones. Agents may sometimes think that people are giving money to people trying to steal it, but this is not usually the case. If a customer is suspected of being a victim of fraud, the company will tell them not to give out the number written on their top-up card. If they do, the customer will lose all their money. Even so, the scammers make their victims keep the name of the person who will get the money from them a secret from the mobile money agent. They wouldn't let their victims say anything about themselves. When regular customers suddenly want a bigger top-up than normal, customer service reps warn them to be wary of award schemes that are not what they seem to be.

Response of victims to agent warnings Agents says that customers' reactions to their warnings vary from one to the next. To stop fraud, agents refuse to take part in any shady deals. Agents say that when fraudsters promise huge amounts of money, it's hard to get people to stop because they believe what the fraudsters are saying. Clients keep sending money to the scammer in the hopes that this will be the last time they send money and that they will eventually get the money they were promised. So that the mobile money agent doesn't notice the scam and tries to stop it, the victims are told to do each transaction at a different store. Most of their customers listened to their advice and didn't send money, say agents who have worked with them. It shows that the customers' trust in the agents helps to keep them safe. This is why con artists tell people not to buy more than one thing at the same store. A store owner explained what was going on. “People who know you well have a lot of respect for you. But if they aren't, you can still tell them and let them decide. (Agent 14)

They don't quit [sending money], according to another agent who shared his experience with clients who refuse to give money. If I prevent people from sending me money, they quit my store and visit other stores. They must send money no matter what. (Victim 15)

According to the account of one victim, she sent money even after receiving a warning from an agent not to do so because she believed that she would receive a greater amount.

Then, I asked him to do something for me while in the mobile agent shop. But he [the agent] warned me it would be wrong to do it for a prize. That could be a trick. Then I said that I was happy. I want to finish the deal. Why should I send 14,000 Pakistani rupees when I already have money saved? I thought about it for a while. In addition to getting much more back. (Victim 16).

Facilitators for compliance with scams. Both the agents and the victims have reported that customers may sometimes come to the office of the mobile money agent in pairs to complete their transactions. This shows that individuals closest to the victims cannot identify deceit when it is perpetrated against them. It was alleged that a couple begged one of the agents for money so that they could participate in a tournament. They chose to send the funds despite the agent's advice. They enquired whether it would be possible to return the item after returning home. Women have admitted to buying top-up cards for other women, buying the cards themselves, or providing other women with cash so they may pay off scammers. A woman confessed that she had agreed to help a con artist in exchange for compensation from a coworker.

One of my friends stole something once. Sister, I recently got a letter telling me I had won a PKR 5 lac prize," she said. For the deal to go through, I must send PKR 3000. He asked, "What do you want to do?" I spoke louder. She said we must give them 3000 rupees to put on their phones. I told him, "OK." I'm on your side. You can count on me to help you get it. She asked, "Could you please give them the cell phone top-up?" It is not possible in this village. I told a boy over the phone to get his bike. He drove me to the store so I could buy a phone to recharge during my break. When I returned, I had PKR 1,000 worth of top- up cards with me. Only this many were left. She kept sending them the rest of the money. (Non-Victim 6)

Someone asked a friend about a fake letter, and someone else was told how to answer. At first, it was hard for me to understand. I didn't understand it or agree with it. My brother lived near where I did. He couldn't believe I had done it when I told him about it. Then I said they were scam artists." (Victim 51)

Restrictions on the observance of cons. Most people who were told to talk to a coworker, a merchant, or someone who could read better than them could avoid falling for a scam or responding to a fake letter. One woman remembers getting a phone call telling her she had won a prize and could get it at a certain place. She decided that she and her sister-in-law, who doesn't know how to read or write, should talk to a college student. The student told them not to act that way, which stopped other people from taking advantage of them.

Someone once called me and told me that someone was talking. Your phone number gave you a gold award and 5 lac rupees. Then, my sister-in-law and I chose to take the award because we thought it would be easy to win. My sister-in-law hasn't gone to college. They told us to get the prize at the place they told us. We travelled. We started to wonder if it was a joke and what would happen if we were scammed while travelling. A young woman who looked like a college student was sitting down. We told her what was going on when we talked to her. She said, "Aunty, I hope you don't mind, but you shouldn't do that." Scams are common in the world today. There could be some problems. So, we went back. (Non-Victim1)

I got an email from Benazir Income Support about what they do. The price ranges from 25,000 rupees to 30,000 rupees. When I got the money, it made me very happy. I didn't think about how I got it, why I got it, or what would happen after that. The next day, I told my coworkers what happened, and they asked how it could have happened since I'm not a widow and don't meet the other requirements. I told them that I didn't meet any of the criteria. I have been told to call this number because they want money from me. Everyone told her to stop, "Sister, please don't do this." This is a way to trick people. This is so common now that it almost always happens. They steal money from other people by not being honest. In every way, they lied to them. We don't know how to carry out the tasks that are expected of us. Since we live in a high-tech world, these scams are done with high-tech tools. After that, I couldn't see it anymore. I thought it was impossible for four or five different women to all be wrong." (Non-Victim 6)

People talked about taking out loans to send money to con artists and getting a warning from the lender. They told me to use Easypaisa to send money. I didn't even have 5000 PKR. I thought about asking a friend for $3,000 and sending it. I needed 3000 points, so I told my friend, "Your brother has won a prize." I questioned, "Are you crazy?" I talked to a person I knew. There is nothing like that. What did you do afterwards? Two or three other people I talked to also agreed it was a fake.

