

**Erosion of Trust in E-Banking: Analyzing the Consequences of Data Breaches
and Fraud on Customer Confidence and Usage in Pakistan**



Farhan Rauf Qureshi

Fall-2K19-EMBA – 00000318858

Department of Finance & Investment

NUST Business School

National University of Sciences and Technology (NUST)

2024

**Erosion of Trust in E-Banking: Analyzing the Consequences of Data Breaches
and Fraud on Customer Confidence and Usage in Pakistan**



Farhan Rauf Qureshi

Fall-2K19-EMBA – 00000318858

Department of Finance & Investment

**A Business Project submitted in partial fulfillment of the
requirements for the degree of
Executive Masters in Business Administration**

Supervisor: Dr Nabeel Safdar

NUST Business School

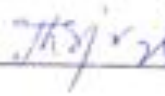
National University of Sciences and Technology (NUST)

2024


BUSINESS PROJECT ACCEPTANCE CERTIFICATE

It is Certified that final copy of EMBA Business Project written by Farhan Rauf Qurashi Registration No. 318858 of EMBA 2K19 has been vetted by undersigned, found complete in all aspects as per NUST Statutes/Regulations/MS Policy, is free of errors, and mistakes and is accepted as fulfillment for award of EMBA degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the said business project.


DR. NABEEL SAFDAR
Program Head "PhD"
NUST Business School (NBS)
Sector H-12 Islamabad Pakistan

Signature of Supervisor with stamp: Dr. Nabeel Safdar 

Date: _____

Programme Head Signature with stamp: Dr. Muhammad Fawad Khan 


Date: _____

Signature of HoD with stamp: Mr. Saad Ul Marwat 

SAAD KHAN ALMARWAT
HoD, Finance & Investments
NUST Business School (NBS)
Sector H- 12, Islamabad
Tel: 051-90853150

Date: _____

Countersign by

Signature (Dean/Principal): 

Principal & Dean
Dr. Nabeel Farwar
NUST Business School

Date: _____

Abstract:

E-banking which greets us with the option of easy access to the services and convenience has been driving out the whole e-finance sector in Pakistan and it continues to grow. Thus, the change itself has caused some cyber security problems which can be a reason for slowing the rate of consumer trust in both products and services. Moreover, some data leakages and fraud issues may come up. This research in particular focuses on the multifaceted traits of e-banking security and customer opinion in Pakistan which serves to conclude the problematic area of digital financial system. This research substantiates the current and future trends by an exhaustive examination of the survey results, consisting of viewpoints on security measures, personal experience with safety incidents and their attitudes to regulatory mechanisms. Risk, fraud, and their influence on trust are the drawbacks that people face and yet more people prefer online banking than the old-style way because it appears more convenient. This research proves that in addition to maintain the effective and the proper security system and measures, we also should create a sophisticated legal framework and clear open communication in preventing and managing new security threats which might be a potential danger for users e- banking services. Pakistan can handle the security problems embarking on electronic banking through customer-centered solutions and engagement of all stakeholders thereby providing a platform for electronic services to be inclusive, result in growth and which in turn motivate financial Independence.

Contents

Letter of Acceptance.....	iii
Abstract.....	iv
Table of Contents.....	v
Chapter 01	1
Introduction	1
1.1 Definition of E-banking	2
1.2 Background	2
1.3 Problem Discussion	3
1.4 Study Purpose	4
Chapter 02	6
Literature Review	6
2.1 Theoretical Framework	8
2.2 Trust Theory	8
2.3 Information Security Theory	9
2.4 Cultural Dimensions Theory	9
2.5 Regulatory Compliance Theory	10
Chapter 03	11
Methodology	11
3.1 Objective and Scope	11
3.2 Data Collection	11
3.3 Ethical Considerations:	11
Chapter 04	12
Data Analysis and Interpretation	12
4.1 Statistical interpretation and discussion	15
4.2 Usage of E-Banking Services:	15
4.3 Perception of E-Banking Convenience:	15
4.4 Information Confidentiality in E-Banking:	16
4.5 Experience of Data Breaches and Fraud Cases:	16
4.6 Effect of Incident on Trust and Future Use:	16
4.7 Bank Compensation for Fraud Losses:	17
4.8 Government rules Are Necessary:	17
4.9 Perception of the Security Priority of E-Banking Providers:	17

4.10 Informational Awareness and Assistance:.....	18
4.11 Impact of Data Breach on Adoption of New Technologies:	18
4.12 Satisfaction with Security Measures:	18
4.14 Recommendation of E-Banking Services:	18
Chapter 05	21
Limitations, Conclusion and Recommendation	21
5.1 Limitations.....	21
5.2 Conclusion	22
5.3 Recommendations.....	23
5.3.1 Strengthen Security Protocols.....	23
5.3.2 Raise Awareness and Education	23
5.3.3 Boost Regulatory Structures	23
5.3.4 Improved Transparency and Communication	24
5.3.5 Invest in Technological Innovations	24
5.3.6 Frequent observation and assessment:	24
5.3.7 Encourage Financial Inclusion:.....	24
5.3.8 Ongoing Investigation and Education:	24
References:	26

Chapter 01

Introduction

Technology has taken the world to greater lengths, and the companies highly rely on it for storage and processing of huge sensitive information. This brings about data breaches, where the primary risk factor is exposed. Nevertheless, data thefts and frauds remain a concern for organizations across all industries though the cyber security measure has undergone a transformation. Such incidents not only are major creative concerns for businesses damages the reputation and trust that customer has in their products and services.

