P-ISSN: 2709-6254	Journal of Development and Social Sciences	October-Dec 2024, Vol. 5, No. 4
O-ISSN:2709-6262	https://doi.org/10.47205/jdss.2024(5-IV)12	[132-139]

Journal of Development and Social Sciences
www.jdss.org.pk

RESEARCH PAPER

A Critical Analysis of Loopholes in Branchless Banking in Pakistan

[1]Syed Arshad Ali Rizvi* [2] Izza Mahfooz and [3]Wahab Ahmad

1. Federal Investigating Agency, Pakistan
2. Govt. Graduate college for women, People's Colony, Faisalabad, Pakistan
3. Federal Investigating Agency, Pakistan

***Corresponding Author:** alirizvi1540@gmail.com

ABSTRACT

This study aimed to critically explore the loopholes in Branchless Banking in Pakistan. This study was qualitative, and a total of 16 cyber investigators were interviewed face-to-face from the district Faisalabad. Collected data were analyzed using the content analysis method. Results of this study are presented under different key themes, i.e. (i) serious violations of Know Your Customer (KYC) & Customer Due Diligence (CDD), (ii) BVS (Biometric Verification System) Failure followed by some sub-themes. This study unveiled that the security of internet-based financial services is a great concern. Whereas violations of KYC and CDD reflect various vulnerabilities that augment financial crimes. Ineffective use of biometric verification systems, poorly maintained retailer records, and the operation of unauthorized individuals aggravate the risks of financial crimes. There is a need for a real-time monitoring system of transactions, a strict BVS, and an awareness campaign for public on safe use of branchless banking.

KEYWORDS Biometric, Customer, Cyber Investigators, Cyber-Crime, Financial Services

Introduction

Since the dawn of civilisation, crime has been a persistent concern for society. With scientific and technological advancements, the nature of crime has evolved. The connection between crime and technology is particularly strong, as advancements in these fields have led to shifts in criminal behaviour in the 21st century. The rapid rise and widespread adoption of computer technology over the past two decades have contributed to a significant increase in cybercrime (Li et al., 2021). Among all technological innovations, the internet stands out as one of the most impactful, becoming an essential part of both personal and professional life (Michael et al., 2023). As internet usage continues to grow, so does the spread of cybercrime in various forms, such as cyber extortion, cyber warfare, and internet fraud (Kumar, 2016).

For millions, the internet has quickly become necessary, influencing how they live and work, driven by the increasing reliance on technology. As a developing nation, Pakistan faces challenges in keeping pace with the global community in many areas, including modern technology and advanced financial transaction systems. According to Hussain et al. (2017) accessibility of the Internet in banking, customer reluctance to access accounts electronically, and lack of cyber security were the key challenges faced by Pakistani people in adopting modern technology and advanced financial transaction systems.

Cyber financial crime, also called virtual financial crime, involves fraudulent activities such as fraud, money laundering, and other financial offenses conducted online. Cybercrime costs the financial sector significantly, driven by strategic priorities, customer trust, and market positioning rather than the number of incidents experienced (Lagazio et al., 2014). These crimes extend beyond large-scale financial schemes, including romance and honey scams, lottery and charity frauds, fake Facebook profiles, online shopping scams, and obtaining account details by impersonating state institutions through phone calls or spoofed bank helpline numbers. In cyberspace, cybercriminals use fake websites, hijacked

emails, anonymous servers, fraudulent apps, unauthorized SIM card issuance, and mobile banking accounts linked to those SIMs to facilitate fraud (Jhaveri et al., 2017; Shahzad, 2023). In many cases of cyber financial fraud, mobile banking services such as EasyPaisa, JazzCash, Zong NayaPay, SadaPay, Digitt Plus, UBL Omini, HBL Konnect, and uPaisa etc. are very commonly used to initially hold the stolen funds, followed by layering and withdrawal of the money. These services have several system vulnerabilities that fraudsters exploit to conceal their identities, making it difficult for law enforcement agencies to trace the perpetrators (Shahzad, 2023; Malik et al., 2023).