Table 4.1 Mobile money users' opinions

cc	Why using mobile money services is a good idea	SD	D	U	A	SA	Mean
1	It makes sending and receiving money simple for anyone with a mobile phone or access to a mobile money agent.	0.3	1.2	2.7	24.1	71.4	4.65
2	More reliable than moving money in person.	0.4	1.1	6.3	31.4	61.6	4.49
3	The use of mobile money saves time.	1	1	6.7	34.2	56.8	4.034
4	You can trust mobile money services.	0.4	3.3	10.3	33.5	52.2	4.08
5	Better and faster deals on the market.	0.8	2.3	11.3	38.2	47.6	4.26
6	Many more people will be able to use banking services better.	0.6	1.5	15.8	33.4	48.2	4.33
7	Costs and delays related to opening, running, and keeping bank accounts are reduced.	0.7	6.5	16.1	31.8	44.3	4.12
8	Because more people save and spend with mobile money, the economy grows and gets better.	1	5.2	18.4	33.4	41.6	3.91
9	It offers many different services, like mobile banking, mobile payments, mobile financial services, and exchange money.	1.3	4.5	18.4	37.2	38.3	4.55
10	It helps people who don't have bank accounts live better.	2.3	6.7	19.9	34.4	36.4	3.95
11	It increases the number of people who use banks and opens new markets cheaply.	0.3	2.4	8.8	33.3	35.2	4.05

SD—Strongly Disagree, D—Disagree, U—Uncertain, A—Agree, and SA—Strongly Agree, M = Mean, Findings

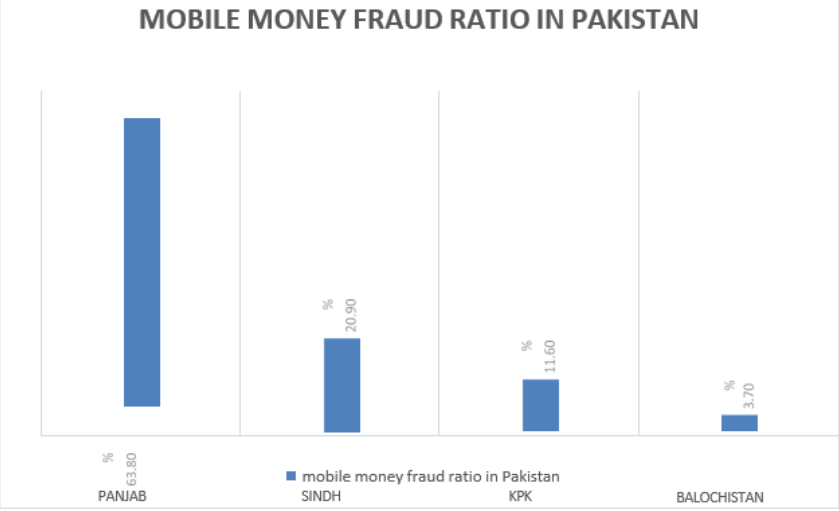

Figure 4.1 Mobile money fraud graph of Pakistan

This study shows that frauds hurt more than just the people who are directly affected and for as long as the fraud lasts. In the long run, these dishonest interactions hurt how people feel about services, cost agents money, and put CNIC users in danger because fraudsters are using their SIM cards. We'll talk about these below.

4.1.1 About victims we noticed two different sorts of behavior changes in victims.

Avoidance.

Some of the victims said they didn't answer any letters that seemed suspicious. Some users said they deleted messages from their service providers because they couldn't distinguish between real and fake messages. "At this point, we no longer believe [these messages] (laughs). We no longer trust Zong because the texts you get from them are fake. Now, when we get a call or text, we put the phone down and delete the message". (Victim 14)

Fall of faith in services. Others explained that they stopped using it because they had lost faith in their financial institution, mobile money service provider, or telecom provider because of fraud. Although I have a bank account, I rarely utilize it since I am too nervous to go into the bank. It's no longer plausible to me. I'm sorry that my clumsiness and confusion caused so much bother. (Appellant 71) For fear of having his account hacked and losing all his money, one of the victims set up a mobile money account but never used it or downloaded the wallet software.

An Easypaisa account is what I have, but I haven't downloaded the app yet. Telenor is for me. Because I thought it would be duplicate and fake software, I withdrew the 2,000 or 3,000 rupees I had initially put in my wallet. I lost all trust in others after being taken advantage of. I'm also concerned that someone might break in and take it if I put money in my wallet. (Victim 24)

4.2 Discovering patterns of (non)reporting attitudes.

Except for a list of mobile phones that have been prohibited because of customer complaints, the PTA claims it doesn't keep track of complaints. An official claimed that even if there had been such a database, consumer protection laws would have prevented access to it. The FIA's reports lumped financial fraud, identity theft, and other crimes together under the term "cybercrime" and didn't say anything about the race or location of the most susceptible groups. So, we looked at how fraud victims felt and thought about reporting. We found problems with their knowledge and understanding of the reporting process, their reluctance to report because of sociocultural factors, and their hopes after reporting.

