GO Green Research and Education

Journal of Business and Management Research
ISSN:2958-5074 pISSN:2958-5066
Volume No:3 Issue No:3 (2024)

Exploring Loopholes in the Cellular Industry Contributing to Cyber Financial Crimes: A Qualitative Case Study in Faisalabad, Pakistan

Syed Arshad Ali Rizvi*
Federal Investigating Agency, Pakistan
Izza Mahfooz
Centre for Clinical Psychology, University of The Punjab, Lahore, Pakistan
Syeda Sitara Murtaza
Department of Computer Sciences, University of Agriculture Faisalabad, Pakistan.
Amir Aslam Saggo
Federal Investigating Agency, Pakistan
Corresponding email: alirizvi1540@gmail.com

Abstract

Since the inception of internet use and mobile technologies, the incidences of cyber-financial crimes have also increased. In this study, the authors attempted to explore the prevailing loopholes in the cellular companies and telecom sector. This study was qualitative in exploring the in-depth probing of the loopholes. This study was conducted in the district of Faisalabad of Punjab province, Pakistan, where the investigating agency deployed 16 investigation officers. These 16 officers were interviewed face-to-face using a validated interview guide. Thematic analysis technique was applied to the collected data using Nvivo software. The results of the study are presented under different themes. Results summarized that significant weaknesses exist in regulating and overseeing SIM activation and distribution, allowing unauthorized agents to operate with minimal accountability. Poor biometric verification processes and insufficient record-keeping practices increase the risk of SIM-based fraud, enabling cybercriminals to exploit these gaps. These regulatory gaps and operational weaknesses in the telecommunications sector create risks for branchless banking systems and broader public security. This study suggests implementing stricter controls on franchise operations, enhancing biometric verification standards, and improving data reporting to the Pakistan Telecommunication Authority (PTA) to prevent fraudulent SIM activations and curb cyber financial crimes.

Keywords: cyber crimes, financial crimes, telecommunication, mobile, internet, cellular networks

Introduction

Advances in mobile and internet technologies further emphasize the significance of the cellular industry to modern society, both in personal and professional life. The availability of cellular services has risen in Pakistan, offering easy access to communication and financial services. Pakistan boasts over 140 million cellular subscribers and about 48 million broadband subscribers, who are a prime consumer of the products and services of ICT (Rizvi et al., 2019). The Pakistan cellular industry is expanding due to such factors as the increase in network coverage, subscribers, reduced call charges, and the quality of service (Khalid, 2006). However,

Journal of Business and Management Research
ISSN:2958-5074 pISSN:2958-5066
Volume No:3 Issue No:3 (2024)

Pakistan is lagging on mobile internet subscriptions as only half of the owners of cell devices avail of broadband subscriptions, and 5G requires costly infrastructural adjustments (Iqbal et al., 2021). Mobile broadband growth in Pakistan stabilizes due to factors like cost, literacy, security, and lack of local content, and it needs the harmonious efforts of the government, service providers, and the people (Hanif et al., 2017). Five G technology can help bridge the gap in the unavailability of mobile internet in Pakistan through developing applications like virtual networking, network slicing, and the Internet of Things (IoT) applications for users (Ali et al., 2022). The growth of the cellular sector has brought a range of vulnerabilities that cybercriminals target in efforts to commit various cyber-financial crimes. Such effects have come up mainly through unauthorized financial transactions, identity theft, and fraud cases that have higher impacts on the individual and diminish public confidence in digital and economic systems. Online fraud through digital microloan apps has also been a significant concern in Pakistan. Weak implementation of cyber-laws puts social media users at risk, as reported by Shahzad (2023). The overall increase in cybercrimes with the advent of 4G technology in Pakistan requires enhancing awareness, education, and enforcement of cyberlaws to control this rapidly growing threat, as discussed by Sattar et al. (2018).

