Kaunas University of Technology
School of Economics and Business

Recovering Consumer Trust in FinTech Products After a Data Breach

Master’s Final Degree Project

Shah Fahad
Project author

Assoc. Prof. Dr. Rita Jucevičienė
Supervisor

Kaunas, 2025

Kaunas University of Technology
School of Economics and Business

Recovering Consumer Trust in FinTech Products After a Data Breach

Master's Final Degree Project

International Business (6211LX029)

Shah Fahad
Project author

Assoc. Prof. Dr. Rita Jucevičienė
Supervisor

Prof. Dr. Mantas Vilkas
Reviewer

Kaunas, 2025

Kaunas University of Technology
School of Economics and Business

Shah Fahad

Recovering Consumer Trust in FinTech Products After a Data Breach

Declaration of Academic Integrity

I confirm the following:

1. I have prepared the final degree project independently and honestly without any violations of the copyrights or other rights of others, following the provisions of the Law on Copyrights and Related Rights of the Republic of Lithuania, the Regulations on the Management and Transfer of Intellectual Property of Kaunas University of Technology (hereinafter – University) and the ethical requirements stipulated by the Code of Academic Ethics of the University;

2. All the data and research results provided in the final degree project are correct and obtained legally; none of the parts of this project are plagiarised from any printed or electronic sources; all the quotations and references provided in the text of the final degree project are indicated in the list of references;

3. I have not paid anyone any monetary funds for the final degree project or the parts thereof unless required by the law;

4. I understand that in the case of any discovery of the fact of dishonesty or violation of any rights of others, the academic penalties will be imposed on me under the procedure applied at the University; I will be expelled from the University and my final degree project can be submitted to the Office of the Ombudsperson for Academic Ethics and Procedures in the examination of a possible violation of academic ethics.

Shah Fahad

Confirmed electronically

Shah Fahad. Recovering Consumer Trust in FinTech Products After a Data Breach. Master's Final Degree Project/Supervisor Assoc. Prof. Dr. Rita Jucevičienė; School of Economics and Business, Kaunas University of Technology.

Study field and area (study field group): Business, Business and Public Management.

Keywords: FinTech, Trust Recovery, Data breach, Consumer trust

Kaunas, 2025. 79 p.

Summary

The research was conducted to study the factors influencing trust recovery post-data breach. For these purposes, an extended version of the Technology Acceptance Model (TAM) was employed. The Model consisted of core TAM elements along with other variables, which were identified via theoretical review, based on current studies. Those variables were transparency, cash culture, regulatory challenges, cybersecurity awareness, perceived risk, and core TAM elements, i.e, perceived usefulness and perceived ease of use.

For the research, a quantitative research methodology was used, and victims of cybercrime from the Pakistani FinTech market were presented with a questionnaire. A total of 187 valid responses were received, shedding light on factors that either positively or negatively impact trust recovery in FinTech. The study revealed that transparency, security, and cash culture were the most significant predictors of trust recovery post-data breach. An ever deeper analysis revealed that among these three predictors, transparency was the most impactful factor, followed by perceived security and cash preference. This proves that post-data breach consumers prefer the FinTech firms to be transparent about the incident, and would like to stay abreast of the prevailing scams and frauds. The analysis also showed that consumers preferred visible security features, which also highlights the importance of effective communication. Cash preference negatively impacts the trust recovery, but also requires a deeper qualitative analysis for a better understanding.

The analysis showed that core elements of TAM, such as perceived usefulness and ease of use, which are very important in the initial trust development phase, failed to make a significant impact on trust recovery post-data breach. Similarly, cybersecurity awareness, regulatory challenges, and perceived risk were also found statistically not significant. It means that conventional factors aren't sufficient to define trust recovery in FinTech. However, these results do not lower the theoretical importance of these factors in FinTech adoption and trust development.

Finally, the research highlights the importance of effective communication, transparency, visible security updates, and the need to discourage cash culture. Since core TAM factors failed to encapsulate the trust recovery idea, there is a need to extend the model beyond the conventional variables to emotional and cultural dimensions as well. These findings can be valuable for policymakers and FinTech companies. Lithiania, being at the forefront of financial innovation, can utilise this study to expand their market reach ot emerging markets like Pakistan.

Shah Fahad. Vartotojų pasitikėjimo finansinių technologijų produktais atkūrimas po duomenų saugumo pažeidimo. Magistro baigiamasis projektas / vadovė doc. dr. Rita Jucevičienė; Kauno technologijos universitetas, Ekonomikos ir verslo fakultetas.

Studijų kryptis ir sritis (studijų krypčių grupė): Verslas, Verslas ir viešoji vadyba.

Reikšminiai žodžiai: Pasitikėjimo atkūrimas, Duomenų pažeidimas, Vartotojų pasitikėjimas.

Kaunas, 2025. 79 p.

Santrauka

Šio tyrimo tikslas buvo ištirti veiksnius, darančius įtaką pasitikėjimo atkūrimui tarp Pakistano FinTech vartotojų po duomenų pažeidimo. Tyrime buvo naudojamas išplėstas technologijų priėmimo modelis (TAM), papildytas pasitikėjimo veiksniais, tokiais kaip skaidrumas, suvokiama rizika, suvokiamas saugumas, grynųjų pinigų kultūra, reguliaciniai iššūkiai, informuotumas apie kibernetinį saugumą, suvokiamas naudingumas ir suvokiamas naudojimosi paprastumas.

Buvo taikyta kiekybinė tyrimo metodologija, remiantis 187 tinkamais atsakymais iš FinTech srityje kibernetinių nusikaltimų aukomis tapusių vartotojų. Tyrimas parodė, kad skaidrumas, saugumas ir grynųjų pinigų kultūra yra reikšmingiausi pasitikėjimo atkūrimo prognozuotojai. Išsamesnė analizė atskleidė, kad tarp šių trijų veiksnių skaidrumas buvo stipriausias pasitikėjimo atkūrimo prognozuotojas. Tai pabrėžia savalaikio duomenų pažeidimų atskleidimo ir vartotojų informavimo apie vyraujančias sukčiavimo ir apgavysčių schemas svarbą. Suvokiamas saugumas buvo antras pagal svarbą pasitikėjimo atkūrimo prognozuotojas tarp FinTech vartotojų. Vartotojai vertina matomus saugumo atnaujinimus, ypač po patirtos pasitikėjimo krizės. Priešingai, pirmenybė gryniesiems pinigams turėjo neigiamą poveikį pasitikėjimo atkūrimui, o tai rodo, kad kultūrinės kliūtys išlieka svarbiu veiksniu tokiose besivystančiose rinkose kaip Pakistanas.

Analizė parodė, kad pagrindiniai TAM veiksniai, tokie kaip naudingumas ir naudojimosi paprastumas, neturėjo reikšmingos įtakos pasitikėjimo atkūrimui. Taip pat buvo nustatyta, kad informuotumas apie kibernetinį saugumą, reguliaciniai iššūkiai ir suvokiama rizika neturėjo statistiškai reikšmingos įtakos pasitikėjimo atkūrimui. Šie rezultatai leidžia manyti, kad įprasti pasitikėjimo prognozuotojai yra nepakankami aiškinant pasitikėjimo atkūrimą.

Tyrimo rezultatai pabrėžia aktyvaus bendravimo su vartotojais, matomų saugumo atnaujinimų ir kultūrinių kliūčių, tokių kaip pirmenybė gryniesiems pinigams, sprendimo svarbą, siekiant veiksmingai atkurti vartotojų pasitikėjimą. Tyrimas taip pat pabrėžia poreikį išplėsti TAM modelį, įtraukiant kultūrinius ir emocinius aspektus tiriant vartotojų elgseną po duomenų pažeidimų. Lietuva, būdama FinTech inovacijų priešakyje, gali pasinaudoti šia galimybe ir plėsti savo veiklą potencialiose rinkose, tokiose kaip Pakistanas. Šie rezultatai gali būti vertingi tiek politikos formuotojams, tiek FinTech vadovams.