The type of e-banking now prevails in banking sector of Pakistan as a significant part of the financial services delivery activity. Following this up these two parties, that is, the consumers and the financial institutions are left exposed to the cyber-criminals where data leaks and fraud are the chief menace, whilst at the same time the hackers provide a new chance for convenience. Stability and sustainability of digital financial ecosystem can only be achieved when we obtain knowledge about the damages caused by security infringements to customers' trust and the use of e-Banking in this fast-changing scenario.

In the context of e-Banking in Pakistan, this research paper aims to explore a complex question: data breaches and frauds might discourage customer purchases. The study intends to untangle the puzzling relationships that establish trust about security struggles and the resultant adoption decisions using the sophisticated interrelationship of technological vulnerabilities, consumers' notion, and regulating framework.

Being aware that E-Banking is not just a platform for transactions but that consumers entrust their financial data in the institutions in exchange for smooth digital services is the position on which these research findings are based. The said situations of data breaches and fraud incidents can be, thus, deemed as a loss of both technological capability and consumer confidence as far as e-banking is concerned.

1.1 Definition of E-banking

Internet banking or electronic fund transfer (EFT), refers to a similar system which uses electronic means for the transfer of money straight out from the account into another, regardless of whether it's done just using the internet, phone banking or an automated teller machine (ATM). This method is applied to help in a variety of financial transactions, including withdrawing money during all hours of both day and night, using present inside the bank or a personal For example, people may use the option of either their bank or credit union to make the payments of their monthly utility bill, payments of loan as well as mortgage installment be automatically deducted from their account on a monthly basis.

Besides that, e-Banking allows to buy canned or fresh food, stuff for the house or gas for the car by using your credit card or something else instead of cash. Lastly, daily routines including paying the telephone service, toll charges, or taking care of college dues and purchases at the bookshop are now handled through a smart card loaded with value which is it.

1.2 Background

Trend of financial services sphere on the world market has been mostly altered by the appearance of electronic money. It provides customers with comfort, transparency and efficiency. The growing e-Banking situations in Pakistan mirror the world trend. They are brought about by increased internet sustainability, high phone penetration and the governmental initiatives for financial inclusion made in 2020, Khalid 2020. E-Banking refers to a broad variety of digital transactions held by virtual banks and other channels like the Internet, mobile banking and ATMs, including online transfers, bills and shopping.

On the one hand, e-Banking delivers tremendous advantages such as in terms of accessibility, while on the other hand true challenges, mostly concerning cyber security issue, remain. Cybercrimes which manifest themselves in form of data breaches and fraud activities are an integral part of e-Banking operations, as a result of their digital attributes. Security breaches refers to any unauthorized access to information such as customers' names and financial records by services or actors seeking to exploit or cause damage (Khan et al., 2019). While forgery is the copying, alteration, or imitation of documents either to illegally acquire electronic payment or to

get gainful amounts of money through the mechanisms like phishing, identity theft or using card skimmers. Ali et al. 2021.

The escalating concerns related to successful data penetration and fraud cases on consumer trust and adoption of e financial banking services in Pakistan is the one that particularly deserved attention, as the digital financial sector in the country has been increasing every day. Customers' trust and confidence in e-Banking products are consequential as it gauges customer's decision to open account and avail themselves of e-Banking services (Shahbaz et al. 2020). Additionally, trust in an e-Banking platform's security and integrity is the primary factor of customers' e-Banking adoption behavior which weakens or strengthens the decisions regarding financial account opening

The awareness of the results of data breaches and cyber incidents on customers' trust and services acceptance trends of electronic banking in Pakistan, where cybersecurity and data protection are regarded as significant issues, would be useful. This is where the matter gets more intricate as compared to others because of the multi-dimensional social-legal-technical texture of Pakistan that is needed to be understood to understand the complexity.

1.3 Problem Discussion

The financial ground of Pakistan has totally changed by the increasing e-Banking services which provide incredible convenience and ease of access to masses. Nevertheless, these issues along with the challenges of cyber security are also raised due to this digital transformation. With respect to Pakistan, the possibilities of e-Banking data breach and hacking cases with severe repercussions on customer trust and adoption are very high.

Privacy and security of e-banking system is the main threat toward integrity of e-banking platforms through data breaching incident. Furthermore, data breaching issues are done through unauthorized access, disclosure or subversion of the confidential information (Khan et al. 2019). To achieve the purpose of putting their hands on consumer data, the cyber criminals take use of the weaknesses existing in the security procedures. What worse the scenario is these hacking not only disturb the client privacy, but also scar the customers' confidence into the banks.

Our trust and faith in online money transactions could be damaged by the frauds found out in e-Banking such as phishing mail, identity theft, and card skimming. According to the researchers, these instances of fraud are meant to confuse the consumers into revealing their personal information or compromising their accounts with the sole purpose to gain forbidden profits. Accordingly, consumers remain unnoticed in using e-Banking activities fearing a possible falling of money or identity theft.