This kind of crime has become associated with vulnerabilities within the cellular industry as cyber-financial crimes grow increasingly in strength. The incidence of cybercrime and digital attacks has risen since businesses and societies depend more on computers and internet-based networking (Singh and Bora, 2013). As more people use smart mobile devices, cybercriminals focus on smart phones rather than targeting end-users to financial institutions (Gaumer et al., 2016). Issues of illegal activation of SIM cards, poor regulatory compliance, and unsupervised selling open doors for criminal offenses to manipulate customers to conspire for unauthorized access to sensitive financial information. The lack of suitable data protection mechanisms and inadequate public awareness also contribute to the problem (Gulyamov and Raimberdiyev, 2023). Such issues are more alarming in populous districts like Faisalabad of Pakistan, where fast population growth and heavy demand for cellular services can buckle the entire regulatory framework and may even let criminal activities thrive. Higher urban development has an association of more connections between urban development and crimes (Algahtany and Kumar, 2016). As reliance on the internet has increased in metro cities, cyber

Journal of Business and Management Research
ISSN:2958-5074 pISSN:2958-5066
Volume No:3 Issue No:3 (2024)

crimes have also come into the limelight; awareness is of paramount importance to protect against them (Sharma et al., 2023).

Despite the advantages of mobile and electronic financial services, regulatory solid and operational barriers in the Pakistani cellular industry expose it to a more significant threat of cyber financial crimes. Lack of oversight in SIM card sales, combined with lenient rules for data protection, becomes an open gateway to exploitation by cyber criminals for fraudulent purposes (Rizvi et al., 2024). This study will explore the specific vulnerabilities that exist in the cellular industry in Faisalabad, which result in the perpetration of cyber financial crimes. The qualitative research will attempt to unearth the views of industry stalwarts, law enforcement agencies, and victims on the loopholes so that practical recommendations can be put forward to make regulatory mechanisms more effective and reduce cyber financial crimes.

Methodology

Study area

The aim of this research work is to investigate the Exploring Loopholes in the Cellular Industry Contributing to Cyber Financial Crimes. The collected the data from Faisalabad district, one of the largest cities in the Punjab province (Figure 1). This city is also known as Manchester of Pakistan for its potential in the textile industry and business opportunities. Faisalabad profoundly contributes to economic acceleration at the provincial and national levels. Urbanization in Faisalabad city has positive and negative impacts on the socio-economic conditions of its surrounding rural areas, affecting health, housing structure, education, and economic conditions (Hassan et al., 2023).The special economic zone in Faisalabad directly impacts local citizens, encouraging foreign and domestic finances, employability, business, financial stability, and human capital expansion (Javaid et al., 2023).The provincial government has established a system where Cybercrime investigators of law enforcement agencies work to minimize cyber-enabled financial frauds. These cybercrime investigators are key persons with diversified information about financial crimes and deal with victims of these fraudulent activities. Thus, in this study, those cybercrime Investigators were considered the population and the Key Informants (KI).

Journal of Business and Management Research
ISSN:2958-5074 pISSN:2958-5066
Volume No:3 Issue No:3 (2024)