4.2.1 Lack of knowledge of the proper reporting authorities

Most of the time, when people in Pakistan talked about problems with reporting scams, they said that phone users didn't know who to call or how to do it. Scams that involve money and happen over the phone or SMS should be reported to the Pakistan Telecommunication Authority (PTA), which is the government agency in Pakistan that oversees the telecommunications business. The PTA sends these files to the Federal Investigation Agency's (FIA) National Response Center for Cyber Crime (NR3C). The NR3C has national power, which includes the ability to look for and catch thieves who, among other things, commit

crimes using information and communication technologies (ICTs). Users are urged to use the helplines and email addresses that the PTA has given them to report any calls or SMS texts they could not make or send. Our qualitative study showed that 35 of the 72 victims, including 29 men and 6 women, did not talk about any scams. Only 16 people, 11 men and 5 women from cities told their phone companies, banks, local police offices, and the FIA about the scams. Both rural and urban places had people who were killed. Only 22% of all crime victims are counted in this number. Even if they had told PTA about a scam, most of the people who were scammed still didn't know about it, so the fact that they didn't know how to tell PTA about it wasn't a big deal.

Reasons, why frauds are not reported Participants' explanations for not reporting scams varied widely. One of these factors is hampering reports from the public. Victims typically reported being accosted by police officials at the station, who then begged for donations "to go catch the criminals from other cities." When losses were below a particular threshold, say PKR 5000, people began to question whether it was worthwhile to report them. Because mobile-based financial scams aren't reported as often as they should be, it's hard to know how common they are or how much money they cost. "Who reports a scam of PKR 2,500? It's not necessary to report. It's not a lot of money. The amount of money the police want as a bribe is PKR 2500." (Victim 1)

Unsatisfactory reporting results. After reporting a scam, those who lost money should get their money back. The FIA employees we talked to said that criminal gangs usually do scams, and there are few chances of getting the money back. The mismatch between what the victims thought would happen and what happened is why they don't tell anyone. "[I: Why didn't you tell anyone?" someone asked. First, just 3000 rupees was a tiny sum. Second, I would have informed them if I had known that visiting the police station would produce positive results. But you are already familiar with the conditions in our police stations. I didn't tell anyone because I thought it wouldn't help. (2) Victim So that more crimes don't happen, and more people don't fall for scams, FIA officials told users to (a) understand how unlikely it is to get money back and how dangerous it is to do iffy transactions and (b) think about reporting.

Someone else is the SIM Owner. Pakistan, as previously indicated, requires SIM verification via biometrics. However, earlier studies have shown that phone users frequently lack SIM ownership. Since of this, victims of mobile-based financial theft felt they could not report the scam since their SIM card was not registered in their name. Only the person whose name the number is registered under may seek action against this. Back then, I lacked a CNIC. My father's name was on the number. (Victim 15)

We lacked proof of fraud or harboring guilt over fraud. Many victims thought they were to blame for falling victim to fraud and that nothing should be reported. Some victims said that the lack of proof prevented them from coming forward. One voice phishing victim claimed that because he lacked documentation because everything happened over the phone, he chose not to disclose it. Another victim chose not to report it because she thought it was her responsibility to fall for the trick. "No, because we were duped through no fault of our own and did not think it appropriate to report. Therefore, there was no reason to report. We should report what? How would we describe what happened to someone? The number we had phoned prevented us from making a report. Therefore, we did not. We called it back, but it didn't answer. No one was grabbing it. (Victim 14)

Victims with College Degrees Feel Embarrassed. We discovered educated respondents who, for fear of appearing silly in front of other people, either did not report such frauds or, if they didn't know how to do it, they didn't ask anyone in their group of friends for help. As I already said, I told a friend, "I didn't report, no," and she scolded me. I was afraid that if I told someone else, they would say that I did this even though I have a lot of education. I was embarrassed because I began to doubt the usefulness of education if people kept falling for such scams. (Victim 62)

4.2.2 Analysis of gender differences in non-reporting

There were clear differences between how men and women reported. Women said that they didn't report or even talk about theft because they couldn't get to it easily, didn't want to hurt their name or their family's name, or didn't want to hear criticism from male family members. Women usually don't report fraud because they trust their male family members to tell the right people and think fraud should be reported at police offices, which they find hard to go to alone because they are afraid of being harassed and for their safety. When women go to the FIA office or a police station to report abuse or extortion, they often go with male family members. This means that family members need to know ahead of time about every event that needs to be recorded, so they can blame women for making bad choices. According to several of our female respondents, they have never told their relatives about these instances since, as was also found in an earlier study, men already perceive women as more trusting and susceptible to such schemes. No, guys think women are foolish in any case and are easily duped, a participant said. That is the reason I didn't tell my husband about it. When I told my family about it, they told me that I shouldn't believe them since such things are scams. (Non-Victim 1)

Mobility and Reporting. Another female responder decided not to report due to a lack of knowledge about reporting and mobility issues. “Report?! I'm not sure. There isn't a man in our home. We used to be cautious about running around and avoided reporting. What should we report, we wondered? For instance, where would women go to report? We decided against going [for reporting]. (Cause 14). Another female participant believed that reporting would lead to further financial loss and humiliation.

True, I did not file a report. It seemed pointless to me. Where might a girl go if she needed to speak up? The situation worsens when you go to the police station to file a report and the staff takes half of the money you lost in payments. (Victim 29)

Concern over the likelihood of adverse effects. One woman said she didn't tell her husband something because she was afraid, he would beat her, take her phone, and steal her money if she called random people. No, I didn't think about writing or telling anyone else about it. I'm telling you this so you might be able to help us somehow. This thief took all my money and ran away. I haven't told my partner in over two and a half years. He would have broken my legs if I had told him how much money I had given the con artist. He would have told me why I should have talked with the con artist on the phone and believed him. He was going to take my phone from me. Because of this, I chose not to report it. I chose not to tell anyone because it would have made things worse. I still experience goosebumps. I didn't tell anyone. I told myself that the money would never be seen again. (Victim 22)

Social Circle Response. Female friends and members of their social circle feel comfortable discussing these topics with them. One woman claimed that while she told her friends about what happened, she kept it from her family. Then, her friends warned her not to believe such calls and informed her of frauds they had learned about.