Table of Contents

List of Figures

List of Tables

List of abbreviations and terms

Terms:

FinTech	Financial Technology
TAM	Technology Adoption Model
PU	Perceived Usefulness
PEOU	Perceived Ease of Use
PII	Personally Identifiable Information
FIA	Federal Investigation Agency (Pakistan)
OTP	One Time Password
AI	Artificial Intelligence
ATM	Automated Teller Machines
UAN	Universal Access Number
EMI	Electronic Money Institution
PSO	Payment System Operator
BNPL	Buy Now Pay Later
IoT	Internet of Things
SBP	State Bank of Pakistan
SIM	Subscriber Identity Module
KMO	Kaiser-Meyer-Olkin

Introduction

Relevance of the selected topic:

FinTech, a portmanteau of “Finance“ and “Technology”, refers to the integration of financial services provided through innovative solutions to enhance their delivery and efficiency. According to a report by Klynveld Peat Marwick Goerdele (KPMG, 2023), global investment in FinTech for the year 2023 amounted to around $113.7 billion. Financial technology, or FinTech, has become crucial to the financial services industry and has transformed it for the better. Leong and Sung (2018) characterize FinTech as a cross-disciplinary subject that synthesizes finance, technology management, and innovation management. One explanation defines it as innovative ideas that can improve financial services by using technological solutions (Sung, 2018). Ayman Mansour (2021) mentions that FinTech has made it possible to move a huge amount of money and make bulk transactions efficiently, and that is why it has not only transformed the way of doing business but has also acquired a center stage in the eyes of decision-makers globally.

Empirical studies indicate that younger demographics prefer digital interaction over face-to-face, reflecting their inclination towards using digital products and services more often than others (Šmahel, 2020). For younger generations, digital technologies play a central role in their daily life since it’s a fusion of digital and physical space (Ayllón, 2020). This makes them a potential market for such FinTech platforms. Overall, in the EU, people between 16-74 have basic digital skills. The Eurostat survey shows that people between the age bracket of 16-44 show high digital skills among both men and women (Eurostat, 2024). People in the older age bracket had a declining trend in digital skills.

This technological revolution came with challenges such as cyberattacks, data theft, and identity theft. These challenges undermine the ability of FinTech firms to maintain trust among their customers. The operational aspect of these FinTech companies makes them vulnerable to data breaches and attacks since they store a large amount of sensitive customer financial and non-financial data. While financial data can be used for economic purposes, non-financial data can also be used for malafide purposes, such as identity theft. Such data breaches can damage customer trust in these FinTech platforms.

Both developed and developing economies face some kind of challenges in maintaining trust in FinTech. For example, developed economies face more frequent cyberattacks and ransomware, which can undermine consumers' trust in the platform’s integrity and strong digital infrastructure. Conversely, developing economies face exacerbated data security risk due to limited digital literacy, & unreliable internet infrastructure. FinTech firms find it increasingly difficult to establish trust, especially since it has been damaged due to a data breach or scam.

Consumer trust, as defined by Jaspers (2022) is consumers' expectation that personal information and sensitive details will not be misused. Maintaining consumer trust is the backbone of success for digital payment platforms, but incidents of breaches and unauthorized access still occur (Chakraborty, 2022). Once a customer suffers a data breach or an online scam, their trust has been broken, and now the fintech firm must earn it back. However, to re-establish trust in FinTech consumers, we must first identify the barriers to establishing trust after a data breach.

Research has confirmed that fears of insecurity and cybercrime intensify once a consumer experiences online banking fraud (Cross, 2022). This behavioral change then negatively impacts the FinTech product and service adoption rates. Consumers' trust in the security and reliability of the overall digital infrastructure is damaged once they experience some kind of digital financial fraud (Tade, 2020). As a result, online freedom, comfort, and opportunities shrink (Gupta, 2022). On top of that, consumers who suffered cyberattacks or digital financial fraud are hesitant to report such incidents to the authorities (C., 2018).

A lot of research has been done on factors and barriers of trust in FinTech, but little to no work has been done on how data breaches and scams shatter consumer trust and what can be done to establish that trust again among consumers (Cook, 2023). This research addresses a critical gap in the literature by analyzing the barriers to trust in FinTech after a data breach and strategies for trust restoration that FinTech platforms can utilize. This will be useful for further studies and policymakers to draft better-suited strategies & policies in the rapidly evolving security landscape of FinTech.

Methods of Research: This study employed a quantitative research methodology to examine the factors influencing trust recovery among Pakistani FinTech consumers following a data breach. Data was collected through a structured online questionnaire targeting individuals who had experienced FinTech-related cybercrime. A total of 187 valid responses were analyzed using SPSS, applying descriptive statistics, correlation analysis, multiple regression, and exploratory factor analysis. The extended Technology Acceptance Model (TAM) served as the theoretical foundation, incorporating additional trust-related constructs to test their predictive power on perceived trust recovery.

Structure of Thesis: The thesis is structured into six main chapters. Chapter One introduces the research problem, objectives, and significance of the study. Chapter Two presents a detailed literature review, covering the theoretical foundations of trust, the Technology Acceptance Model, and relevant empirical studies. Chapter Three outlines the methodological approach, including data collection and analytical techniques. Chapter Four presents the results of the quantitative analysis. Chapter Five discusses the findings in relation to existing theories and research. Finally, Chapter Six provides practical recommendations, theoretical implications, and suggestions for future research.

1. Problem Analysis

The research focuses on the main obstacles that prevent trust recovery in FinTech sector operations after data breaches occur. The analysis investigates how digital financial services have become more popular while cybercrime rates increase, which leads to declining consumer trust. The research investigates particular problems faced by FinTech users in emerging markets such as Pakistan, which include inadequate regulatory systems and limited digital knowledge and cultural preferences for cash transactions. The identified factors serve as the foundation to establish the research gap and demonstrate why this study requires an extended trust-based model.

1.1. Importance of FinTech in the Modern World

The history of FinTech is often misunderstood as a recent phenomenon. Historically, it can be traced back to 1866 with transatlantic cables and telegraphs. There are three stages of the FinTech revolution:

1. 1866-1967: The first phase of FinTech, when financial information was transmitted using telegraphs and transatlantic cables.
2. 1967-2008: The second phase started when financial institutions used information technology in the form of automated teller machines, clearing systems, and other electronic payment channels.
3. 2008-present: The present phase is where financial services are available on an individual basis (Patria Laksamana, 2023).

Nicoletti (2017) believes that the term FinTech emerged when Citicorp established the Financial Services Technology Consortium (FSTC) in the 1990s. The purpose of FSTC was to establish a bridge between financial institutions and technology providers. Every researcher and scholar defines FinTech in a slightly different way:

- Xin (2015) highlights how financial technology has made access possible to online payments, mobile financial services, savings, and investments, etc.
- Leong (2017) defines FinTech as the "design and delivery of financial products & services through technology".
- Abbasi (2021) consider FinTech to be a key element in the fourth industrial revolution.
- Huang (2022) defines FinTech as a combination of "software, algorithms, applications, and hardware for multiple platforms, such as internet, mobile devices, wearables, and virtual reality".

The transition of FinTech shows how it evolved from bridging financial institutions to catering to individual consumers' financial requirements. Consumer behavior, attitudes, and preferences have also evolved and transformed with these new technologically innovative services, for example, digitized payment systems, banking, and now rapidly evolving AI applications.

Consumers can use FinTech products and services for their everyday payments, financial decision-making, chatbots, and advisory services. This is why, in some regions, FinTech has reached a scale where it has disrupted conventional banking services altogether (Buckley, 2016).

Xiao Xiang (2017) highlights the importance of AI in FinTech by mentioning how voice recognition, machine learning, deep learning, and image recognition services have transformed the financial service industry. It doesn't just give consumers a seamless experience but also helps them in the economic decision-making process, and as a result, it has optimized operational efficiency. However, the role of blockchain and distributed ledger technology, cloud computing, and IoT will give FinTech a solid boost in the future (Market Data Forecast, 2022). To reap the fruits of these endless possibilities, non-financial companies like Google, Apple, and even social media platforms have started offering and developing their FinTech services. Boston Consulting Group estimates that the global FinTech market is expected to grow to the size of $1.5 trillion in revenue by 2030 (BCG and QED, 2024). For the past two years, FinTech revenues have grown by 14%. While Market Data Forecast (2022) forecasts a growth rate of 25.18%.