Cyber financial crime has become a major global issue, threatening the world economy (Chambers-Jones, 2012). Efforts to address the problem have led to international cooperation to prevent, detect, and prosecute such crimes. Virtual financial crime, such as fraud and money laundering, threatens global economies and requires international agreements to prevent, detect, and punish perpetrators. (Chambers-Jones, 2013). However, law enforcement agencies and governments face increasing challenges in managing these threats. Various countries, police forces, and intelligence agencies are taking steps to combat cross-border cyber risks.

The government has introduced general and specialized laws to address cyber financial crime in Pakistan. For instance, the Prevention of Electronic Crimes Act (PECA) 2016 is a comprehensive law in Pakistan addressing cyber-crime issues (Bilal and Khan, 2022). The other legal frameworks in Pakistan, including the Pakistan Computer Emergency Response Team (Pak-CERT) Act, 2017; and the Data Protection Act, 2018, also exist (Masudi and Mustafa, 2023). While the system effectively deals with traditional offences, it struggles with the complexities of cybereconomic crime, a newer and more technologically sophisticated phenomenon. This situation opens up opportunities for researchers to explore ways to enhance mobile banking and telecom systems, reducing the likelihood of fraud and protecting people's hard-earned money. In a study, Shahzad (2023) highlighted that weak implementation of cyber-laws in Pakistan was contributing to online fraud occurring through digital microloan apps among female students in particular (Shahzad, 2023). Graduate and postgraduate students in Pakistan are at a higher risk of facing fraud from cyber criminals and have inadequate knowledge of how to stay safe on the internet (Munir and Shabir, 2023).

The need arises from the increasing reliance on mobile banking services such as EasyPaisa, JazzCash, Zong NayaPay, SadaPay, Digitt Plus, UBL Omini, HBL Konnect, and uPaisa etc., which play a significant role in financial inclusion. A critical analysis should be conducted to examine the current scenario of cyber-financial crimes in Pakistan. However, these services have also become vulnerable to exploitation, with fraudsters taking advantage of system loopholes to commit cyber financial crimes. A critical analysis of these weaknesses is essential to identify the gaps in security, regulation, and technology, which hinder the effective tracing of criminals. Such a study would help improve the integrity of branchless banking, ensuring safer financial transactions and boosting public confidence in digital financial services in Punjab. It would also provide valuable insights for policymakers to strengthen regulatory frameworks and protect consumers from financial fraud.

Material and Methods

Study area

This study was conducted in the purposively selected Faisalabad district, one of the largest cities in the Punjab province. This city is also known as Manchester of Pakistan for its potential in the textile industry and business opportunities. Faisalabad has a profound contribution to economic acceleration in the province and as well as on the national level.

The government has established a system where Cybercrime investigators of law enforcement agencies are working to minimize cyber enabled financial frauds. These cybercrime investigators are key persons with diversified information about financial crimes and are dealing with victims of these fraudulent activities. Thus, in this study, those cybercrime Investigators were considered the population and the Key Informants (KI).

Population and sample size

There are 16 cybercrime Investigators working 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 to which it will be put, 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 believed that all the 16 cybercrime investigators were knowledgeable and could give diverse experiences of dealing with different cyber financial crimes. Therefore, researchers preferred selecting all the investigation officers as the case study.

Data collection and analysis

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

Ethical considerations for this study were strictly followed. First, permission from the office of law enforcement agency was sought to conduct this study. 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 and Discussion

Serious violations of Know Your Customer (KYC) & Customer Due Diligence (CDD)

Know Your Customer (KYC) and Customer Due Diligence (CDD) are mandatory for financial institutions and other regulated entities to identify clients and collect essential information for financial transactions. In compliance with the customer identity program required by the State Bank of Pakistan, Pakistani banks implement KYC to verify client identities. Understanding customers' needs is crucial to prevent identity theft, money laundering, and terrorist financing. KYC includes various security measures beyond identity verification, such as monitoring customers' activities concerning their profile, account history, and transactions with others.