I told my friends, "No" How could I have told anyone at home after receiving such abuse? Then they provided actual fraud cases. However, I knew of frauds involving Benazir Support but not Jeeto Pakistan.

I had no idea that someone would contact me from a short number (a "short code"), identify myself as me, and inquire about my availability after my lesson. The conversation appears to be about business as a result. (Victim 62)

An Embarrassment to the Family. One woman explained that her family does not file a report because they believe going to the police officer will make them feel ashamed.

Sister, tell me where a poor person should go and what they should do. We have a hard time keeping our money in order. In our group of friends, going to a police station is bad. Since the jealous and extended family members were already talking, we chose not to tell anyone. They wouldn't have said we were ripped off. They would have said they were going to the police station because something strange was happening. (Victim 33).

4.3 Security Concerns with Mobile Payment Systems

Table 4.2 responders' views on the security concerns related to mobile payment systems.

No	Problems with the security of mobile money systems	SD	D	U	A	SA	Mean
1	Identity fraud	8.6	18.2	9.5	28	34.6	3.62
2	Attack on authentication	6.6	18.2	9.5	33	34.4	3.68
3	Attack by phishing	14.7	24.2	10.8	19.6	30.5	3.28
4	malicious attack	6.3	12.6	9.7	21.5	49.7	3.95
5	Attack by smishing	15	22.6	14.4	16.8	32.3	3.31
6	Sharing PIN	7.5	16.3	10.3	32.2	33.4	3.67

SD—Strongly Disagree, D—Disagree, U—Uncertain, A—Agree, and SA—Strongly Agree, M—Mean,

4.3.1 Security features

Confidentiality using Java components is available. The people who used cryptography to ensure that information stays private. (S Marvi et.al 2013) The PKI system and OTP are used to protect privacy. The GSM security system uses the A5 and A8 algorithms to keep things private. Using symmetric key cryptography makes it possible to keep information private. The authors use the RSA encryption technology to keep the information secret. (C Ruan et.al2014) say that DES and ECC are used to protect

privacy. Secrecy is achieved by using RSA and AES. For privacy, Use of end-to-end encryption with added security. When symmetric key cryptography is used, the data is kept secret. The RSA encryption method keeps the information secret. With an asymmetric cryptosystem, you can encrypt data. They were using symmetric key encryption like AES to protect private data. The data is kept secret by encrypting it with asymmetric keys and keeping the key pair in a safe place where only people can access it (Bahrini et,al 2019) say that ECC, a type of asymmetric key cryptography, can be used to protect privacy.

Authentication entails reading the RFID identifier contained within the SIM card. In this procedure, an RFID reader verifies the user's identity by requesting a PIN and account number. The authors used a communicative and controllable platform for authentication. authentication is performed with a QR code or PIN and an NFC-enabled mobile phone. The challenge-response protocol is used for the triple authentication procedure to function. SMS and a secret key are employed for authentication. Using signature methods (DES and ECC) ensured the authenticity of the information. Authentication employs short numerals. (P Kotecha 2018) demonstrate their identities using isomorphic forms.

Integrity To make sure that the data was not changed during the transaction, hash packets were used, and the hash was confirmed. Authors use a secure payer confirmation system and a hidden financial network to ensure integrity. By using QR-Codes, the RSA-Digital signature process ensures integrity. A message authentication code (MAC) in the ciphertext, encrypted with a shared key between the user and the bank and signed with the user's private key, protects the data against unauthorized alteration.

Mutual authentication to verify that both parties are who they claim to be, payment requests are signed with the client's and the merchant's signing keys (digital signatures). Mutual authentication is provided using the RSA-PKI method. Thanks to the RSA digital signature, both parties are verified to be who they claim to be. Both parties' identities are confirmed using identity-based signatures. For mutual authentication, having asymmetric keys, a reliable username, and a strong password would be beneficial. A mobile wallet number and PIN are used for this. Use challenge-response authentication with session keys for authentication. PKI and hidden keys must be used for mutual authentication. Digital signatures are used for authentication. In this procedure, only the person and the bank must provide identification. (D. L. Lavanya, et.al 2021)

Customer anonymity Before or during the transaction, the client does not have to register with the seller or any third parties. This keeps the client's information private. The merchant doesn't know the client's long-term ID, which protects their privacy. The consumer's privacy is assured since all that is needed is the consumer's cellphone number or a short code given by the payment application service provider. So that a customer can stay anonymous, their name is always changing. The client's anonymity is protected by making session and transit details hard to understand. Virtual accounts are used to hide the identities of clients whom the bank has chosen. It uses a hybrid location and payment authentication approach to develop a new way to protect identity, privacy, and confidentiality (Amoah et,al 2020).

Non-Repudiation is protected by the date and the signing key. Their approach uses IBC signatures to ensure non-repudiation. The client's status response, the session key, and the offline PIN are provided as three examples to demonstrate that the client cannot be refuted. The information regarding transactions

was signed using RSA digital signatures. This prevented any transactions from being cancelled in the future. Non-repudiation was guaranteed by hashing the transaction data with the shared key and using signatures to confirm the identity of the true user. Look into the usage of blockchain to exchange and secure patient IoT device information. They use secure NFC storage to create a pair of keys (public and private) for a virtual account, and a private key sign all messages sent during a transaction to ensure that their strategy cannot be challenged (W. Chen & R. Tso 2016).