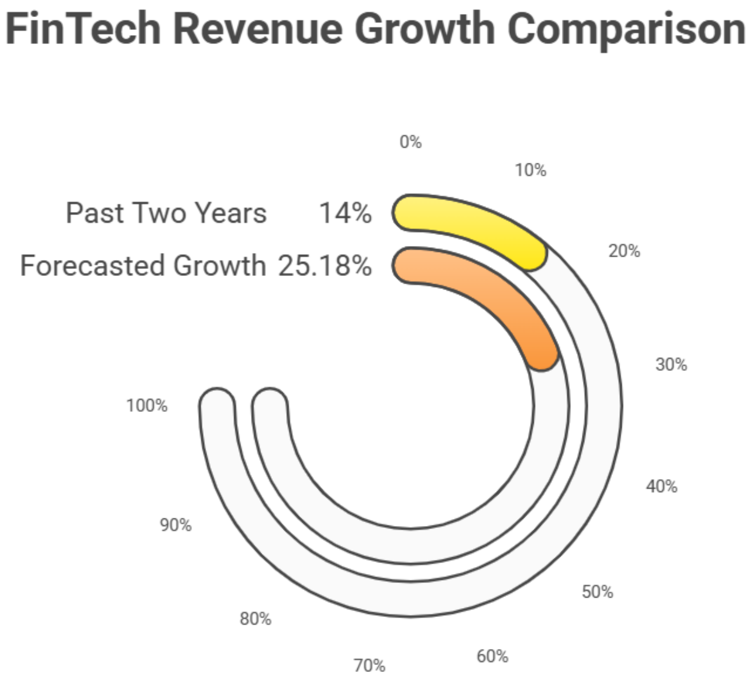


Figure. 1. FinTech Revenue Growth Comparison (Prepared by Author)

1.2. Trust Challenges in the FinTech Sector

Firmansyah (2023) concluded that among all the studies, “trust” has been considered an essential element in improving FinTech adoption. He presents the notion that FinTech transactions are virtual and, therefore, require a higher level of trust from the consumer. Zhang (2003), Whitman (2009), Siau (2003) studied elements that influence trust:

- Data confidentiality
- Integrity
- Availability
- Mobile application usability
- Transactional security
- Trustworthiness of the organization.

In developed economies where the digital structure is strong and literacy rates are higher, cyberattacks and ransomware have exposed vulnerabilities in FinTech firms, which damages consumers' trust. Such concerns are more significant in developing economies like Pakistan, where digital literacy and internet penetration rates are low (Erum Irfan, 2022).

The Pakistani FinTech market has been chosen to conduct this study because of the rapidly growing consumer demand in the FinTech sector. Especially with lower levels of digital literacy and high susceptibility to data breaches and scams, it offers critical insights into understanding trust dynamics.

A country with more than half of its population comprising young individuals with a median age of 22 and with more than 100 million mobile broadband subscribers holds immense potential for FinTech growth (McKinsey & Company, 2022). The ever-increasing number of smartphone users and the growing freelance market will continue to fuel this growth for years to come. In previous years, the government introduced initiatives such as issuing Electronic Money Institutions (EMIs) and digital banking licenses. These initiatives are aimed at supporting FinTech startups with the help of 300,000-plus tech professionals.

As per the official reports, the number of mobile users has risen from 1.4 million in 2012 to 12.3 million in 2022. The volume of digital transactions in the country was recorded to be 12.3 million in 2022, and the value was 12 trillion rupees, whereas in 2012, it was 3.3 million and 13.6 billion rupees (Banking Mohtasib Pakistan, 2023).

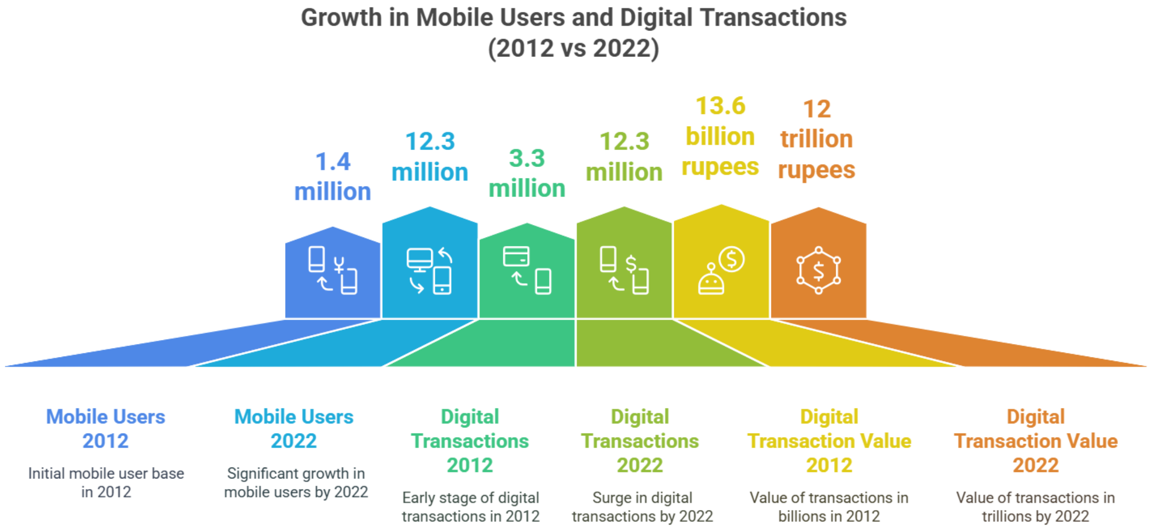


Figure. 2. Growth in Mobile Users & Digital Transactions (Prepared by Author)

What are the factors that act as barriers to trust restoration once a data breach or fraud has occurred?

The digital revolution has redefined the financial sector through new innovative solutions such as digital wallets and mobile applications. These innovative solutions provide the opportunity for consumers to benefit from lower transaction costs, enhancing inclusivity (Ayse Demir, 2022). Singh argues that despite the exponential growth and numerous benefits of FinTech, the acceptance rate among users is still low, particularly because of a lack of trust (Singh, Sahni, & Kovid, 2021).

Trust as a Critical Factor for FinTechs

There are some inherent vulnerabilities in FinTechs that can expose a consumer to various online/offline risks. These risks make the concept of trust a vital element for long-term sustainability (Joubert, 2013). FinTech companies manage a lot of sensitive financial and non-financial data that can be used for malicious purposes. Breach of this sensitive data would damage the trust of consumers beyond repair. Therefore, protecting this sensitive data is naturally the top priority for any FinTech firm (Meena Akileswaran, 2024). When users are assured that their data is safe, they tend to share information and make payments and purchases more comfortably, which enhances their trust in the FinTech platform or service (Bongomin, 2020).

The case of Pakistan in FinTech

The reason for choosing Pakistan for this study was because of its rapidly growing FinTech sector. As an emerging market, it has its advantages along with some challenges related to consumer trust and digital security. With a massive upward potential, the Pakistani FinTech market coexists with a cash culture, along with growing digital payment platforms. What makes trust recovery a critical issue in the Pakistani FinTech industry is the lack of cybersecurity awareness among consumers and a weak regulatory environment. Cash is considered a symbol of control, and digital literacy rates are very low. Along with that, the country is gifted with a larger young population ready to embrace FinTech. This complex web of cultural, technological, and institutional factors makes Pakistan a good case to study factors that impact trust recovery post-data breach.

Memon (2015) considers financial theft, malware, money laundering, hacking, and electronic terrorism as cybercrimes. In Pakistan, more than 600 consumers from 22 banks collectively suffered a financial loss of $11.7 million due to such cyberattacks in one incident alone (Shahzad, 2023). Such a mass-scale data breach significantly damaged consumer trust in digital payment systems across the country.