The Financial Action Task Force (FATF) released an Interpretative Note on Customer Due Diligence to help banks and financial institutions assess customer-related risk factors more effectively. This system distinguishes between different types of risks, including product, service, and transaction risks, customer risk factors, geographical risks, and risks associated with distribution channels. In countries with strong anti-terrorism financing and anti-money laundering frameworks, regulatory bodies require the immediate reporting of suspicious transactions by law. Banks in Pakistan are required to implement Customer Due Diligence (CDD) principles to ensure that banking transactions are in accordance with the profile, characteristics, and transaction patterns of prospective customers or walk-in customers (Johannes, 2019).

Lack of KYC and no information about source of income

During the discussion, respondents agreed that;

……in branchless banking (BB), since customers are not required to submit any documents or forms, there is limited information available about them. The practice of performing KYC (Know Your Customer) is absent, meaning that no one knows the customer's profile. This allows criminals, terrorists, fraudsters, or even individuals listed in the country's red book or on the fourth schedule to open accounts in BB. The absence of KYC in branchless banking exposes it to substantial risks, including financial, legal, and reputational threats.

Another issue in branchless banking (BB), as revealed by the study participant was;

……there is no information available about the source of income of the account holder. The money kept by him in the account is whether from legal means or illegal means; no one knows as it is never asked of him. The lack of sound KYC policies and procedures and no verified information about branchless banking account holders' source of income and business authenticity paves the way for branchless banking to become a vehicle for money laundering, terrorist financing, and unlawful activities. This lacuna attracts criminals towards branchless banking, a safe haven for them.

Accounts opened at a fake address

It was synthesized from the discussion that the address of an account holder is very important to confirm the originality of the account holder. There is no practice of submitting copies of CNIC and other documents, and also, no form has to be signed & submitted by the BB account holder at any office before opening the account. So, people with malafide intentions enter wrong information about their location and address while opening an account online. Branchless banking does not have any mechanism to confirm and verify the address entered in the Application. Thus, the Branchless banking service providers never confirm the given address. It provides shelter to the criminals as their real location and address remain hidden, creating difficulties for law enforcement agencies tracing them.

No generation of STRs and CTRs

Branchless banking lacks essential monitoring and reporting systems, such as Suspicious Transaction Reports (STRs) and Currency Transaction Reports (CTRs), which are vital for combating money laundering and terrorist financing. According to FATF Recommendation 20, financial institutions and concerned citizens must report STRs or Suspicious Activity Reports (SARs) if there are reasonable grounds to suspect a transaction is linked to criminal activity. An unusual transaction refers to one that raises concerns due to specific circumstances, the people involved, or the organization conducting the transaction.

One of the respondents arbitrated that;

……..to identify changes in a customer's transaction risk profile, institutions evaluate factors like customer due diligence, real-time payment screening, transaction monitoring, and behavioral monitoring. While STRs do not always involve specific transactions, they have a broader scope by flagging discrepancies between a customer's actions and industry standards. Enforcing STRs is a proven method to prevent money laundering and criminal infiltration into the legitimate economy, especially in countries with strong anti-money laundering and counter-terrorist financing frameworks. As a result, filing STRs promptly after detection is legally required.

Understanding local money laundering drivers helps gauge the community's vulnerability to the issue. As a unique financial model, branchless banking lacks transaction monitoring systems and a mechanism to detect suspicious transactions, preventing the submission of STRs. Consequently, significant money laundering goes unreported after banking fees are deducted. Pakistan has faced serious challenges in exiting FATF's grey list, before getting out of it and the absence of STR and CTR reporting mechanisms in branchless banking are also among those. Cybercriminals often use branchless banking accounts to transfer and withdraw illicit funds, turning them into "clean" money. The absence of automated STR and CTR generation processes in branchless banking facilitates the goals of cybercriminals and money launderers.

Heavy Sales Targets

By assigning sales targets to employees, banks increase the chances of financial crimes being committed. In branchless banking, service providers often set high targets to rapidly open new accounts, linking agents' profitability to meeting these goals. To achieve these targets, agents may compromise on rules and regulations. Many registered agents enlist unregistered sub-agents to help meet their targets. These unregistered individuals often visit markets or even people's homes, persuading them to open accounts, sometimes without the customer's full understanding of their control over the account.