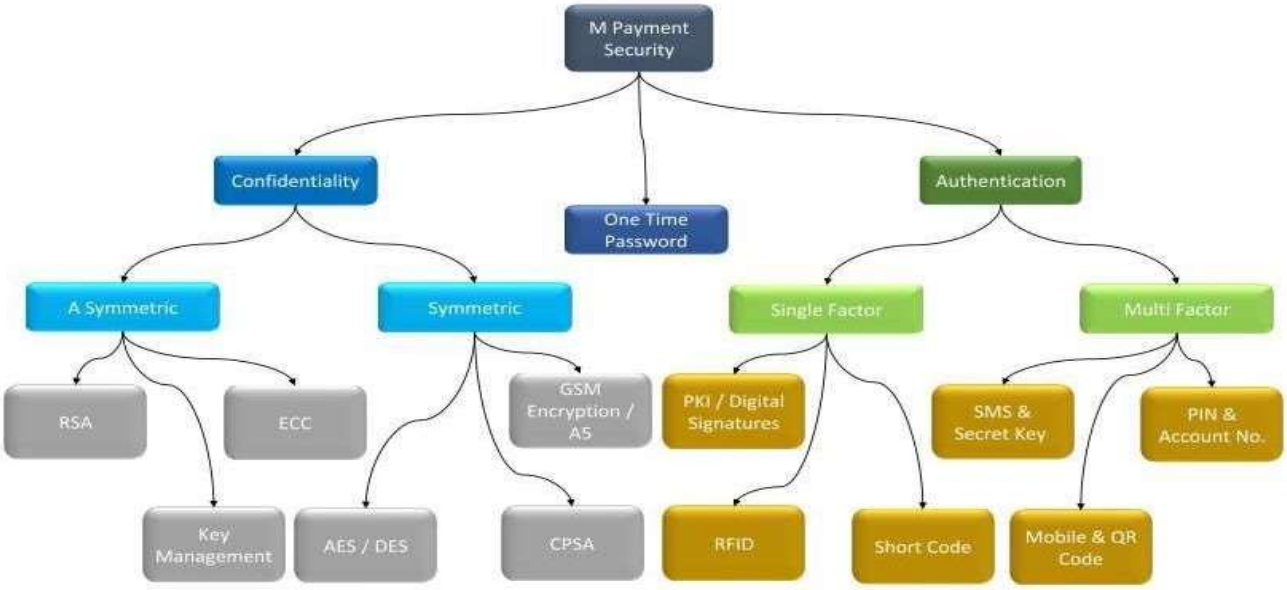

Figure 4.2 M-Payment security

5. Discussion

The research conducted in Pakistan on mobile-based schemes and the emphasis placed on the protection and privacy of users in the disciplines of Human-Computer Interaction (HCI) and Computer-Supported Cooperative Work (CSCW) is an important and well-timed undertaking (F Annan 2017). The creation of technology solutions that can withstand attacks of this sort can be greatly aided by analyzing the experiences of both those who have been scammed and those who have not, mobile money agents, and industry specialists. Investigating these people is a great approach to learn these things (D Chawla 2019).

By interviewing 71 scam victims, 7 victims who were caught off guard, 15 mobile money agents, and 3 experts in the field, participants in the qualitative study were able to gain a thorough understanding of the most common types of fraud patterns prevalent in the region. Participants in the activity were required to engage in conversation with members of the victim community. This theme analysis not only determined who the primary participants in the fraud cycle were, but it also demonstrated how each of these players contributed either positively or negatively to the con artists' schemes. (Bahrini et,al 2019). The study provided a comprehensive breakdown of the ways in which key players assisted con artists. It was also very valuable to learn how victims' feelings and behaviors vary over time, as well as how they feel about reporting scams. This information was gleaned from interviews with victims of fraud. The study was designed around a social engineering scam loop as its foundation from the beginning. The goal of the

research was to gain a better understanding of the methods used by con artists to deceive their victims into handing over sensitive personal information, ceding control, or engaging in other behaviors that are beneficial to the con artists. Con artists resort to these strategies to persuade their victims to perform actions that are beneficial to them, such as parting with money or revealing private information. You will be able to obtain a clear image of how things are progressing and look at each stage of the false process in more detail if you use this method (Amoah et,al 2020).

It is commendable that the research extends beyond a narrow focus on individual crimes and victim stories. The importance of a holistic plan to combat mobile fraud is recognized by the study, which does so by examining the roles and interactions of multiple stakeholders. These stakeholders include law enforcement organizations, mobile money agents, top-up firms, as well as friends and family of the victims. This more holistic perspective elucidates the human resources and social interactions that can be utilized to effectively raise awareness about mobile fraud and counteract it (D Chawla 2019).

One other method that may be used to stimulate thought is to think about what life might be like in a socialist or communist society at each subsequent level of analysis. This is just one example of a technique that can be used. The research investigates the repercussions that these ideological frameworks have for society in addition to the potential solutions that exist inside them. This broadens the scope of the discourse beyond only the technological remedies that are currently available. By including this, we hope to encourage analytical thinking on the part that structural variables play in preventing mobile fraud and the significance of collective responsibility. (F Annan 2017). Overall, the research makes an important contribution to the fields of HCI and CSCW by shedding light on the prevalent forms of mobile fraud in Pakistan and revealing the complex interactions that take place between con artists, their victims, and a wide variety of other stakeholders. Bringing awareness to the most common forms of mobile fraud in Pakistan is one way to attain this goal. (Bahrini et,al 2019). The findings give a basis for the development of technological solutions that put the safety and confidentiality of users at the forefront of their list of priorities. In addition, having a broader perspective on the effects and interconnections of society opens options for addressing mobile fraud prevention through collaborative efforts involving law enforcement, industry actors, and the general community at large as a whole.