As FinTech experienced rapid technological growth, maintaining consumer trust became a critical issue for FinTech firms. According to official statistics from the State Bank of Pakistan, the volume & value of e-banking transactions in the country between 2012 and 2022 rose by 273% and 88,135% (13.6 billion in 2012 and 12 trillion in 2022), respectively. Similarly, the number of e-banking users witnessed an upward trend from 24 million to 42 million. As the number of users of e-banking increased, the complaints of financial fraud also increased. The Fraud Investigating Authority (FIA) reported that out of all the complaints received, 40% of them were related to financial fraud (Abbasi S. , 2023). The number of fraud complaints for the year 2021 was 467, which increased to 3,626 in 2023 (Banking Mohtasib Pakistan, 2023).

Global Trust Barriers in FinTech

The lack of trust in FinTech is not limited to developing markets like Pakistan; it extends to developed economies as well. Adoption rates in some technologically advanced countries, such as Germany, are also low. Jurjens (2018) discussed how data security concerns have become a critical barrier to trust in FinTech among users in Germany. Around 82% of the users expressed unwillingness to share their information, which shows the severity of this barrier. That’s why understanding the barriers to trust recovery among consumers of FinTech is of critical importance in every market.

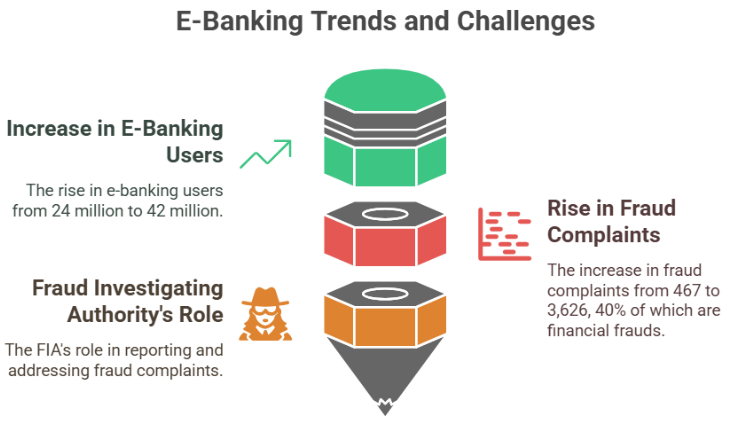

E-Banking Trends and Challenges
Increase in E-Banking Users
The rise in e-banking users from 24 million to 42 million.
Rise in Fraud Complaints
The increase in fraud complaints from 467 to 3,626, 40% of which are financial frauds.
Fraud Investigating Authority's Role
The FIA's role in reporting and addressing fraud complaints.

Figure. 3. E-Banking Trends and Challenges (Prepared by Author)

Cybersecurity challenges

A relatively younger FinTech market of Pakistan has been facing constant cyber attacks, data theft incidents, among other cybercrimes. These challenges make the Pakistani market a good case to study because as the number of FinTech users increased, the cases of data theft and fraud also witnessed a sharp increase. This suggests that there is a probable correlation between the volume of digital payments and the probability of data breaches (Ballaji, 2024).

Researchers and academics have been researching FinTech data breaches globally. When a malicious actor, or a hacker, gains unlawful or unauthorised access to the private and sensitive information or data of consumers for financial gain, it can be called data theft. It damages FinTech platforms on many fronts, such as the FinTech products suffer service degradation, or disruptions that can cause consumers financial loss. Such incidents also cause reputational damage to the firms. Because of that, FinTech consumers lose their trust in the integrity of the product (FinTech Magazine Article, 2025). These events push back consumers to use FinTech products to meet their financial needs (Swammy, 2019).

According to the Data Breach Investigations Report, around 68% of the data breaches involved social engineering attacks. Among all the data breaches that were reported, 62% of them were financially motivated, using ransomware or extortion (Verizon Business, 2024).

A usual technique of digital fraud is online banking fraud, where funds are being moved from the consumer's account without their knowledge and consent (Leukfeldt, 2020). In social engineering attack techniques, the attackers don’t take advantage of the technical weakness of the system but rely on the emotional manipulation of consumers. According to Ahmad (2021) social engineering attacks comprise phishing, vishing, malware, and identity theft. Given the nature of sophistication, financial recovery and trust restoration become a serious challenge for FinTech companies since it involves emotional dimensions such as feelings of shame. In order to address these technical and emotional challenges, robust security frameworks should be implemented.

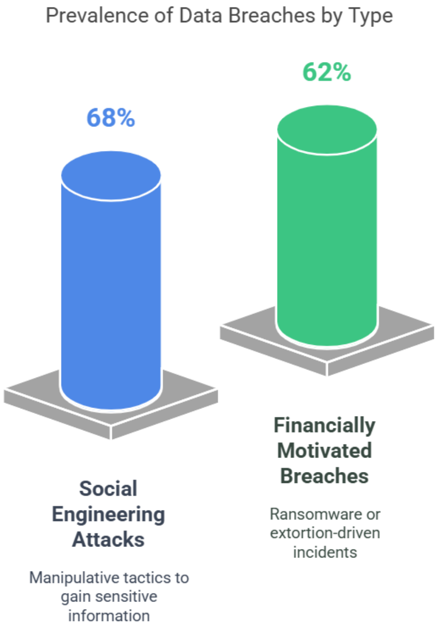


Figure. 4. Prevalence of Data Breaches by Type (Prepared by Author)

Phishing Fraudsters often trick FinTech consumers into revealing their sensitive information by sending malicious links via email. This technique is referred to as Phishing. The apparent link is disguised as an advertisement or seemingly from the bank itself, but they redirect the users and steal their banking information, which is then used to carry out financial transactions.

These attacks are carried out to steal personally identifiable information (PII) or login credentials. Such information can then be used to get access to online accounts, credit card data, etc. They can compromise entire networks until a ransom amount is paid (Cisco, 2025).

With the use of AI, it is now much easier for attackers to use PII and carry out a highly personalized phishing campaign, which is called spear phishing. Since these attacks are personalized to the target consumer, they can look very realistic to them, and they can fall victim to the spear phishing campaign (Cisco, 2025).

Vishing involves fraudsters impersonating a representative of a legitimate organization, such as a law enforcement officer or bank staff, etc. They trick the consumers into revealing their financial information and then use it to move funds from one account to another. For example, consumers in Pakistan received phone calls and messages from attackers impersonating bank officers asking for personal information like ATM PIN codes and one-time passcodes. That information was then used to steal money from consumers' bank accounts (Pakistan Telecommunication Authority, 2021).

Malware Attacks are carried out to steal sensitive financial information from the consumer's mobile device or computers in stealth mode. The attackers use viruses and spyware for such purposes (Dawn, 2023). Consumers are deceived into installing malware, which then gathers all the information and sends it back to the fraudsters to be used for their financial gain.

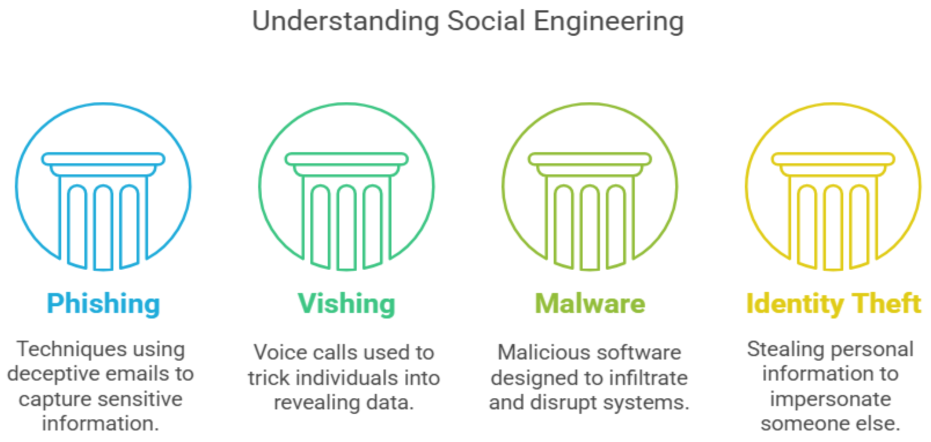

Understanding Social Engineering
Phishing
Techniques using deceptive emails to capture sensitive information.
Vishing
Voice calls used to trick individuals into revealing data.
Malware
Malicious software designed to infiltrate and disrupt systems.
Identity Theft
Stealing personal information to impersonate someone else.