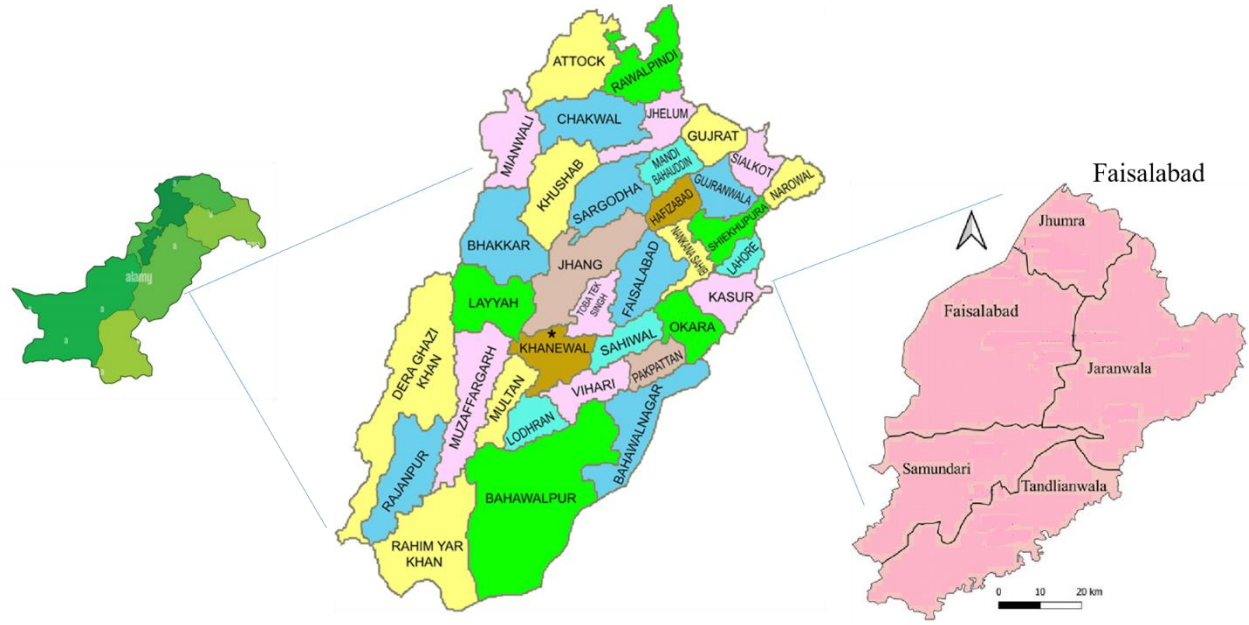

Figure 1. Study area: Faisalabad District.

Population and sample size

16 cybercrime Investigators work in the District of Faisalabad, and all 16 were chosen for this study's sample. In qualitative studies, the sample size is usually small based on the saturation point. Adequate sample size in qualitative research is a matter of judgment and experience, evaluating the quality of the information collected against the uses, the research method, and the research product intended (Sandelowski, 1995). There is no consensus on the exact size of a proper sample in qualitative research, and researchers follow various guidelines to determine the appropriate sample size (Mocănaşu, 2020). In this study, we believe all 16 cybercrime investigators were knowledgeable and could give diverse experiences in dealing with different cyberfinancial crimes. Therefore, researchers preferred selecting all the investigation officers as the case study.

Data collection and analysis

Data were collected using an interview guide that encompasses open-ended questions. Interviews were conducted using face-to-face interview techniques. The responses were noted on the paper and recorded for assistance with data analysis. Collected data were analyzed using a content analysis approach.

Journal of Business and Management Research
ISSN:2958-5074 pISSN:2958-5066
Volume No:3 Issue No:3 (2024)

Ethical consideration

Ethical considerations for this study were strictly followed. First, permission to conduct this study was sought from the office of the law enforcement agency. After permission, formal verbal consent was obtained from each participant. Respondents were ensured that their personal information would be kept anonymous and the information explored would only be used for research purposes.

Results

In this section, the results of the study are presented. The results are mainly divided into the two sections:

- Loopholes with cellular companies
- Loopholes with Telco/Mobile Operators' Sales Channels & Record Upkeep

These results are interpreted in terms of qualitative themes, developed based on the codes generated through in-depth qualitative interviews.

i. **Cellular Companies Sales Channels**

Illegal selling and activation of fake SIMs at Kiosks and by walking agents

The findings highlight significant issues in SIM distribution, where unauthorized agents—kiosks or walking agents—play a central role in fraudulent SIM activations. Investigation officers pointed out that although cellular companies mandate biometric verification for SIM issuance, franchisees often delegate this responsibility to unauthorized personnel who misuse the process. As one officer explained:

..... Franchisees are supposed to handle SIM activations, but they often hand over devices to untrained, unauthorized agents who operate in public spaces, leading to numerous fraud cases.

These agents extend their reach to public locations like streets, bazaars, and shopping malls. They are often found activating additional SIMs deceitfully and keeping the activated SIMs with them for potential misuse. Another officer described the process as follows:

..... Walking agents mislead people with prize offers, getting the SIM activated under pretenses but never giving the activated SIM to its rightful owner.

Interview responses indicate that franchise owners are frequently complicit in illegal SIM activations. Officers reported that these franchisees not only ignore but sometimes encourage fraudulent activities as a way to increase sales. As one officer commented:

Journal of Business and Management Research
ISSN:2958-5074 pISSN:2958-5066
Volume No:3 Issue No:3 (2024)

..... Franchise owners know these agents conduct fraudulent activations, but they allow it because it boosts their profits.