6. Conclusion and Recommendations

6.1 Conclusions

This research is based on mobile scams in Pakistan, and now want to talk about what we found. We report on the primary players and types of mobile-based schemes in Pakistan based on qualitative interviews with 78 people (victims and non-victims), 56 males and 22 women, and 18 parties (regulatory officials and mobile money brokers). We discuss our findings and investigate the persons behind these efforts within the context of social engineering. In many types of fraud, we talk about the victims' contacts with scammers, their social networks, and those working at banks. We show how these interactions and social views affect how victims react, what they say back, and what they do when they report. During the life cycle of social engineering, we also find different human resources and intervention places. Our research demonstrates that con artists constantly alter their plots, which are made-up tales intended to persuade

people to trick more and more individuals into falling for them. But the approach is supported by initiatives to lessen losses and increase awareness. We also discuss the various reasons why victims decide not to report an incident, such as the fact that they don't trust the reporting authorities and feel ashamed. After all, the reporting process is hard because they think filing a report will worsen things. We also investigate how, compared to men, women can't learn from each other. After all, they don't talk about or tell what's happening because they're ashamed of their families or afraid of their agencies.

6.2 Recommendations

It proposes formal schooling as a way for collectivist societies to maximize their potential and get around the problems with social warning systems. The help agents get is in the form of knowledge. Some ways to do this are to teach users about the signs of social engineering attacks, new scam schemes, what personal information is, and the risks that come with sharing this information. People with bank accounts or cell phone plans shouldn't be the only ones who can watch or listen to educational videos. It should be easy for everyone to get to, especially those who live in remote places. People who don't have access to the internet are very unlikely to be able to see material that is hosted on the internet. From our point of view, if you want to talk to these customers, you should use an approach that gives the most weight to assets. During social engineering, we figure out which family members, close friends, coworkers, and store workers are "human assets." Mobile money agents can only stop fraud, so people who fall for scams almost always call them first. Even though the level of social capital between agents and their clients is a big factor in how well agents' warnings work, agents can improve the credibility of their warnings when social capital is low by using technological tools that can identify or confirm agents' suspicions of fraudulent communication and give information about the typical traits of common scams and fraudulent numbers. For example, a customer is less likely to listen to an employee's advice if they don't feel like they know that employee. We think it would be a good idea to give customer service reps tools that help customers believe their tips are real and help customers spot and report fake phone numbers or SMS messages. These things should be easy to get. It is possible to teach mobile clients so that they will ask for advice from agents before moving money to someone they don't know and will listen to agent warnings. Because new ways to commit fraud are always considered, the government must keep track of the most common kinds of fraud and the most common ways to commit fraud. Mobile users should be taught (and informed) about the latest developments in mobile fraud using the most up-to-date information. The government runs programs to teach and train people. According to the study that has been done, a big part of whether a victim takes part in a scam is how much they trust the con artist. This makes the victim stop thinking about how real the message is and start thinking about the exchange itself. Because of this, information is processed illogically instead of logically, which makes it harder for the victim to make choices. Our investigation shows how con artists claim to be many kinds of authorities to take advantage of their victims' trust in them. People in the military and other institutions, people working on game shows, and government workers working in different ways to move money make up these officials. Among other things, they will try to be a contact center, say things that only telecom providers, banks, or the government would know, and call from numbers marked as helplines or short codes. The quickest way to break this link is to go after the offline trust’s scammers use to make themselves look legit. This could involve game show hosts giving information at the end of their shows or a government backed advertising effort since the government of Pakistan already uses commercials for health and other

services. (D Chawla 2019). Caller music is another choice for the last few meters of the last mile. During COVID-19, the governments of some developing countries, such as Pakistan, are required to play caller tunes 6. You could use a similar method to tell people about scams, with the focus being on rural areas that don't have access to other media like social media and newspapers.

Redesigning Reporting for Social Influences says that (Vashitha et.al 2019), security and privacy protections should be integrated into developing nations' sociocultural practices, requirements, and behaviours. Family members influence how women use and possess technology in both the Islamic and developing worlds. They rely on men's perceptions regarding their financial and technological reliability. Gender influences how individuals in the Global South approach safety and privacy. We contribute to this study by demonstrating how gender influences how individuals report mobile phone fraud. Women do not report because they fear their family, friends, and their husbands' reactions and judgments. In addition to the possibility of losing money, women fear that their families' reactions to phone calls with outsiders will cause them to lose their independence regarding cell phone use. Women do not report scams because they believe they must do so at a police station, but they cannot get there on their own and must rely on males to transport them. The cultural factors we discovered in our study of how people report indicate that reporting must be altered to protect people's privacy, and the process is simple and unobtrusive. It is crucial to rethink reporting methods and channels so that women can report without leaving the house, asking a male for assistance, enduring harassment, or risking their privacy. With a convenient reporting method, such as a smartphone app, the labour required to do so could be greatly reduced, and the number of reports could potentially increase. After the FIA's website for reporting cybercrimes went live, the number of reports made by women increased dramatically.