Figure. 5. Understanding Social Engineering (Prepared by Author)

Identity theft is stealing a consumer's identity by fraudsters, which is then used to open new bank accounts, credit cards, and other credit lines (Dawn, 2023). In many cases, stolen identities are used to open new bank accounts, apply for credit cards, or secure loans under the victim's name. Beyond establishing new financial accounts, identity thieves may also gain access to existing accounts, lock victims out by changing credentials, and initiate unauthorized transactions. These funds are often quickly transferred across multiple accounts to obscure their traceability. The consequences for victims can be severe, ranging from immediate financial loss to long-term credit damage, legal complications, and emotional distress. In the context of FinTech platforms, which rely heavily on digital onboarding and automated identity verification, the risk of identity theft is particularly acute due to the volume of sensitive data processed and stored online.

SIM swapping is duplicating a consumer's SIM and using it to steal information. The Pakistan Telecommunication Authority issued a threat alert in 2022 stating that the number of cases of SIM swapping has been on the rise (Pakistan Telecommunication Authority, 2022). In SIM swapping, the attackers contact the service provider of the user, impersonating them and transferring the phone number to another SIM card. That SIM card is then used to access email accounts and digital banking accounts. Even though it was not a direct attack on the financial institution, the weak verification procedures of telecom companies were exploited for this identity theft scheme. As a result, consumers suffered financial and non-financial losses.

A data breach is when a consumer's personal information, such as financial records or other sensitive data, is accessed by attackers. it is known as a data breach (R. Sabillon, 2016). Such activity is performed mostly to sell the data on the Dark Web or to any potential buyer. This data is then used to carry out personalized attacks on consumers. FIA reported that in 2018 alone, hackers illegally obtained data from around 20,000 ATM cards and then sold them over the Dark Web in (Shahzad, 2023). Further in the thesis, real-world examples are provided to illustrate data breaches in the Pakistani FinTech market.

Incidents review on data breach:

A FinTech consumer in Pakistan experienced data theft when a digital loan application demanded his national identity card and facial recognition data. The victim received a call from a different loan application, which stated that the individual had defaulted on a loan through the use of his private credentials. The incident demonstrates a major violation of data integrity because private information entered into one system was exploited by another system. The two loan applications proved to be scams after further investigation. The case demonstrates the increasing dangers of unmonitored digital lending platforms and the necessity for enhanced data protection protocols in Pakistan's FinTech sector (Dawn, 2022).

Incident Review on Data Breaches in Financial Institutions in Pakistan:

A major Pakistani news outlet published an investigative report that showed how consumer data was being widely sold throughout the banking industry of the country. The study showed that personal data was being openly traded on social media platforms while bank staff members actively participated in the transactions. A major data breach revealed a 400 million PKR scam, which led authorities to arrest a bank employee. Bank customers received phone calls from the official UAN number, which suggested that the callers accessed customer databases internally. The bank failed to take any public legal action against the breach despite its extensive nature, which raised substantial questions about institutional transparency and accountability. The incidents have damaged consumer trust while showing that financial institutions in Pakistan lack adequate data governance systems (Abbasi S. , 2022).

A vishing scam targeted various family members who lived in Pakistan. The victims received calls from phone numbers that matched official contact numbers of local banks and digital platforms. The attackers pretended to be customer service representatives while obtaining family relationships, together with ATM card details and identification numbers from victims (Arshad, 2023). Some victims received false information about winning a lottery or a reward, which led them to reveal their digital wallet access credentials. Social engineering attacks in Pakistan have become highly sophisticated because attackers easily take advantage of public trust in institutional communication channels.

In 2018, Bank Islami stated that a "digital copy of a consumer's credit card information was leaked to hackers", which led them to trigger international payments from Brazil and the US amounting to Rs2.6 million. However, international payment partners claimed the amount of the transaction was $6 million. The bank was forced to disconnect its international payments immediately to avoid further damage and claimed to refund Rs2.6 million to their respective customers (Bhatti, 2018). Pakistan's biggest bank, Habib Bank Limited (HBL), also suffered a similar attack. This massive data leak across the banking sector took a toll on customer trust.

In the year 2020, an online investment company named "PSlash" scammed more than 100,000 consumers in Pakistan for nearly $19 million. The company promised a return of 13% but then suddenly disappeared. Newspapers reported that suspicious reports about the company were submitted to the authorities, but they failed to act in time, resulting in massive financial loss (Yousafzai, 2020). Such incidents damage not only the trust of victims but also that of potential consumers.

A case was reported where a fraudulent company started mimicking a genuine company from Bahrain (Tahir, 2023). This company lured people into investing with them for a small amount. However, once the consumers started getting some returns before they were able to book their profits, the website suddenly became inaccessible, leaving consumers shattered. This company was using all the top-tier security measures, which gave a feeling of security to the consumers and added credibility to the platform. It was nothing more than a scam to lure them into the trap. Once consumers are cheated in this way, their level of trust in enhanced security measures might never be fully redeveloped. The previously stated two cases are examples of attacks that require more expertise on behalf of the fraudsters and damage the institutional and regulatory trust of the consumers. Consumers believe that the competent authorities failed to protect them.

Government Actions on Data Breach Incidents: The President of Pakistan in 2022 ordered two private banks to pay four victims of digital financial fraud a total of four million Pakistani rupees (Banking Mohtasib Pakistan, 2023). The cases included different types of unauthorized access and negligent banking practices. A victim received a phone call from a number that was similar to the official bank helpline number and used to trick them into revealing their sensitive information. Two other cases involved large unauthorized withdrawals that were made directly from the victims' accounts without their knowledge. The investigations showed that the breaches happened because the banks had insufficient security systems and weak internal controls. The activation of electronic fund transfer (EFT) facilities without account holders' consent allowed fraudsters to access and move funds without supervision. These incidents demonstrate critical failures in digital banking security and demonstrate the need for regulatory enforcement and consumer protection mechanisms in Pakistan's financial sector.

The rising number of frauds, scams, and data breaches in Pakistan is alarming for FinTech companies. For a market where digital literacy rates are already low, establishing trust is a challenge. Following a data breach, it becomes even more difficult to regain the consumer's trust. Understanding the barriers to trust restoration and their solutions is an important pillar for growing the FinTech industry in Pakistan.

2. Theoretical Solution for Trust Recovery in FinTech

This chapter covers solutions for trust recovery post-data breach among consumers of FinTech. This section will utilise already established research in the field of trust and devise a framework that can explain how FinTech firms can recover consumer trust post-data breach. It will also draft a clear understanding of FinTech, its components, stakeholders, benefits, and consumer trust in digital platforms. The study will examine elements such as transparency, effective communication, and institutional credibility in the context of trust recovery.

2.1. Theoretical Analysis on Concepts of Trust in FinTech

The concept of trust has been defined in various ways by different scholars. Chervany (2001) defines trust as a very complex concept, while Lewis (1985) uses Luhmann's theory to define trust as decreasing social interaction uncertainty and complexity. The definition of trust from Mayer et al. (1995) explains it as the readiness of one party to expose itself to another party's actions. According to Chakraborty (2022) trust emerges as a positive outlook consumers have toward their service providers. Xiongfei Cao (2018) shows that trust drives user retention by passing through satisfaction.

In FinTech, consumers are required to trust virtual products, which makes it a crucial factor for FinTech firms, especially post-data breach. The main idea is that consumers have to trust their FinTech service providers with their private and sensitive information. In case of a data breach, consumers' trust is broken and requires the FinTech firms' special attention.

The research by Singh, Sahni, & Kovid (2021) explains that affective trust is driven by common values and user satisfaction, but cognitive trust requires a rational assessment of FinTech products' reliability and security measures. The study found ease of use and perceived usefulness as key factors influencing affective trust.