These unauthorized SIMs are later sold at high prices to cybercriminals, fueling financial fraud and cybercrime. This has far-reaching implications, as these fake SIMs enable illicit activities without easily traceable identities, making investigations challenging.

A recurring sentiment among officers was frustration with the lack of oversight by cellular companies, who are seen as neglectful monitoring franchise activities. One officer remarked:

..... Cellular companies don't seem to take action against franchisees involved in illegal activations; they aren't monitoring these activities closely enough, rather unrealistic targets to activate SIMs monthly are assigned to franchises resorting them to use all out means to meet the targets, which are often tied to their proceeds & bonuses

The absence of accountability measures for franchisees contributes to ongoing SIM-related fraud, creating security vulnerabilities within the branchless banking ecosystem and other cybercrimes.

Exploitation of Biometric Vulnerabilities through Silicon Thumb Impressions

The findings reveal that cybercriminals exploit vulnerabilities in the fingerprint-based biometric system for SIM activation using artificial silicon thumbs. Despite expecting biometric devices to detect only live fingerprints, many fail to differentiate between natural and artificial impressions. This loophole has enabled criminals to activate SIMs fraudulently, using sensitive data from government and private records to fabricate silicon thumb impressions. One investigation officer emphasized this problem:

..... Biometric devices are supposed to reject artificial impressions, but cybercriminals create silicon thumbs from stolen data and activate fake SIMs without detection. In addition to this it has also been found that with the availability of more sophisticated scanning devices the leaked bio metric data from govt& private record is now being sold/used by the organized criminals that does not require silicon thumb impressions to be used rather directly may be scanned for successful activations of SIMs. Also, the data intelligence regarding the availability of users empty slots on their CNICs (as in total 5 SIMs may be issued for voice & 3 data Sims) is passed by cellular companies assisting/colluding with the criminals for the needful.

Journal of Business and Management Research
ISSN:2958-5074 pISSN:2958-5066
Volume No:3 Issue No:3 (2024)

Through these methods, cybercriminals gain unauthorized access to SIMs and proceed to open branchless banking accounts in the names of innocent individuals. These accounts are subsequently used for fraudulent activities, including economic crimes such as establishing illegal gateways.

Pressure on Franchise Owners to Meet Sales Targets and Resulting Malpractices

As implied earlier too, another significant factor driving fraudulent SIM activations is the intense pressure on franchise owners to meet high sales targets set by cellular companies. The unrealistic targets compel franchisees to compromise legal and ethical standards to achieve the required sales volumes, as their profits are directly tied to these targets. To meet these demands, franchisees often employ unregistered agents, including kiosks and walking agents, to distribute and activate SIMs in various public areas. As one officer noted:

..... Franchisees feel forced to cut corners because of high sales targets; they bring in unregistered agents who activate SIMs using manipulated information to meet quotas."

These unregistered agents exploit the system by deceiving people into activating SIMs with enticing offers. Some of these SIMs are retained and later sold to cybercriminals. Cellular companies' involvement in setting such aggressive targets indirectly contributes to the proliferation of fake SIM activations, ultimately facilitating cybercrime.

Collaboration among Franchisees, Agents, and Cybercriminals

The collaboration between franchisees, walking agents, and cybercriminals is a concerning trend that emerged from the interviews. Franchisees and agents frequently work together, facilitating fake SIM activations and branchless banking account creation for criminals. This coordinated effort enables cybercriminals to carry out financial crimes with minimal traceability, as these accounts are often created under the names of unsuspecting individuals. These accounts are heavily used to avoid taxes/tax frauds, illegal money transfers, and money laundering. One of the hot-selling items is this context is biometric details & CNIC data of deceased individuals that is sought after by these gangs.

According to an officer:

..... There's an unfortunate alliance forming between franchisees and criminals. SIMs activated through this partnership fuel numerous financial frauds."