Reporting has a bad effect on society right now. But it is important to encourage, praise, and link reporting to the good of society. Being good and responsible means filing reports and helping others do the same. Updated ideas about the benefits of reporting should consider more than just the personal benefits of financial recovery. For example, there may be a desire to protect others. It will be easier to get in touch with the police. There may be good reasons to do this if there are established reporting authorities and protocols (like providing screenshots, SMS, or timestamps), if citizen reports of fraud are taken seriously, and if reporting mechanisms for online and low-value crimes are kept separate from reporting mechanisms for in-person and more serious crimes. The number of con artists and what they say in their letters could be used to make a report. Telecom companies can give scammers the serial numbers of top-up cards, which can then be used to find the user IDs of people who have used these cards. This finding has stopped people from making up more numbers. Crowdsourced algorithms that try to stop spam can't stop these fake phone calls and texts because hackers constantly change their phone numbers. Reporting can help stop fraud by making it harder for scammers to get SIM cards that have been fraudulently verified. These cards are used to send and receive many fake text messages and phone calls. The less likely it is that fraud will happen, the faster a fake SIM card is found and stopped.

References

Adedoyin, A. (2018). Predicting fraud in mobile money transfer (Doctoral dissertation, University of Brighton).

Akomea-Frimpong, I., Andoh, C., Akomea-Frimpong, A., and Dwomoh-Okudzeto, Y. (2019). Control of fraud on mobile money services in Ghana: an exploratory study. Journal of Money Laundering Control, 22(2), 300-317.

Ali, G., Ally Dida, M., and Elikana Sam, A. (2020). Evaluation of key security issues associated with mobile money systems in Uganda. Information, 11(6), 309.

Al-Okaily, M., Rahman, M. S. A., Ali, A., Abu-Shanab, E., and Masa'deh, R. E. (2023). An empirical investigation on acceptance of mobile payment system services in Jordan: extending UTAUT2 model with security and privacy. International Journal of Business Information Systems, 42(1), 123-152.

Amoah, A., Korle, K., and Asiama, R. K. (2020). Mobile money as a financial inclusion instrument: what are the determinants? International journal of social economics, 47(10), 1283-1297.

Annan, F. (2017). Fraud on mobile financial markets: Evidence from a pilot audit study. Available at SSRN 3049376.

Apiors, E. K., and Suzuki, A. (2022). Effects of mobile money education on mobile money usage: Evidence from Ghana. The European Journal of Development Research, 1-28.

Aron, J. (2017). Leapfrogging': A survey of the nature and economic implications of mobile money.

Becher, M., Freiling, F. C., Hoffmann, J., Holz, T., Uellenbeck, S., and Wolf, C. (2011, May). Mobile security catching up? revealing the nuts and bolts of the security of mobile devices. In 2011 IEEE Symposium on Security and Privacy (pp. 96-111). IEEE.

Bergadano, F., Boetti, M., Cogno, F., Costamagna, V., Leone, M., and Evangelisti, M. (2020). A modular framework for mobile security analysis. Information Security Journal: A Global Perspective, 29(5), 220243.

Biryukov, A., and Tikhomirov, S. (2019). Security and privacy of mobile wallet users in Bitcoin, Dash, Monero, and Zcash. Pervasive and Mobile Computing, 59, 101030.

Blumenstock, J. E., Callen, M., Ghani, T., and Koepke, L. (2015, May). Promises and pitfalls of mobile money in Afghanistan: evidence from a randomized control trial. In Proceedings of the Seventh International Conference on Information and Communication Technologies and Development (pp. 1-10).

Bosamia, M. P. (2017, December). Mobile wallet payments recent potential threats and vulnerabilities with its possible security measures. In Proceedings of the 2017 International Conference on Soft Computing and its Engineering Applications (icSoftComp-2017), Changa, India (pp. 1-2).

Bosamia, M., and Patel, D. (2019). Wallet payments recent potential threats and vulnerabilities with its possible security measures. Int. J. Comput. Sci. Eng, 7(1), 810-817.

Botchey, F. E., Qin, Z., and Hughes-Lartey, K. (2020). Mobile money fraud prediction—a cross-case analysis on the efficiency of support vector machines, gradient boosted decision trees, and naïve bayes algorithms. Information, 11(8), 383.

Chale, P., and Mbamba, U. (2015). The role of mobile money services on growth of small and medium enterprises in Tanzania: Evidence from Kinondoni District in Dar es Salaam Region. Business Management Review, 17(1).

Chawla, D., and Joshi, H. (2019). Consumer attitude and intention to adopt mobile wallet in India–An empirical study. International Journal of Bank Marketing.

Das, A., Satija, T., Zilpe, S., Kavya, J., and Kar, N. (2018). A Study of Threat Model on Mobile Wallet Based Payment System. International Journal of Computational Intelligence and IoT, 2(4).

Devi, K., and Indoria, D. (2023, March). Study on the waves of blockchain over the financial sector. In List Forum für Wirtschafts-und Finanzpolitik (pp. 1-21). Berlin/Heidelberg: Springer Berlin Heidelberg.

Di Castri, S. (2013). Mobile money: Enabling regulatory solutions. Available at SSRN 2302726.

Garrouch, K. (2021). Does the reputation of the provider matter? A model explaining the continuance intention of mobile wallet applications. Journal of Decision Systems, 30(2-3), 150-171.

He, C., He, L., Lu, Z., and Li, B. (2023). “I Have to Use My Son’s QR Code to Run the Business”: Unpacking Senior Street Vendors’ Challenges in Mobile Money Collection in China. Proceedings of the ACM on Human-Computer Interaction, 7, 1-28.