Punyatoya (2019) investigated trust by studying cognitive and affective trust among online consumers in India. The research found that website quality, security measures, and privacy policies are the main factors that influence cognitive trust. However, the emotional engagement of consumers impacts their affective trust. The study highlights the importance of post-breach effective communication and an easy-to-use product interface as leading trust recovery factors. Conversely, if consumers perceive a product to be unreliable, it leads to a negative emotional connection, which then impacts user engagement.

Punyatoya emphasises that past experiences of consumers, along with their perceived reputation of the company, affect both affective and cognitive trust. The author suggests that restoring the institutional reputation follow a data breach can greatly impact the trust recovery process. Further, the study points out that cognitive trust is the foundation for affective trust. Both of these trusts then translate into customer satisfaction, which can make consumers continue to use the product. However, the research was conducted in specific cultural settings, therefore, it lacks universal application.

Zhenning Wang (2019) investigated consumer trust in YuEbao through the examination of herding behavior and subjective norms as a Chinese FinTech platform. When consumers base their decisions on following others during uncertain times, it's called herding. Subjective norms can be explained as the social pressure to conform to societal expectations. Both of these behaviors can be called affective trust, but both of them serve different psychological functions. The phenomenon of following others isn't trust, but it provides structural assurances. These structural assurances represent cognitive trust because they involve rational decision-making by consumers. The social reinforcement of subjective norms directly affects trust recovery.

Ahmed Shuhaiber (2023) found that consumers with better digital literacy tend to use the services responsibly. Conversely, consumers with lower levels of digital literacy tend to receive incorrect information regarding FinTech products, leading them to develop incorrect beliefs about the product. This behavior then harms social trust in FinTech products and services. Arli (2020) belives that trust is the most crucial factor in cryptocurrency adoption and valuation.

Dimensions of Trust

Lewis (1985) discusses different dimensions of trust in his research, and it is of special importance in understanding trust. Lewis defines trust as the rational decision to accept that the probability of a negative outcome is present, but it will not occur. He proposes that rational behaviour alone doesn't translate into trust. Which means that to understand trust recovery post-data breach, we will require a much deeper investigation dimension. Lewis (1985) suggests three different dimensions of trust: cognitive, affective, and behavioural trust. We will analyse into each dimension to see how they interact and contribute to the process of trust recovery in the context of FinTech post-data breach.

Cognitive Trust arises from the rational evaluation of the consumer. According to Lewis (1985) a cognitive process of classifying institutions into which are trustworthy, untrustworthy, and unknown is known as cognitive trust. The research argues that cognitive trust requires some level of familiarity in advance. For example, a consumer affected by a data breach now has a level of familiarity with the actual causes. From this point on, if the consumer is well-informed, they can predict the future with full certainty, eliminating the need to trust. Conversely, an uninformed consumer would withhold trust. There is another possibility: if the consumer is faced with an unknown circumstance and still chooses to use the platform, it will be a gamble. Therefore, we can say that no amount of information alone can establish cognitive trust; it can only be established once the consumer no longer requires the evidence or rational reasons to develop trust.

Affective Trust is defined as the emotional bond between the two parties, much like friendship (Lewis, 1985). Similar to friendship, a breach of trust can cause emotional outrage among consumers. The breach of trust can negatively impact all parties involved. In our context, a breach of trust post-data breach would negatively impact consumers, including consumers suffering from emotional trauma.

Lewis (1985) also proposes the behavioral dimension of trust as well along with affective and cognitive trust. The author says that trust means the expectation of ethical action. FinTech consumers from the behavioral trust dimension expect FinTech platforms to do the right thing if a data breach occurs. Consumers expect the platform they remain vigilant and take necessary actions to protect their private and sensitive information to avoid any financial loss.

Trust Erosion in Fintech

Post-data breach, consumers' trust reduces and over time may completely erode in FinTech systems. Data breach, identity theft, unauthorized user access, unauthorized transactions, etc all lead to trust erosion among consumers. Lewis (1985) believes that trust requires a person to be vulnerable and therefore extends beyond the rational calculation. However, when such vulnerability is exploited by attackers and hackers, it immediately damages trust. The trust further deteriorates when FinTech firms fail to provide efficient disclosure of the data breaches, ineffective customer service further makes it worse. Our research will focus on these factors that can help us understand how consumers lose their trust post-data breach and what is required to restore it. When trust starts to erode, it can lead to major consumer actions such as discontinuation of usage and reverting to cash culture.

Trust Recovery in FinTech:

Trust recovery is a process that can make consumers start trusting the FinTech application again after their trust has been breached. Dietz (2009) believes that trust recovery is possible if FinTech firms use effective communication techniques, acknowledge their failure, and then implement corrective actions to ensure it doesn't repeat. These corrective actions can be security improvements, but the FinTech firms need to communicate them to the consumers as well. One of the most important aspects of trust recovery is having an active communication channel with consumers. The concept of trust recovery is based on responsive customer service, transparency, and regulatory compliance. Trust recovery requires consumers to feel assured by the firm that their data and money are secure. Our study will focus on trust recovery because it decides if the consumer is willing to resume using the FinTech product.

The next section of this study will discuss concepts of trust recovery in FinTech post-data breach. It will include definitions of trust and its dimensions from different perspectives. For example, Lewis (1985) and Mayer (1995) explains trust as the willingness of an individual to be vulnerable. In FinTech, consumers are dependent on the digital service provider and share their sensitive information with them. This is a symbol of consumers making themselves vulnerable to the FinTech service provider. There are three different types of trust:

1. Institutional trust
2. Relational trust
3. Technology-based trust

The analysis shows cases of how trust is negatively impacted by security breaches and institutional negligence. Conversely, effective communication, transparency, and visible security updates can lead to trust recovery.

2.2. Theoretical Analysis of the Concept of FinTech

Definition of FinTech

FinTech is the technology application that is employed to deliver financial services to consumers (Baber, 2020). These are the new financial intermediaries that are leveraging innovative technology-enabled solutions to support emerging business models, processes, and product & service improvements (Bryan Zheng Zhang, 2021). The US Financial Stability Board (FSB) concurs in defining FinTech as technologically enabled innovation in financial services that can facilitate the emergence of new business models, applications, and products (Financial Stability Board). However, this definition further extends its impact by stating that such applications have a material effect on the financial markets and the provision of financial services.

For our research, we will prefer FSB’s definition of trust because it highlights both the innovative aspect of FinTech and also the impact it has on the financial services. Since we will study factors that can positively or negatively impact trust recovery in FinTech, we would also require the impact it can have on the operational side of FinTech firms.

FinTech as Financial Innovation

FinTech is the compatibility between technology and financial services. This amalgamation is giving rise to numerous innovative solutions that are constantly transfiguring the financial service industry. These innovations have compelled companies to undergo structural changes to better adapt to market trends. As previously discussed, FinTech is disrupting the existing norms of conventional banking and financial services. These innovative solutions demonstrate success because they can provide personalized services to customers that best suit their financial requirements.

Mark A Chen (2019) studied the Internet of Things (IoT), robot advising, and blockchain as among the most popular technological aspects of FinTech in the financial sector. His study also showed that most of the innovation in FinTech has been fueled by publicly traded companies.

Mobile wallets (m-wallets) exemplify FinTech innovation, serving the same core function as a physical wallet. They provide more security and flexibility because they allow customers to carry money without the risk of it being stolen or lost. That is a combination of technology and financial need. These mobile wallets are gaining prominence in countries such as China, where the comprehensive platform WeChat can fulfill most of the financial requirements (Rahman, 2024). It is widely accepted and trusted by consumers because of its convenience and security. It offers various modes of payment to customers. Comparable platforms, including Google Pay and Apple Pay, are more popular among American users, Easypaisa and JazzCash are famous among Pakistani users, MTN and Orange Money are famous among African customers, and Revolut and Paysera, among others, are commonly used in Lithuania. Rahman (2024) notes that such mobile wallets are becoming increasingly popular in developing economies. However, the factors affecting consumer adoption intentions toward these FinTech services after a data breach or a digital scam have not been studied.