In some cases, biometric scanners, like those on phones, are used by unauthorized operatives to create fake identities by scanning people's silicon thumbprints. These identities are then sold to criminals for illegal activities. A significant number of branchless banking accounts created through such efforts are fraudulent and later exploited by cybercriminals for laundering money and other illegal operations.

BVS (Biometric Verification System) Failure

Failure of live finger detection on BVS device

The vulnerabilities in fingerprint-based biometric verification systems, particularly the failure of live finger detection devices, make branchless banking susceptible to exploitation by cybercriminals. The biometric devices used to open branchless banking accounts are intended to detect only live fingers and reject fake thumb impressions. However, these devices often fail to distinguish between real and artificial thumb prints. Cybercriminals illicitly acquire sensitive personal data from different government and private databases and use it to create silicon thumbprints. These fake thumbs, along with the stolen data, are then used to open branchless banking accounts with the help of BB agents and sub-agents, bypassing the biometric verification systems.

Once these fraudulent accounts are created, they fall under the control of criminals who use them for illegal activities and financial crimes. The failure of biometric systems to detect fake thumbs enables cybercriminals to use branchless banking as a preferred method to park, store and withdraw money obtained through fraudulent activities.

No updated retailer information of BVS.

The records of registered retailers equipped with biometric verification system (BVS) devices are not properly maintained, resulting in incomplete information available to branchless banking service providers. Factors such as the retailer's financial status, reputation, credibility, eligibility, and education are not evaluated before issuing a BVS device. Additionally, retailers are not assigned specific areas for opening branchless banking accounts and may receive devices at temporary addresses. This situation creates opportunities for retailers to misuse the BVS devices to open fake accounts in collaboration

with cybercriminals, who later use these accounts for financial crimes. One investigation officer explained;

……..When a retailer changes and a new one takes over, the records are not updated promptly. Consequently, branchless banking service providers are reluctant to share records about retailers because the information is poorly maintained. This gap in the branchless banking system complicates investigations for law enforcement agencies while providing cover for cybercriminals, making it difficult to trace and apprehend them.

Use of BVS devices by unauthorized persons

Another problem with the Biometric Verification System (BVS) in branchless banking is that BVS devices are often registered in the name of individuals who do not actually operate them. The BVS machine is issued to a registered branchless banking (BB) agent responsible for its operation at a designated location. However, the reality is often different. Many BB agents do not use the BVS devices themselves; instead, they hire individuals to operate the machines door-to-door or in busy markets to open accounts. These hired individuals approach people in the streets, markets, and even at their homes, opening numerous fraudulent accounts by obtaining thumbprints in exchange for gift hampers or through deception.

These uneducated and unsuspecting individuals often have no understanding of the situation. The private operators, employed by the registered BB agents, misuse the BVS devices for personal gain. They gain control over multiple branchless banking accounts, which they then sell to cybercriminals. As a result, the unauthorized use of BVS devices contributes to the increased exploitation of branchless banking by cybercriminals for committing cyber financial crimes.

Cash-out leaves no traces of recipient

The mechanism for withdrawing money in branchless banking is inadequate and facilitates cybercriminal activities. Biometric verification is not required for cash withdrawals; only a code is needed. As a result, it is often unclear who has made the withdrawal. Additionally, BB agents and cash outlets are not required to maintain records, such as the name or CNIC of the person receiving the cash. Only a one-time password (OTP) is necessary for cashing out from these accounts. This lack of record-keeping consistently attracts cybercriminals, making branchless banking a preferred method for committing cyber financial fraud.

Conclusion

This study shows that internet-based financial services are increasing over time, but their security still remains questionable. Cyber financial crimes are increasing as internet-based services are mounting. The analysis of serious violations of Know Your Customer (KYC) and Customer Due Diligence (CDD) regulations in the context of branchless banking reveals significant vulnerabilities that facilitate financial crimes, including money laundering and terrorist financing. The absence of stringent KYC procedures, lack of verification of income sources, and inadequate monitoring systems like Suspicious Transaction Reports (STRs) and Currency Transaction Reports (CTRs) create a permissive environment for cybercriminals. Furthermore, the ineffective use of biometric verification systems, poorly maintained retailer records, and the operation of unauthorized individuals exacerbate the risks associated with branchless banking, ultimately undermining the integrity of the financial system.