The role of data breaches, and hacking incidents in inviting mistrust and preventing the adoption of e-banking cannot be ignored. The main feature of a customer-bank relationship is based on the trust, which in turns makes customers either to embrace or reject e-banking as described in Shahbaz et al (2020) although technology has lighter risk profile compared to trusted bank.

Additionally, the unique societal-cultural, regulatory, and technological environment of Pakistan intensify the challenges which are faced due to the data breaches and fraud on e-banking. The cultural factors which may result in privacy or security concern are among the major determinants of consumer attitude towards the e-banking services and therefore they influence their trust on integrity of the electronic banking platform Majeed et al., 2021. One another vital factor in justifying the security risks development consumer confidence in e-banking services is a regulatory framework that governs cyber security and data protection.

Linked with the sector going more digitalized with the passage of time as well as growing cyber security concerns in Pakistan, it is important that the impacts of such events on consumer trust and adoption of electronic banking are thoroughly understood. In order to study the multifaceted aspects which, shape the consumer behavior and the attitude towards the e-banking, in the country, Pakistan, a study would be done after considering the social, cultural, legislative or technical impacts.

1.4 Study Purpose

The focus of this research paper in the light of recent technological development is the investigation of the effect of the breaches of clients' data and frauds on customers' confidence and their e-banking adoption. Recognizing the result of consumer behavioral shifts and attitude

towards e-Banking will be vital to vigorously expanding e-Banking services in Pakistan, which are getting accelerated by mobile internet penetration and launching of new banking apps.

This study aims to delve into the following objectives:

1. Assessing the prevalence and nature of data breaches and fraud incidents in the e-banking sector in Pakistan: The research will measure disaster cases, badged-it up and take down banking platforms in terms of unauthorized access, phishing attacks, identity theft and card skimming.
2. Investigating the impact of security breaches on customer trust in e-Banking: The study is going to compare the former event and inform the level of consumer's perception, which is subsequently based on their experiences of psychological and behavioral dimension. By so doing, they will be able to gain vital information concerning electronic banking services safety, reliability confidentiality and privacy.
3. Investigation of the relationship between trust and adoption behavior in e-Banking: The question of the present study is the same as to what extent customers confidence in banks affects customers' willingness to use banking services whether it is to open an account transfer funds or to carry out transactions on the internet.
4. Analyzing the social, regulatory and technological factors that shape consumer attitudes towards e-Banking Security: The research will focus on the major attributes of culture step, legislation and technological infrastructure that are all aimed at reducing security risks and increasing banking customers' confidence.

This research aims to provide valuable insight into the complex dynamics of data breaches and fraud incidents in electronic banking, their impact on customer confidence and adoption in Pakistan by addressing these objectives. These findings will contribute to the development of strategies and interventions aimed at improving cyber security, strengthening consumer trust and promoting sustainable growth in e-Banking in Pakistan's digital economy.

Chapter 02

Literature Review

E-banking has witnessed significant global adoption due to its convenience and accessibility (Mishra & Anand, 2019). However, this growth has been accompanied by an increase in security challenges, including data breaches and fraud incidents. Research indicates that the proliferation of e-banking services has made financial institutions prime targets for cyber-attacks (Chakraborty et al., 2020). Data breaches and fraud incidents not only jeopardize customer trust but also pose substantial financial and reputational risks to banks worldwide (Choudhary et al., 2018). Studies have highlighted the detrimental effects of security breaches on customer trust and adoption of e-banking services. Research by Gupta et al. (2020) underscores that security breaches lead to a decline in consumer confidence, resulting in reduced usage of e-banking platforms. Similarly, Al-Ghazali et al. (2019) found that customers' trust in e-banking institutions diminishes significantly following security incidents, leading to decreased adoption rates and increased customer churn. Consumer perceptions of security play a pivotal role in shaping their attitudes towards e-banking services. Studies have shown that perceived security risks significantly influence individuals' trust and adoption behavior in electronic banking (Luarn & Lin, 2020). Research by Kim & Park (2018) suggests that enhancing customers' perceptions of security through robust cyber security measures can foster trust and encourage greater adoption of e-banking services. The regulatory landscape surrounding cyber security and data protection also plays a crucial role in mitigating security risks in e-banking. Research indicates that stringent regulatory frameworks are essential for safeguarding consumer interests and maintaining the integrity of e-banking systems (Lim et al., 2017). Effective governance mechanisms, including compliance with international standards such as GDPR and PCI DSS, are imperative for enhancing cyber resilience and building consumer trust in electronic banking platforms (Kshetri, 2021). Consumer attitudes towards e-Banking security and adoption are influenced by the differences between cultures. Research suggests that cultural factors such as individualism, collectivism, and uncertainty avoidance shape consumers' perceptions of risk and trust in electronic banking (Suh & Han, 2019). The importance of taking cultural dimensions into account when developing cyber security strategies and promoting trust

between different consumer segments is highlighted in Liang et al., 2020 studies. Technological advancements play a crucial role in enhancing the security of e-banking systems. Research has focused on innovative solutions such as biometric authentication, block chain technology, and artificial intelligence for bolstering cyber security in electronic banking (Kshetri & Voas, 2018). These advancements offer promising avenues for mitigating security risks and enhancing consumer trust in e-banking platforms globally. Educating consumers about cyber security best practices is essential for promoting trust and adoption in e-banking services. Research suggests that consumers can be empowered to recognize and reduce security risks by means of awareness programs and financial literacy initiatives, Alzahrani et al. 2020 Greater confidence in e-banking Platforms can be promoted by strengthening consumer knowledge and skills on topics such as password management, Phishing detection or safe online practice