Journal of Business and Management Research
ISSN:2958-5074 pISSN:2958-5066
Volume No:3 Issue No:3 (2024)

The combination of unregulated practices, sales pressures, and technological vulnerabilities results in a lucrative yet dangerous cycle of fraud in the branchless banking system as well as other cybercrimes and in more serious crimes involving ransom, murder & terrorism activities.

ii. Telco/Mobile Operators

Lack of Reporting to the Pakistan Telecommunication Authority (PTA)

Investigation officers emphasized that cellular companies are not adequately reporting the issuance of new SIMs to the Pakistan Telecommunication Authority (PTA), despite a legal obligation to do so. This oversight leads to significant gaps in record-keeping, which hinders law enforcement's ability to trace SIM ownership in criminal investigations. One officer explained:

..... When law enforcement needs data on a SIM used in a crime, PTA often replies with 'no data found,' or provides outdated information from a former subscriber.

This failure to keep updated records weakens the accountability system within telecommunications and creates exploitable opportunities for criminal activities.

On the other hand, mainly the illegally issued SIMs are often registered in the name of a rightful owner but do not remain in the use of these illicitly issued SIMs, hence in the event of a reported crime the tracking takes the LEAs to the Owner (who is innocent & unknown about the SIM that has been issued but not handed over) and not the user/criminal hence makes it hard to curb the menace of crimes

Misuse of Biometric Thumb Impression Systems by Retailers and Franchisees

The SIM activation process, which relies on thumb impression verification, has been widely misused by retail franchises. Officers reported that retailers often perform multiple unauthorized activations under a single person's identity. For example:

..... Retailers get a second thumb impression without the customer's knowledge, activating two SIMs and withholding one for fraudulent purposes and in many cases just replying to the naive users that authentication failed despite it being successfully carried out."

Additionally, franchises sometimes use thumb impressions to open unauthorized branchless banking accounts. This misused data is then sold to cybercriminals, creating fraudulent financial accounts under innocent people's names. Another officer noted:

..... Franchisees also use fake silicon thumbs created from stolen data to activate SIMs and branchless accounts, which are later used for economic crimes."

Journal of Business and Management Research
ISSN:2958-5074 pISSN:2958-5066
Volume No:3 Issue No:3 (2024)

This misuse of the biometric system represents a critical failure in SIM activation security, undermining both user trust and regulatory intentions.

Inadequate Customer Documentation and Record-Keeping

An ongoing issue identified is the lack of accurate customer data collection by cellular companies. Often, SIM activations occur without any form of customer identity verification, and no copy of the CNIC (national ID card) is retained to ensure subscriber legitimacy. This practice creates a loophole for criminals to obtain SIMs through unverified means. As an officer pointed out:

..... Without proper records, even disowned SIMs are untraceable. This leaves law enforcement agencies unable to investigate effectively when criminal activity is suspected.

This inadequate record-keeping poses severe challenges to investigations, with missing records making it difficult to track disowned SIMs or validate current ownership, despite NADRA BVS IDs are stored to identify the transactions however, integrity and manipulation of such data is highly likely especially when such data is already in the custody of cellular companies

Communication Delays between Franchises and Cellular Companies

A significant delay in communication between franchises and cellular companies also emerged as a major concern. Officers reported that franchises often fail to promptly update companies with details of SIM sales and subscriber records, contributing to data management and regulation issues. This delay provides criminals with more time to exploit the activated SIMs. The issue has less severity since the inception of BVS transaction IDs, however in the event of a malfunction, hacking or deliberate break of communication between Franchise and cellular companies may hinder the timely data updating. One officer remarked:

..... The lack of stringent monitoring on franchise data sharing further aggravates this delay, impeding cellular companies' abilities to regulate and maintain accurate subscriber information.

Failure to Maintain SIM Sale Records

Franchisees are often more focused on maximizing SIM sales than on following procedural standards, which leads to poor record-keeping. Officers noted that many franchises do not store any documentary records, such as customer CNICs or sales records. This disregard for record maintenance hinders accountability, as one officer described:

Journal of Business and Management Research
ISSN:2958-5074 pISSN:2958-5066
Volume No:3 Issue No:3 (2024)

..... When records are requested, franchises frequently have nothing to provide. They prioritize sales over compliance, making it impossible to verify who has purchased a SIM."

This lack of responsibility for maintaining sale records allows for unregulated SIM distribution, further exacerbating issues with fraud and illegal activations.