Recommendations

Regulatory bodies and financial institutions must implement comprehensive reforms to mitigate these risks. First, establishing robust KYC and CDD protocols that require thorough identity verification and customer documentation will help ensure account holders' authenticity. Second, creating a real-time monitoring system for transactions, including automated generation of STRs and CTRs, is essential for promptly detecting and addressing suspicious activities. Third, banks should enforce strict guidelines on using biometric verification systems, ensuring that these devices are operated only by authorized individuals. Additionally, continuous training and monitoring of agents and sub-agents are vital to uphold compliance and integrity. Lastly, improved record-keeping practices for retailers and stringent penalties for non-compliance will enhance accountability and support law enforcement efforts in combating cyber financial crimes.

References

Bilal, H., & Khan, M. (2022). Cyber Crime Legislation in Pakistan: A Critical Analysis from Islamic Law Perspective. *Al-Idah*. https://doi.org/10.37556/al-idah.040.02.0802.

Chambers-Jones, C. (2012). *Virtual economies and financial crime: Money laundering in cyberspace*. Edward Elgar Publishing.https://doi.org/10.4337/9781849809337.

Chambers-Jones, C. (2013). Cyber economic crime and commonwealth laws. *International Journal of Intellectual Property Management*, 6, 95.

Hussain, Z., Das, D., Bhutto, Z., Hammad-u-Salam, M., Talpur, F., & Rai, G. (2017). E-Banking Challenges in Pakistan: An Empirical Study. *Journal of Computational Chemistry*, 5, 1-6.

Jhaveri, M., Çetin, O., Gañán, C., Moore, T., & Eeten, M. (2017). Abuse Reporting and the Fight Against Cybercrime. *ACM Computing Surveys (CSUR)*, 49, 1 - 27.

Johannes, E. P. (2019). Customer Due Diligence Dalam Mencegah Tindak Pidana Pencucian Uang Melalui Lembaga Perbankan. *Law Review*, *19*(1), 77-97.

Kumar, P. (2016). Growing cyber crimes in India: A survey," *2016 International Conference on Data Mining and Advanced Computing (SAPIENCE)*, Ernakulam, India, 2016, pp. 246-251 https://doi.org/10.1109/SAPIENCE.2016.7684146.

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Comput. Secur.*, 45, 58-74. https://doi.org/10.1016/j.cose.2014.05.006.

Li, Y., and Qinghui, L. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports,* 7: 8176-8186.

Malik, A. A., Asad, M., & Azeem, W. (2022). The Frauds in Banking and Entrepreneurs by Electronic Devices and Combating Using Software and Employment of Demilitrized Zone in the Networks. *International Journal for Electronic Crime Investigation*, *6*(4), 5-12.

Masudi, D., & Mustafa, N. (2023). Cyber security and data privacy law in Pakistan: protecting information and privacy in the digital AGE. *Pakistan Journal of International Affairs,* 6(3), 356-366. https://doi.org/10.52337/pjia.v6i3.906.

Michael, O. O., Oluwafunmilayo, B. G., & Oyedepo, O. T. (2023). The adoption and impact of Internet-based technological innovations on the performance of the industrial cluster firms. *Journal of Economy and* Technology. 1, 164-178

Mocănașu, D. R. (2020). Determining the sample size in qualitative research. In *International multidisciplinary scientific conference on the dialogue between sciences & arts, religion & education* (Vol. 4, No. 1, pp. 181-187). Ideas Forum International Academic and Scientific Association. https://doi.org/10.26520/MCDSARE.2020.4.181-187.

Munir, A., & Shabir, G. (2018). Social Media and Cyber Crimes in Pakistan: Facts, Propaganda, Awareness, and Legislation. *Global Political Review*, 3(2), 84-97

Sandelowski, M. (1995). Sample size in qualitative research. *Research in nursing & health*, 18 (2), 179-83. https://doi.org/10.1002/NUR.4770180211.

Shahzad, M. (2023). Emerging Cyber Crimes in Pakistan: A Case Study of Online Fraud through Digital Microloan Apps. *Global Digital & Print Media Review, VI*, 411-421.