Global trends driven by factors such as increased Internet penetration, the adoption of mobile phones and government initiatives to promote financial inclusion have played a role in developing electronic banking across Pakistan. E-banking encompasses a wide range of electronic transactions, including fund transfers, bill payments, and online purchases, facilitated through digital platforms such as internet banking, mobile banking, and automated teller machines (ATMs) (Khalid, 2020).

Despite the benefits of e-banking, the digital nature of transactions exposes consumers and financial institutions to various cyber security risks. Security breaches, including data breaches and fraud incidents, pose significant threats to the integrity and security of e-banking platforms. A data breach involves the unauthorized access, disclosure, or misuse of sensitive information, such as customer data and financial records, by malicious actors (Khan et al., 2019). Fraud incidents encompass deceptive practices aimed at manipulating electronic transactions for illicit gains, such as phishing, identity theft, and card skimming (Ali et al., 2021).

In e-banking, the impact of security breaches on customer confidence is profound. The key determinant of the relationship between the bank and the customer is trust, which influences the willingness of the customer to embrace e-banking services, Shahbaz et al., 2020 As a result of security breaches, consumer confidence in the safety measures taken by financial institutions is

undermined and concerns are raised as to the confidentiality and integrity of e-banking Platforms. Research indicates a strong relationship between customer trust and adoption behavior in e-banking. Consumers who trust in the security and reliability of e-banking platforms are more likely to adopt electronic banking services (Majeed et al., 2021). Conversely, security breaches undermine consumer trust, leading to decreased adoption rates and limited engagement with digital banking services. Understanding the interplay between trust and adoption behavior is essential for designing effective strategies to promote e-banking adoption in Pakistan.

The complexity of the security breaches in e-banking is exacerbated by the unique social, legal and technical environment of Pakistan. Consumer attitudes towards electronic banking are shaped by cultural factors such as concerns about privacy and safety, according to Majeed et al., 2021. In addition, the regulatory framework on cyber security and data protection plays an essential role in mitigating safety risks and promoting consumer confidence in electronic banking services.

While existing literature provides valuable insights into the impact of security breaches on customer trust and adoption in e-banking, several gaps remain to be addressed. Future research should focus on exploring the effectiveness of cyber security measures and regulatory interventions in mitigating security risks and enhancing consumer trust in e-banking platforms. Moreover, longitudinal studies are needed to assess the long-term implications of security breaches on e-banking adoption and consumer behavior in Pakistan.

2.1 Theoretical Framework

It could be said, more specifically, that these writings reveal the requirement for cyber-security problems to be solved so that the consumers' trust would be supported and the service of e-banking would expand in Pakistan's digital economy.

2.2 Trust Theory

The essential for the decision making and relationships in e-banking is trust theory. It is also prescribed by the theory of the trust because the service providers create such impression about their reliability, integrity, and competence Morgan & Hunt (1994). Factors like an individual opinion on security and the level of protection for privacy and transparency have a large influence

on customers when it comes to trust about e-banking. Shahbaz et al. 2020. Disrupting security does bring down the trust level to the limit by trespassing the expectation of confidentiality and integrity that degrade bank-client trust.

2.3 Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM) considers that the opinion on technology usefulness and user-friendliness is a major determinant in users' acceptance and adoption of new technologies (Davis, 1989). With regard to e-banking, customers are more eager to use the service when they see it as a pleasure to operate via a simple and safe interface. Khalid (2020) highlighted the unpredictability and safety of e-banks, and this could possibly bring about unwanted factors that may threaten perceived usefulness and ease of use. Such factors include security breaches and fraudulent activities which could, in turn, slow down their widespread adoption.

2.4 Information Security Theory

The idea of information security theory is to be aware of the importance of defense against the information asset and to assure the confidentiality, integrity, and availability of data (Anderson, 2001). The gaining accesses to e-banking may technically widen the doors of those who desire to violate information security principles, thus compromising customer data and financial records (Khan et al., 2019). Strategies of installing additional cyber security measures can be supported by the understanding of the reasons for the security breach hence the customers can feel secure in using e-Banking platforms again.

2.5 Cultural Dimensions Theory

Cultural Dimension Theory consists of two parts – first, cultural norms and values have a significant sway over human decision-making and second, technology use of people stands or falls depending on their attitude toward it. In Pakistan, societal factors, including concern about privacy, security, and trustworthiness, shape the individual's opinion on using e-banking (Majeed et al., 2021). Cultural dimension theory is a framework which provides insights in how culture affects customer's perception of cybercrime and fraud in e deposit banking, providing information on strategies to overcome cultural barriers that are mostly the reason consumers are not embracing

online banking. (Hofstede, 1980). In the thinking of Pakistan people, particular societal elements such as privacy, security, and trust act as determinants for loop in the uptake of e-banking (Majeed et al., 2021). Culture dimension framework enables one understand how cultural determinants affect the public evaluations of security leakages and wrongdoings in e-banking consequently guiding appropriate approaches to confront cultural barriers to its acceptance.