Inadequate Monitoring of Biometric Verification System (BVS) Devices and Sales Officers

The analysis also uncovered weak oversight regarding Biometric Verification System (BVS) devices. BVS devices, meant to be operated only by authorized personnel, are frequently handled by unauthorized individuals. These individuals are often hired on a temporary or commission-based basis, and their misuse of BVS devices facilitates fraudulent SIM activations and unauthorized branchless banking accounts. According to an officer:

..... BVS devices are left in the hands of unqualified daily wage earners who exploit them for illegal SIM activations.

Compounding this issue is the inadequate monitoring of sales officers responsible for managing SIM activations and record collection. Without proper tracking, there is minimal accountability, leaving a significant gap in monitoring franchise operations.

Discussion

The key findings of this study included critical issues in the Sim distribution primarily through unauthorized agents, intense pressure on franchises for the achievement of huge targets, which led them to weaken the security protocols, failure in keeping the updated records of the SIM sales weakened the accountability system, lack of accurate customer data collection by cellular companies and weak oversight regarding Biometric Verification System devices. Based on these weaknesses, cyber criminals find exploitable opportunities for criminal activities. These results are more or less similar to those of Ahmad et al. (2022) and Shahzad (2023) as they revealed that weak policies from the cellular companies, poor compliance to security frameworks, and excessive use of social media had contributed to the increasing cyber-criminal activities.

In this study, weak accountability systems and oversight regarding biometric verification system were limiting factors. Perhaps based on these weakness cybercriminals consider the cellular industry of Pakistan to be one of the easiest targets of their sneering operations. To make the cellular companies accountable to security measures and regulation, the government implemented Prevention of Electronic Crimes Act (PECA) 2016, which was crucial for focusing

Journal of Business and Management Research
ISSN:2958-5074 pISSN:2958-5066
Volume No:3 Issue No:3 (2024)

on Pakistan's approach to cybercrime. However, its delayed enactment and limited scope provide significant loopholes in the act. The legislation lacks comprehensive measures to deal with the changing nature of cyber threats, especially in financial crimes promoted through mobile networks (Iqbal, 2023; Ismail and Gul, 2022). According to studies, despite numerous such laws, there is still inadequacy in the process of enforcement due to insufficient infrastructure and trained employees (Sattar et al., 2018).

Based on the lack of proper security, selling of SIMs through unauthorized agents and not updating the record, studies such as Ismal and Gul (2022) and Kundi (2014) reported that most service providers lack appropriate security implementations, making it very easy for attackers to capitalize on the weakness of mobile applications and payment systems. They also raised their concerns on governance issues and linked this loophole with increasing vulnerabilities to the cyber-crimes. In another study, Kim (2022) reported that Pakistani citizens are disposed to hacking, cyber-organized crime, cyberterrorism, and cyber warfare due to its rapidly increasing application of ICT and minimum cyber preparedness. Users are profoundly unaware of security practices. It helps phishing schemes and other frauds targeting mobile users to achieve their targets (Sattar et al., 2018).

Our study showed that SIMs are usually sold through unauthorized agents, and citizens frequently buy sims from those agents having no awareness about their authorizations and consequences the users of those SIMs can face in the future. This is well related with the fact that most mobile users lack appropriate awareness about cybersecurity practices that render them very vulnerable to cyberattacks. The knowledge gap has presented an easy avenue for cyber criminals to manipulate users, especially through phishing schemes and other frauds that seem legitimate, such as fake messages, calls or links. Without knowing basic security precautions such as checking sources, suspicious requests, or protection of personal details, users inadvertently provide cybercriminals with opportunities to hack sensitive data and commit financial fraud. This lack of knowledge, therefore, directly influences the high success rate of these schemes (Hameed and Naqvi, 2021; Mjunir and Shabir, 2018).In order to curtail cybercrimes, cybersecurity options need to be improved, and the awareness level among people about the prevention of cybercrimes is also important (Farooq et al., 2012; Roberson and Das, 2008). The key findings of this study emphasize on the need for the development of an

Journal of Business and Management Research
ISSN:2958-5074 pISSN:2958-5066
Volume No:3 Issue No:3 (2024)

integrated policy framework, comprising legislation as well as operational, which will encompass all facets of cybersecurity within its purview. Advancement in technology is very rapid and creates a host of both opportunities and challenges. Much emphasis is being put on advanced technologies such as machine learning and data analytics in cybersecurity to develop a preventive measure to identify and mitigate risks of cyber financial crimes (Anjum, 2015; Mushtaque et al., 2014). International collaboration in the fight against cyber-financial crimes and knowledge sharing among law enforcement agencies may also help in creating more strength in combating cyber-financial crimes (Ismail and Gul, 2022; Kundi, 2014).