Kumar (2023) conducted a literature review and studied the impact of blockchain technology on small and medium enterprises. He researched the issues that SMEs face in raising debt capital, and with the emergence of FinTech, they have access to finances, which is essential for any business.

Opportunities for end users

As reported by Remitly, Africa has the world's largest mobile money market. One reason is the limited access to basic banking and financial needs due to a dilapidated financial infrastructure. Consequently, FinTechs are enhancing financial inclusion by offering services to those who have no access to conventional banking services (Remitly, 2023). Rahman (2024) also argues along the same lines, discussing how such FinTech services have provided customers with seamless transactions in a cost-effective and timely manner. Kumar (2023) posits that FinTech can improve financial inclusion because of the unique properties of blockchain technology. His study focused on investigating whether blockchain technology has the potential to revolutionize small and medium enterprises by giving them access to credit. He substantiated this claim by analysing different aspects of blockchain, such as transparent record-keeping and minimal risk of fraud in smart contracts.

Opportunities for businesses

FinTechs are now catalyzing economic growth in many countries. Boehm (2022) found that digital trust leaders are 1.6 times more likely to generate 10% higher earnings as compared to others. To achieve this economic growth, financial institutions and FinTech have formed strategic partnerships. Ruhland (2023) studied how such partnerships achieve success. Ruhland states that the main purpose of FinTech services is to provide faster, cheaper, and easy-to-use channels. Market competition compels providers to enhance customer satisfaction and focus on customer value creation. McKinsey and Company reports also show that most banks prefer using AI because it enables them to reduce costs, boost revenues, and provide superior customer service around the clock (McKinsey & Company, 2022). This enables them to expand their business by providing more products and improving customer retention rates by encouraging existing customers to continue to use the platform or service. Rahman (2024) states that FinTech has allowed businesses to reach the market segments that were previously untapped by the conventional financial industry. Kumar (2023) describes how blockchain could help bring down the transaction cost and time to process the transaction. The enhanced security consequently strengthens the trust of customers, thereby benefiting businesses. The author supports his study with an example of El Salvador, which has planned to grant crypto loans of $10 million to SMEs. This funding could prove to be a critical support for some SMEs since raising debt capital for them is often very costly, inefficient, and time-consuming.

Hentzen (2022) conducted a literature review on the use of AI in the financial industry. His research found that financial institutions are using Robo-advisors for digital advisory services. He identified research on how such robo-advisors would help address the issue of behavioral biases. He identified that one subject of research is the use of AI for credit scoring and risk assessment, especially in combating money laundering.

Drivers of FinTech innovation

The primary users of FinTech services are Millennials, whose preferences have shifted with time. Cost-effective and speedy transactions are the new focus of this generation, and they have moved on from the traditional payment methods that require days to process one payment. Pakistan has a large population working as freelance with international clients, these people require efficient digital payment solutions that can fulfil all of their requirements. Their consumer preference has not changed on its own; the ever-evolving technological landscape, advances in AI, the availability of metadata, mobile technology, and massive computing power have also impacted them and the financial industry. For example, in Pakistan, new entrants such as JazzCash achieved faster market penetration than traditional banks. Consequently, these new entrants leveraged the market where traditional financial institutions scaled back due to high capital requirements or fear of bad debts (Financial Stability Board, 2017).

After the financial meltdown of 2008, under Basel 3, capital requirements for the banks were increased for better risk control. As a result of these requirements, the finances available for SMEs and individual consumers are significantly hampered (Douglas Arner, 2015). To mitigate unemployment in the US, the Jump Start Our Business Startups (JOBS) Act was enacted in 2012, bolstering FinTech startups.

As per FSB, the drivers of FinTech innovation can be divided into demand side and supply side drivers. Figure. 6. below aligns perfectly with our earlier discussions on the shifting consumer demand preferences. As a balancing effect, on the supply side, rapid advances have been made in the technological ground and the impact of changing financial regulations.

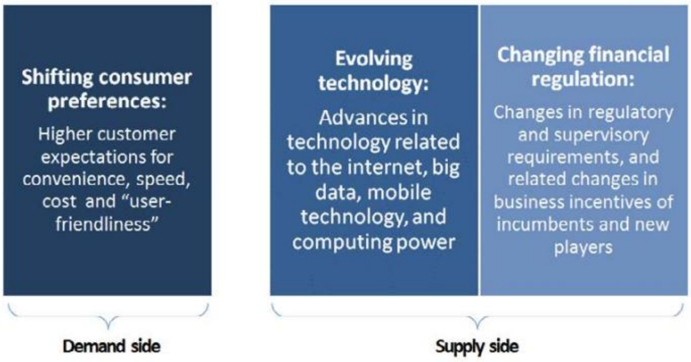

Shifting consumer preferences:
Higher customer expectations for convenience, speed, cost and "user-friendliness"
Evolving technology:
Advances in technology related to the internet, big data, mobile technology, and computing power
Changing financial regulation:
Changes in regulatory and supervisory requirements, and related changes in business incentives of incumbents and new players
Demand side
Supply side

Figure. 6. Drivers of FinTech Innovation (Financial Stability Board, 2017)

FinTech Typology

Douglas Arner (2015) in their research paper, classify the typology of FinTech by conducting an evolutionary analysis. Douglas categorizes FinTech into five components.

1. Finances and investments
2. Operations and risk management
3. Payments and infrastructure
4. Data security and monetization
5. Customer interface

The scope of FinTech expands opportunities for finance and investments as compared to the traditional methods. For example, crowdfunding, robo-advisors, venture capital, P2P lending, private equity, coin offerings, etc. Robo-advisors are platforms that provide financial and investment advice to consumers, helping them manage their finances.

FinTechs can help improve the risk management and operational aspects of financial institutions. For example, blockchain is an excellent means of processing transactions with complete transparency. Similarly, various AI tools can be used to detect fraud and strengthen anti-money laundering checks and balances. A FinTech from Pakistan, PostEx, is one example; they provide services to e-commerce.

The most basic and popular form of FinTech is the payment processing applications that improve financial infrastructure and promote financial independence. For example, Jazz Cash, Raast, NayaPay, and Easy Paisa mobile applications are becoming increasingly popular in Pakistan for payment transfers. Recently, Google Wallet facilities were also introduced, which will strengthen the overall FinTech market.

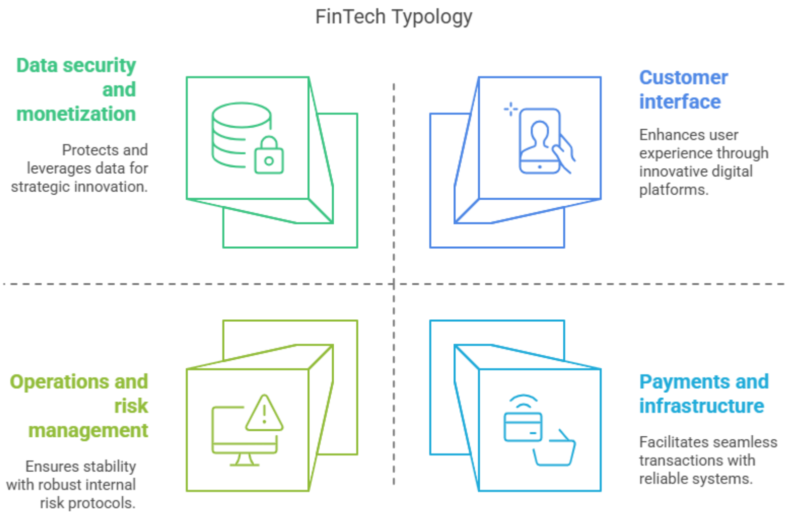

FinTech Typology
Data security and monetization
Protects and leverages data for strategic innovation.
Customer interface
Enhances user experience through innovative digital platforms.
Operations and risk management
Ensures stability with robust internal risk protocols.
Payments and infrastructure
Facilitates seamless transactions with reliable systems.