2.6 Regulatory Compliance Theory

The regulatory frameworks of Pakistan regarding cyber security and Data Security are instrumental in providing assurance of no digital security issues and earning the trust of customers to e-banking services. Ali et al., 2021 can be a guide to the development of strategies aimed at strengthening the regulatory institutions and making sure that the Institutions follow the safety standards to the letter.

Chapter 03

Methodology

3.1 Objective and Scope

This, questionnaire is aimed at assessing how data breach and fraud happen that thwarts the customer trust and adoption of e-banking by the people of Pakistan. With this regard, it will endeavour to find the different beliefs of the consumers about security, trust forming patterns and adoption behavior of e-banking.

3.2 Data Collection

The information obtained during the use of provided online questionnaires to bank clients. Measures on perceptions of security attacks, trust in e-banking, adoption behavior and demographic information are among the topics covered. Whether the target sample will be hard to reach or not, planned to outsource the questionnaire to the nearby population through:

Either personally or through online means. As data has been analyzed with the statistical methods like descriptive analysis, the patterns, relationships, and trends will be explored to make suggestions from the results.

3.3 Ethical Considerations:

Ethical principles guiding the research with human's sample, such as assuring the informed consent and protecting the anonymity/confidentiality of participants, are assured in this study. Before Researcher Ethical Approvals are granted by the Institutional Review Board (IRB) corresponding to the institution.

Chapter 04

Data Analysis and Interpretation

Details of respondent		Frequencies	Percentage (%)	Mean	Standard deviation
Gender	Male	56	66.7	1.6667	.48305
	Female	28	33.3		
Age	18-25	56	66.7	1.4286	.67612
	26-35	20	23.8		
	36-45	8	9.5		
	45 or above	0	0		
Qualification	Intermediate	24	28.6	1.8095	.60159
	Graduation	52	61.9		
	Masters	8	9.5		
	Other	0	0		
Occupation	Student	28	33.3	1.5238	.67964
	Employee	48	57.1		
	Business	8	9.5		
	Retired	0	0		
Do you use e banking services?	No	16	19.0	.8095	.40237
	Yes	68	81.0		
Do you feel e banking is more convenient than traditional banking regardless of risks associated with it?	No	8	9.5	.9048	.30079
	Yes	76	90.5		
Do you have any major concerns with data security when using mobile banking?	No	44	52.4	.4762	.51177
	Yes	40	47.6		

Do you believe that bank provide enough security on their websites and mobile applications?	No	20	23.8	.7619	.43644
	Yes	64	76.2		
Do you believe that confidentiality of information is protected in e-banking?	No	24	28.6	.7143	.46291
	Yes	60	71.4		
Did you face any data breach or fraud incident while using e banking?	No	64	76.2	.2381	.43644
	Yes	20	23.8		
Did the incident affect your trust and future use of e-banking?	No	60	71.4	.2857	.46291
	Yes	24	28.6		
Does your bank provide compensation for losses due to mobile banking fraud?	No	44	52.4	.4762	.51177
	Yes	40	47.6		
Do you believe that government regulations are necessary to ensure the security of e banking services in Pakistan?	No	12	14.3	.8571	.35857
	Yes	72	85.7		

Were you satisfied with the response of the e banking service provider to the data breach?	No	16	19.0	.8095	.40237
	Yes	68	81.0		
Do you believe e banking providers in Pakistan prioritize the security of customer data?	No	20	23.8	.7619	.43644
	Yes	64	76.2		
Did you adequately informed about the data breach and assistance by your e banking provider?	No	28	33.3	.6667	.48305
	Yes	56	66.7		
If you ever faced a data breach incident did it affect your willingness to adopt new e banking technologies or services?	No	40	47.6	.5238	.51177
	Yes	44	52.4		
Did the e banking provider handle the situation effectively following data breach or fraud incident?	No	16	19.0	.8095	.40237
	Yes	58	81.0		

Are you satisfied with the security measures provided by e banking providers in Pakistan?	No	20	23.8	.7619	.43644
	Yes	64	76.2		
Would you recommend e banking services to others based on your experiences?	No	4	4.8	.9524	.21822
	Yes	80	95.2		

Statistical interpretation and discussion

4.1 Usage of E-Banking Services:

Emphasizing the mean value of 0.8095, which reflects the percentage of respondents in Pakistan, who made use of e-banking services. Though the samples majority members have opted to use e-banking services, it can be noted that the sample population's modes of banking service usage vary (inferred by the standard deviation of 0.40237).

4.2 Perception of E-Banking Convenience:

However, this form of banking still presents potential risks. In light of this, people strongly choose e-banking over traditional banking as suggested by the average integer of 0.9048.

Relative to the use of e-banking versus traditional banking, consumers are generally in concurrence as observed with the standard deviation values of 0.30079 that is considerably low. The mean

value of 0.4762 refers to the fact that for mobile banking, the respondents gave a leading role to data security-related concerns by reporting on them more frequently.