He, C., He, L., Lu, Z., and Li, B. (2023). “I Have to Use My Son’s QR Code to Run the Business”: Unpacking Senior Street Vendors’ Challenges in Mobile Money Collection in China. Proceedings of the ACM on Human-Computer Interaction, 7, 1-28.

Ibtasam, S., Mehmood, H., Razaq, L., Webster, J., Yu, S., and Anderson, R. (2017, November). An exploration of smartphone based mobile money applications in Pakistan. In Proceedings of the Ninth International Conference on Information and Communication Technologies and Development (pp. 1-11).

Jakhiya, M., Bishnoi, M. M., and Purohit, H. (2020, February). Emergence and growth of mobile money in modern India: A study on the effect of mobile money. In 2020 Advances in science and engineering technology international conferences (ASET) (pp. 1-10). IEEE.

Joshi, H., and Chawla, D. (2023). Identifying unobserved heterogeneity in mobile wallet adoption–A FIMIX-PLS approach for user segmentation. International Journal of Bank Marketing, 41(1), 210-236.

Kanimozhi, G., and Kamatchi, K. S. (2017). Security aspects of mobile based E wallet. International Journal on Recent and Innovation Trends in Computing and Communication, 5(6), 1223-1228.

Kanimozhi, G., and Kamatchi, K. S. (2017). Security aspects of mobile based E wallet. International Journal on Recent and Innovation Trends in Computing and Communication, 5(6), 1223-1228.

Kapoor, A., Sindwani, R., Goel, M., and Shankar, A. (2022). Mobile wallet adoption intention amid COVID-19 pandemic outbreak: A novel conceptual framework. Computers and Industrial Engineering, 172, 108646.

Khan, I. U., Hameed, Z., and Khan, S. U. (2017). Understanding online banking adoption in a developing country: UTAUT2 with cultural moderators. Journal of Global Information Management (JGIM), 25(1), 43-65.

Kotecha, P. S. (2018). An empirical study of mobile wallets in India. Online Journal of Multidisciplinary Subjects Research Guru, 11(4), 605-611.

Krishna, P. V. (2023). INVESTIGATING THE EFFECTS OF THE METAVERSE ON BUSINESS MODELS. Journal of Advances in Management, 1(01).

Leavitt, N. (2011). Mobile security: finally a serious problem?. Computer, 44(6), 11-14.

Mogaji, E., and Nguyen, N. P. (2022). The dark side of mobile money: Perspectives from an emerging economy. Technological Forecasting and Social Change, 185, 122045.

Mumtaza, Q. M. H., Nabillah, S. I., Amaliya, S., Rosabella, Y., and Hammad, J. A. (2020). Worldwide mobile wallet: A futuristic cashless system. Bulletin of Social Informatics Theory and Application, 4(2), 70-75.

Mustafa, M., Mazhar, N., Asghar, A., Usmani, M. Z., Razaq, L., and Anderson, R. (2019, May). Digital financial needs of micro-entrepreneur women in Pakistan: is mobile money the answer?. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (pp. 1-12).

Nanda, S. K., Panda, S. K., and Dash, M. (2023). Medical supply chain integrated with blockchain and IoT to track the logistics of medical products. Multimedia Tools and Applications, 1-23.

Ndzimakhwe, M., Telukdarie, A., Munien, I., Vermeulen, A., Chude-Okonkwo, U. K., and Philbin, S. P. (2023). A Framework for User-Focused Electronic Health Record System Leveraging Hyperledger Fabric. Information, 14(1), 51.

Omar, A., Sultan, N., Zaman, K., Bibi, N., Wajid, A., and Khan, K. (2011). Customer perception towards online banking services: Empirical evidence from Pakistan. Journal of Internet Banking and Commerce, 16(2).

Razaq, L., Ahmad, T., Ibtasam, S., Ramzan, U., and Mare, S. (2021). " We Even Borrowed Money From Our Neighbor" Understanding Mobile-based Frauds Through Victims' Experiences. Proceedings of the ACM on Human-Computer Interaction, 5(CSCW1), 1-30.

Saranya, A., and Naresh, R. (2021). Efficient mobile security for E health care application in cloud for secure payment using key distribution. Neural Processing Letters, 1-12.

Sasongko, D. T., Handayani, P. W., and Satria, R. (2022). Analysis of factors affecting continuance use intention of the electronic money application in Indonesia. Procedia Computer Science, 197, 42-50.

Shaw, N., Eschenbrenner, B., and Brand, B. M. (2022). Towards a Mobile App Diffusion of Innovations model: A multinational study of mobile wallet adoption. Journal of Retailing and Consumer Services, 64, 102768.

Singh, A., and Kalra, A. (2021). ‘Impact of Mobile Wallets Security on Consumer Attitude towards Use.

Psychology and Education, 58(4), 3140-3146.

Sujith, T. S., Sumathy, D. M., and Anisha, T. (2019). Customer perception towards mobile Wallet among Youth with special reference to Thrissur city. International Journal of Scientific and Engineering Research, Volume10, Issue3.

Tonuchi, J. E. (2020). How to improve mobile money service usage and adoption by Nigerians in the era of covid-19. International Journal of Finance, Insurance and Risk Management, 10(3), 31-52.

Vlčková, J., and Klimková, V. (2023). The digital transformation of Czech healthcare: trends and COVID19 impact. International Journal of Electronic Healthcare, 13(1), 15-32.

Yao, M. L., Chuang, M. C., and Hsu, C. C. (2018). The Kano model analysis of features for mobile security applications. Computers and Security, 78, 336-346.