Conclusion

The analysis of interviews with investigation officers reveals significant regulatory and oversight gaps in SIM activation and distribution practices within Pakistan's telecommunications sector. The involvement of unauthorized agents, inadequate biometric verification, and poor record-keeping create vulnerabilities cybercriminals exploit, posing risks to branchless banking and public security. Officers recommend stricter controls on franchisee operations, enhanced biometric verification, and improved data reporting to the PTA as essential steps to prevent fraudulent SIM activations and reduce associated cybercrimes. There is a need to implement stringent monitoring systems for franchises, enforce proper documentation, and improve oversight on BVS device usage to curb SIM-based fraud and related financial crimes.

References

Ahmad, A., Naz, M., Meer, Y., Gillani, S., Manzoor, A., & Hussain, Z. (2022). Factors Affecting the Criminal Behavior among Pakistani Youth: A Case Study of Punjab Province Pakistan. *Journal of Education and Social Studies*. https://doi.org/10.52223/jess.20223305.

Algahtany, M., & Kumar, L. (2016). A Method for Exploring the Link between Urban Area Expansion over Time and the Opportunity for Crime in Saudi Arabia. *Remote. Sens.*, 8, 863. https://doi.org/10.3390/rs8100863.

Ali, T., Waqas, A., & Mahmood, H. (2022). Mobile Communication landscape: From 1G to 4G and the interest of 5G in Pakistan. *2022 17th International Conference on Emerging Technologies (ICET)*, 212-217. https://doi.org/10.1109/ICET56601.2022.10004670.

Journal of Business and Management Research
ISSN:2958-5074 pISSN:2958-5066
Volume No:3 Issue No:3 (2024)

Anjum, R. (2015). An Appraisal of Cyber Laws with Reference to E-Banking in Pakistan. *Computer Engineering and Intelligent Systems, 6*, 1-5.

Farooq, M., Islam, A.M., &Ghulzar, F. (2012). Social and economic causes of crime among the female (a case study in district and central jail faisalabad, Pakistan).

Gaumer, Q., Mortier, S., &Moutaib, A. (2016). Financial institutions and cyber crime – Between vulnerability and security. *Financial Stability Review*, 45-52.

Gulyamov, S., &Raimberdiyev, S. (2023). Personal Data Protection as a Tool to Fight Cyber Corruption. *International Journal of Law and Policy*. https://doi.org/10.59022/ijlp.119.

Hameed, I., & Naqvi, S. (2021). An Analysis of the factors affecting Cybercrime against individuals in Pakistan. *2021 15th International Conference on Open Source Systems and Technologies (ICOSST)*, 1-6. https://doi.org/10.1109/ICOSST53930.2021.9683986.

Hanif, M., Shao, Y., &Hanif, M. (2017). Growth prospects, market challenges and policy measures: evolution of mobile broadband in Pakistan. , 20, 00-00. https://doi.org/10.1108/DPRG-04-2017-0014.

Hassan, R., Waseem, L., Yasmin, S., &Maqbool, S. (2023). Impact of Urbanization on Socioeconomic Conditions of Rural Areas of Faisalabad City. *Review of Education, Administration & Law*. https://doi.org/10.47067/real.v6i2.337.

Iqbal, M. (2023). The Prevention of Electronic Crimes Act (PECA) 2016 Understanding the Challenges in Pakistan. *Siazga Research Journal*.

Iqbal, M., Rahim, Z., Hussain, S., Ahmad, N., Kaidi, H., Ahmad, R., &Dziyauddin, R. (2021). Mobile communication (2G, 3G & 4G) and future interest of 5G in Pakistan: a review. *Indonesian Journal of Electrical Engineering and Computer Science*, 22, 1061. https://doi.org/10.11591/IJEECS.V22.I2.PP1061-1068.