The responses with a high standard deviation of 0.5117 greatly differ from one respondent to another, betraying the fact that while some respondents consider data security a profound challenge, others may not be so worried. Looking at the midpoint or mean value of 0.7619, it is perhaps the safest to conclude that the majority of the respondents feel that the banks have sufficiently done in this regard.

Despite a little bit of dispersion fact we see, the mean standard deviation 0.43644 proves the general opinion respondents have is that bank security systems are sufficiently secure.

4.3 Information Confidentiality in E-Banking:

Having in mind the fact that the average response rate is 0.7143, it can be stated that most respondents generally accept that information security in e-banking is protected very well. Responses differed and showed lower Faith in the certainty of the privacy protection, standard deviation of 0.46291.

4.4 Experience of Data Breaches and Fraud Cases:

With the mean value at 0.2381, it is evident that the minority of the respondents perceived slim chance that their data would be breached or finances would be affected by fraud when using online banking. The standard deviation of 0.43644 represents the range of differences among respondents as to how data breach incidents have impacted them in their experiences.

4.5 Effect of Incident on Trust and Future Use:

Reflecting this mean value, i.e., 0.2857, the statement suggests that customers, on average, experienced a considerable trend of lowered confidence and/or discharge from e-banking transactions as a result of accomplishing fraud or cracking of their account's data.

The range of answers that impacted a searcher's trust in online banking and future use of it is shown by the difference in the z-scores (standard deviation) of 0.46291.

4.6 Bank Compensation for Fraud Losses:

Consequently, from the average answer rate which equals 0.4762, it seems that banks do not reimburse them for loss which is caused by mobile banking and owe the customer for such incident.

With regard to compensation for fraud losses by banks, the answer is not uniform whereas the medium of deviation indicates this variation which is shown in the form of a standard deviation of 0.51177.

4.7 Government rules Are Necessary:

The essence of the mean value of 0.8571 was that the majority of the respondents require government regulations for smooth running of e-Banking services. Diverse responses could be seen as the moderate standard deviation of 0.35857 suggests, yet characterizes the agreement similar to the view of employee about regulation.

Satisfaction with E-Banking Service Provider's Response to Data Breach: If we assume the average mean of 0.8095 as the data breach handling score, it is gratifying to see that respondents as a whole were happy with the service provider.

4.8 Perception of the Security Priority of E-Banking Providers:

The score average of 0.7619 itself represents that the major proportion of people thought that e-banking service providers are most concerned with the user's data security in Pakistan.

The standard deviation of 0.43644 implies that there is variation and difference in respondent's perception.

4.9 Informational Awareness and Assistance:

The average score of 0.6667 outlines the fact that, on the whole, responders evaluate themselves as being pretty knowledgeable when it comes to identifying if there is a security breach as an online banking customer. The consensus on the respondents' levels of information literacy, and help available may not be as much as assumed based on the statistical mean as indicated by standard deviation of 0.48305 which is not small.

4.10 Impact of Data Breach on Adoption of New Technologies:

The response rate of 0.5238 is a confirmation of the fact that on average the participants quoted that the data breaches impede their readiness to use electronic banking services or technology at a moderate level. The high standard deviation of 0.51177 shows that data breaches incidents were found to provide a influence which varied to different extents on individuals' propensity to adopt new technology.

4.11 Satisfaction with Security Measures:

Satisfaction with Security Measures: According to the mean value of 0.7619 in this case, we would say that generally respondents are able to get the security guarantees from local Pakistani banks through online banking channels.

While the respondents show a divergence in terms of how they rate their satisfaction levels, the standard deviation indicates a level of variation of 0.43644.

4.12 Recommendation of E-Banking Services:

The mean of the responders' substitute was of 0.9524. It, therefore, manifests that the responders would have no inhibitions to recommend banking transactions through the internet to other people that they had previously observed. The normalized small standard deviation is 0.21822 where in high level of agreement is found between responders regarding the likelihood to recommend e-

Banking rather e-banking services to family and friends. The survey bears witness to the increasing tendency to use internet the convenient way to process various banking transactions and operations thus confirming favorability for e-banking services. It proves, from evidence, that e-banking is more convenient than the traditional banking, though the accompanying risks are considered by a larger number of members of the society. The calculated mean, median, and mid-point values obviously suggest the financial convenience seen by majority of the respondents in e-banking. On the other hand, a low standard deviation suggests that population is pretty much on the same trend line confirming that majored group think the same regarding this perception.

These findings emphasize a fact that e-banking is becoming more and more popular, whereas traditional banking facilities are being replaced with latest e-solutions. This data can be used by financial institutions for improving the e-banking services by making users' experience enjoyable and handling the risks to encourage more people to adopt the financial services. In addition, while making the rules and regulations governance of digital money services, legislators and regulators could possibly include them. The e-banking is seen as more convenient than conventional banking which may be explained as a beginning of digital transformation of the banking industry to fulfill the fast-evolving requirements and preferences of the customers. It reveals that across online banking and traditional banking, the evaluations of clients are not of similar consistency. With the value below 0.5, indicating a general-predilection-to-this-perception, the mode demonstrates that the most common response is that online banking is less convenient. While the high standard deviation does not deny the variability in the population respondents and therefore raises doubt on the uniformity of the population belief system. The importance of the above finding indicates to the fact that without taking care of the security of the mobile apps as well as of the websites it will be almost hard for the banks to manage their customers. A good security perception builds trust among clients, customer loyalty, and increase in the use of online banking services. Moreover, it can help banks to attract customers in a competitive market by projecting the image of a bank being professional and trustworthy custodians of financial information and funds safety.

Based on the study, for average user 28.57% often experience banking fraud or data breach. Standard deviation is showing some sort of a difference in incidents of respondents, while median and mode indicate that most respondents (more than 50%) did not experience any of those incidents.

The investigational data yields that with regard to security of e-banking, on an average, 28.57% of the respondents compare the two. The standard deviation does provide a glimpse into the number variance in incidents occurrence among respondents; however, the median and mode value indicates that a predominant number of respondents (more than 50%) did not experience the same.

The data received differ from each other where some respondents were victims of fraud while others lost data in both cases. 23.81% usually to 28.57% are the occurrence rate. While the main category of health issues echoed the same thoughts these responders did not come across such problems. The standard deviation suggests that the level of experience differs among the responders as it varied within the study sample, giving a clue that the majority did not have any issues but some did. These fluctuations point to how significant is to maintain the cyber protection tight the hackers and criminals cannot breach the information of the consumers because the consumers rely on the services thereby their confidence plumps in the services. This data indicates that there is quite a contrast in the ways in which people see whether or not Pakistani e-banking services must be regulated with rules.

Chapter 05

Limitations, Conclusion and Recommendation

5.1 Limitations

Such responses are based on the self-assessment information provided by the respondents. However, the rating made may be biased depending on many factors for which respondents may have to rely on their knowledge, social position, and other aspects. There can come imprecision in the data provided if respondents say what they think is right are if they cannot reproduce their experiences exactly. Here the results of the research conducted are going to have only a narrow scope and cannot be directly translated for the majority of the species outside of the considered population. The study dedicated to the Pakistani attitudes to e-banking was carried as the main research. The impact may be significant for particular countries with the social and economic situation differing from the one as in the case of this document. There's the possibility that people were answer to the question from their lifestyle or view. Philosophically, individuals who have had second thoughts and ignored online banking security may opt for the poll, and their impressions might be the ones that will be considered important. The research that bears the issue may have used all the data obtained at one time which can be considered as a profile of the thoughts and experiences of the respondents. A study by longitudinally design can filled the sense of security in e-banking perception by depicting the happening of attitudinal and behavioral changes in time. At the point that some elements of e-banking security like effectiveness of specific security measures or particular fraud occurrence types were not shown in the study, there is still a huge gap in understanding e-banking security. Moreover, the study would have been more vigorous and could have been viewed from various angles by being stricter in the research.

5.2 Conclusion

This study was concentrated on the security of E-Banking which reflects the complexity of Digital Financial Services across in Pakistan. Several crucial findings have surfaced in a comprehensive examination of the survey information, which are very helpful in understanding the issues and chances of e-banking. Consequently, the researches brought out a high rate of e-Banking adoption among respondents pointing at the fact that they are gradually shifting to digital platforms for financial services. Despite the wide usage, critical data security issues in mobile banking were found out as most of the participants were expressing their concern about their personal data being protected. Moreover, there was still a wide range of opinion about the efficiency of these measures in the opinion of the survey participants regarding the banks' overall assurance that they take appropriate security measures on their websites and applications. It stresses the significance of unceasing initiatives through financial institutions geared towards security enhancement and guarantee of users' peace of mind.

The study has also given some view on how security issues influence customers' trust and adoption behavior. With a few cases of data breaches and fraud, but their influence in perception of trust and future electronic banking use were strong. That is why it is imperative to talk about these security risks if we want to maintain customer trust and to make sure e-Banking is sustainable in Pakistan. Moreover, the study indicated that the government regulation is taken crucial role in the security of e-Banking services. A common ground among respondents in the need for regulatory frameworks that shield consumers' interests and boost trust in the Digital Financial Ecosystem was uncovered. Moreover, public research makes evident the fact that governmental regulation is of great significance when it comes to providing safety e-Banking services. Respondents either way showed their support for the rule systems that will give consumer interests the defense and as well as help build trust in Digital Financial Systems. On the whole, people demonstrate satisfaction with response of e-Banking service providers to security incidents by socializing the data on security threat. While that, possibilities of better communication and transparency ought to be sought in situations of breaches of personal data and the aid provided to the users who have been affected. Another important point in this study is the fact that the current situation of being on the

alert and implementing preventive measures is needed to respond to the threats which arise in the e-Banking. Through prioritizing trust, security, and collaboration among stakeholders, Pakistan has good chance to overcome the challenge of digital financial Services and have a grip on e-Banking advantages for Poverty reduction, economic growth and financial entrepreneurship. The output illustrates the main ideas that arose from the study, emphasizing the crucial points for e-banking stakeholders and signaling the potential routes for further research and action.