Ismail, M., & Gul, N. (2022). Cyber Security and Policy Making: An Analysis of Pakistan. *Journal of Strategic Policy and Global Affairs*.

Javaid, L., Kousar, N., Anjum, F., Nida, N., Anwar, M., &Javaid, U. (2023). Sociological Study on Residents' Perception of Special Economic Zone Regarding the Consequent Change in the Area; A Case Study of District Faisalabad. *Journal of South Asian Studies*. https://doi.org/10.33687/jsas.011.01.4704.

Journal of Business and Management Research
ISSN:2958-5074 pISSN:2958-5066
Volume No:3 Issue No:3 (2024)

Khalid, S. (2006). Reasons for Growth and the Future of the Cellular Industry of Pakistan. *Information Systems & Economics*. https://doi.org/10.2139/ssrn.996259.

Kim, Y. (2022). Cellular Security: Why is it difficult?. *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*. https://doi.org/10.1145/3488932.3522770.

Kundi, G.M. (2014). Digital Revolution, Cyber-Crimes And Cyber Legislation: A Challenge To Governments In Developing Countries. *Journal of Information Engineering and Applications, 4*, 61-70.

Kundi, G.M. (2014). Digital Revolution, Cyber-Crimes And Cyber Legislation: A Challenge To Governments In Developing Countries. *Journal of Information Engineering and Applications, 4*, 61-70.

Munir, A., &Shabir, G. (2018). Social Media and Cyber Crimes in Pakistan: Facts, Propaganda, Awareness, and Legislation. *Global Political Review*. https://doi.org/10.31703/gpr.2018(iii-ii).09.

Mushtaque, K., Umer, A., Ahsan, K., & Mahmood, N. (2014). Digital Forensic Models: A Comparative Study based in large enterprises of Pakistan.

Rizvi, S. A. A., Mahfooz, I., & Ahmad, W. (2024). A Critical Analysis of Loopholes in Branchless Banking in Pakistan. *Journal of Development and Social Sciences*, *5*(4), 132-139.

Rizvi, S., Zubair, M., Ahmad, J., Hashmani, M., & Khan, M. (2019). Wireless Communication as a Reshaping Tool for Internet of Things (IoT) and Internet of Underwater Things (IoUT) Business in Pakistan: A Technical and Financial Review. *Wireless Personal Communications*, 116, 1087 - 1105. https://doi.org/10.1007/s11277-019-06937-3.

Roberson, C., & Das, D.K. (2008). An Introduction to Comparative Legal Models of Criminal Justice.

Sattar, Z., Riaz, S., , S., & Mian, A. (2018). Challenges of Cybercrimes to Implementation of Legal Framework. *2018 14th International Conference on Emerging Technologies (ICET)*, 1-5. https://doi.org/10.1109/ICET.2018.8603645.

Sattar, Z., Riaz, S., Shafia, & Mian, A.U. (2018). Challenges of Cybercrimes to Implementation of Legal Framework. *2018 14th International Conference on Emerging Technologies (ICET)*, 1-5.

Shad, M. (2019). Cyber Threat Landscape and Readiness Challenge of Pakistan. *Strategic Studies*. https://doi.org/10.53532/ss.039.01.00115.

Journal of Business and Management Research
ISSN:2958-5074 pISSN:2958-5066
Volume No:3 Issue No:3 (2024)

Shahzad, M. (2023). Emerging Cyber Crimes in Pakistan: A Case Study of Online Fraud through Digital Microloan Apps. *Global Digital & Print Media Review*. https://doi.org/10.31703/gdpmr.2023(vi-ii).30.

Shahzad, M. (2023). Emerging Cyber Crimes in Pakistan: A Case Study of Online Fraud through Digital Microloan Apps. *Global Digital & Print Media Review*. https://doi.org/10.31703/gdpmr.2023(vi-ii).30.

Sharma, V., Manocha, T., Garg, S., Sharma, S., Garg, A., & Sharma, R. (2023). Growth of Cyber-crimes in Society 4.0. *2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM)*, 1-6. https://doi.org/10.1109/ICIPTM57143.2023.10118185.

Singh, A., & Bora, M. (2013). Cyber Threats and Security for Wireless Devices. . https://doi.org/10.2139/SSRN.3419703.