5.3 Recommendations

5.3.1 Strengthen Security Protocols:

E-banks need to be all-time enlisting with reinforced security programming to nullify the risk of cyber-attacks and safe guard the client information. This is done, which includes multi-factor authentication implementation, encryption methods, and frequent security audits to find and eliminate the weak points.

5.3.2 Raise Awareness and Education:

Start the educational initiatives that help the clients to know the good practices for e-banking safety, so they never fall for phishing scams, create the strong passwords and monitoring the account activity closely! With the skills they will learn, the users will be to detect and guard against all security issues and they will be able to make rational decisions based on the knowledge they gained.

Envisage the exhaustive incident response procedures to tackle the fraud and data breaches in the shortest time. Hence, communicating with consumers, particularly notifying the ones who are going to be impacted, and helping and supporting them, are the essential parts of this task.

5.3.3 Boost Regulatory Structures:

Cooperate with the regulatory agencies to design a third-party control system for security and data protection of e-banking. To ensure complexness with the security necessities and in protection of

the consumer interests, include this indirectly in the directives, and the rules and monitoring procedures.

5.3.4 Improved Transparency and Communication:

In case of e-banking failing in security the main task for a company is to support and to improve the transparency and client's trust. This would entail ensured people early and clear information about security breaches, and outline of the actions taken in order to fix them, and giving out information on self-defense tactics.

5.3.5 Invest in Technological Innovations:

In order to ensure the high level of the online banking security the means for the biometric identification, the machine learning, and the artificial intelligence, should be used. Customers would get strong reassurance through these developments which can help in real-time fraud detection and prevention that ultimately.

5.3.6 Frequent observation and assessment:

Define monitoring procedures and reporting in place to track the performance of security measures and the perception of customers long-term. That would allow e-banking providers to identify the most acute points, to catch added risks and adjust plans when customer needs and preferences change.

5.3.7 Encourage Financial Inclusion:

Make sure that e-banking services are at hand to and inclusive of all segments of society, particularly people of less privileges and those who are living in rural areas. These can be done through empowering digital literacy programs, delivering tailor made services and expanding data coverage, for instance.

5.3.8 Ongoing Investigation and Education:

Ensure that dedication and data exchange of customers on perceptions of e-banking and security are given continued attention. It requires continually updating and gaining new knowledge through longitudinal research, benchmarking against international best practices, and collaborating with

expert's world. The e-banking institutions as well as the regulators, the lawmakers, and other stakeholders will have to come together, put forward these proposals and ensure that this becomes a reality. Pakistan can motto a fearless and all-inclusive e-banking system relying upon financial stability and enabling which for all individuals by giving emphasis to security, transparency, and consumer trust.

References:

1. Ali, F., Hanif, M., & Ahmad, M. (2021). Cyber Fraud Detection Techniques: A Comprehensive Survey. *IEEE Access*, 9, 120997-121018.
2. Khalid, S. (2020). Adoption of E-Banking in Pakistan: An Empirical Investigation. *Journal of Business and Social Sciences*, 4(2), 7-21.
3. Khan, M. S., Iqbal, S., & Butt, A. A. (2019). Impact of Data Breaches on Consumer Trust: A Study from Pakistan. *International Journal of Information Management*, 49, 37-47.
4. Majeed, S., Khurshid, M., & Shaheen, M. (2021). Factors Affecting Customer Adoption of Internet Banking in Pakistan: A Moderating Role of Customer Trust. *International Journal of Bank Marketing*, 39(1), 35-55.
5. Shahbaz, M., Sattar, A., & Zia, M. (2020). Understanding the Role of Trust in E-Banking Adoption: An Empirical Investigation from Pakistan. *International Journal of Bank Marketing*, 38(5), 1042-1061.
6. Ali, M., Raza, A., Zaidi, S. H., & Syed, A. (2021). Phishing and its Impacts on E-Banking Customers: A Study of Pakistan. *Information and Communication Technologies in Modern Banking Operations*, 155-175.
7. Khalid, M. (2020). Adoption of E-banking in Pakistan: A Study on the Major Factors Affecting. *Journal of Asian Finance, Economics, and Business*, 7(8), 715-722.
8. Majeed, S., Iqbal, J., & Javaid, A. (2021). Determinants of Customer Trust in E-banking: An Empirical Study from Pakistan. *Journal of Islamic Accounting and Business Research*, 12(1), 48-65.
9. Shahbaz, M., Zakaria, N. H., & Hussain, A. (2020). Customer's Trust in E-banking and its Relationship with Adoption: A Study of Pakistan. *Future Business Journal*, 6(1), 1-12.
10. Khalid, M. (2020). Adoption of E-banking in Pakistan: A Study on the Major Factors Affecting. *Journal of Asian Finance, Economics, and Business*, 7(8), 715-722.
11. Khan, A. B., Niazi, M. K., Khan, I. A., & Ahmad, R. (2019). Fraud Detection in Banking Sector Using Machine Learning: A Case Study of Pakistan. *Journal of Advanced Research in Dynamic and Control Systems*, 11(2), 2051-2060.

12. 15. Majeed, S., Iqbal, J., & Javaid, A. (2021). Determinants of Customer Trust in E-banking: An Empirical Study from Pakistan. *Journal of Islamic Accounting and Business Research*, 12(1), 48-65.