Figure. 7. FinTech Typology (Prepared by Author)

Data security focuses on technologies that protect information for different digital channels. Such as encrypting technologies or other cybersecurity measures. This category also includes tools for processes such as big data analytics. The State Bank of Pakistan introduced the RAAST payment system for real-time secure payments.

The customer interface focuses on systems to interact with users and improve their experiences with the company. The importance of user experience is increasingly prioritized and many Pakistani FinTechs, NayaPay for example, have implemented chatbots to improve user interactions.

FinTech Ecosystem and Its Key Stakeholders

FinTech applications include banking, insurance, and stock trading companies. This enables electronic access to these businesses to carry out their financial responsibilities efficiently and safely (Shin, 2018). It ensures cost-effective means of transit funds while maintaining full transparency and efficiency. Setiawan (2024) calls FinTech the best non-financial invention of the modern age. The eco-system of FinTech comprises:

1. FinTech startups
2. Technology developers
3. Governments
4. Customers
5. Traditional financial institutions

Startups are at the very core of the FinTech ecosystem, driving innovation. These startups are unbundling financial services that have disrupted the traditional banking system. It is because of this ability that FinTech has shown tremendous growth over the years. These startups give a variety of options to consumers to choose from. FinTech startups are attracting a lot of venture capitalists and private equity for fresh investments.

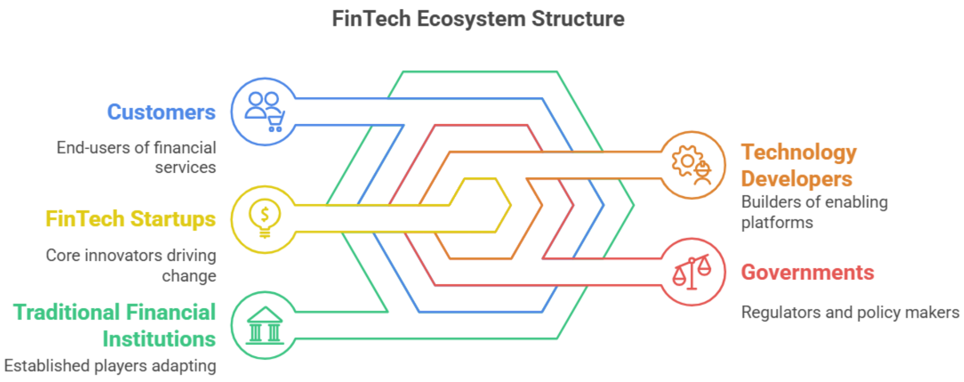

FinTech Ecosystem Structure
Customers
End-users of financial services
FinTech Startups
Core innovators driving change
Traditional Financial Institutions
Established players adapting
Technology Developers
Builders of enabling platforms
Governments
Regulators and policy makers

Figure. 8. FinTech Ecosystem (Prepared by Author)

Technology developers are those who provide digital platforms for mobile banking, social media, data analytics, etc. Their main responsibility is to create a favorable environment for startups. A good example of technology developers is Amazon Web Services (AWS), Google Cloud, Blockchain, etc.

Governments include regulatory bodies that play a crucial role in shaping the FinTech ecosystem. They provide a favorable regulatory environment for FinTechs to thrive. It also involved the policymakers, who designed suitable policies for FinTechs to flourish with the help of financial service licenses, relaxation of capital, etc (Shin, 2018). In Pakistan, the State Bank of Pakistan has been a very instrumental part of this ecosystem by issuing licenses to creditable FinTech institutes.

Traditional financial institutions are banks that have been in the financial sector long time before FinTech. However, they understand the changing landscape and have been a major source of the FinTech ecosystem. They have a competitive advantage in economies of scale, experience, and resources as compared to FinTechs.

Individual customers are the major source of revenue for these FinTechs. Even though corporate customers can be a good source of revenue, small and medium-sized companies and individuals are the major revenue streams (Shin, 2018). As we discussed earlier, after the financial crisis, the availability of capital for SMEs and individuals dried up; therefore, they were the first ones to opt for these FinTechs. While corporate consumers look for fast and efficient processes, individuals are more skewed towards cost-effectiveness.

FinTechs in Pakistan

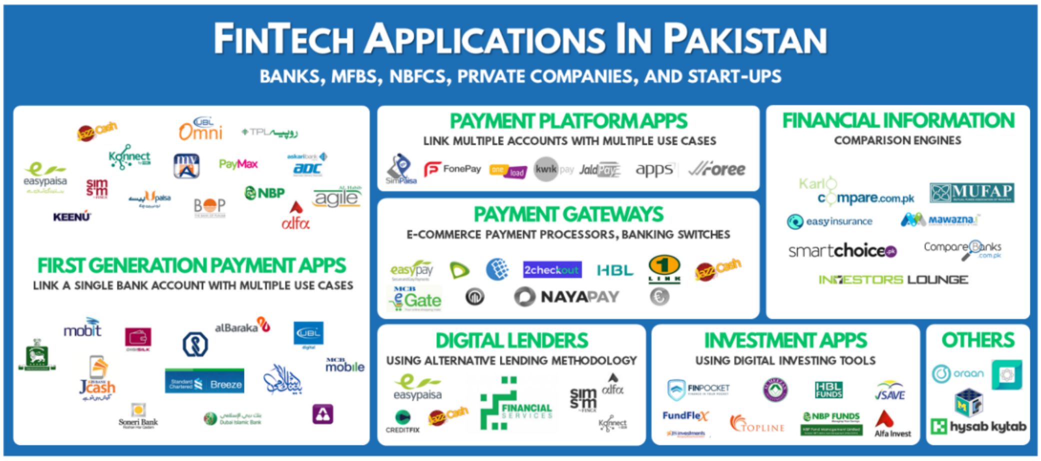
The reason for choosing Pakistan for this empirical analysis was its rapidly growing FinTech market, despite having a weak regulatory setup, and rising cybercrimes. These incidents need to be understood from the perspective of trust breach because consumers will revert to using traditional means of payment. This can impact FinTech adoption and usage trends in the country. The study will focus on the responses given by consumers of FinTech who have suffered a data breach. But before that, it is important to analyse the overview of Pakistan's FinTech environment.

Even though Pakistan doesn't have access to world-renowned FinTech products such as PayPal, the overall market is still evolving rapidly and maturing along with the local brands. The market potential can be measured from the fact that around 85% of the population is still financially excluded in the world's 6th most populated country (Ahmad Fraz, 2021). Nevertheless, other applications are expanding swiftly to fill this void. Most of these FinTech applications operate primarily in major cities like Karachi, Lahore, & Islamabad.

Major FinTech business models that can be observed in Pakistan are as follows:

1. Insurance
2. Crowdfunding
3. Payment
4. Lending
5. Wealth management & capital markets

Table 1 below has the list of FinTech applications with their categories. The data is sourced from their official websites (JazzCash, n.d.) (Finja, 2023) (Creditbook, n.d.) (Payoneer, n.d.) (Aysonline, n.d.).


FINTECH APPLICATIONS IN PAKISTAN
BANKS, MFBS, NBFCS, PRIVATE COMPANIES, AND START-UPS
PAYMENT PLATFORM APPS
LINK MULTIPLE ACCOUNTS WITH MULTIPLE USE CASES
FINANCIAL INFORMATION
COMPARISON ENGINES
PAYMENT GATEWAYS
E-COMMERCE PAYMENT PROCESSORS, BANKING SWITCHES
FIRST GENERATION PAYMENT APPS
LINK A SINGLE BANK ACCOUNT WITH MULTIPLE USE CASES
DIGITAL LENDERS
USING ALTERNATIVE LENDING METHODOLOGY
INVESTMENT APPS
USING DIGITAL INVESTING TOOLS
OTHERS

Source: https://www.tezfinancialservices.pk/tfs/FinTech.php

Figure. 9. FinTech Applications in Pakistan (tezfinancial services website)

Figure 9 and Table 1 both show FinTech applications that are operating in Pakistan by their category. These FinTechs are categorized by mobile wallets, banking and lending, cross-border payments, and buy now, pay later. Among these applications, JazzCash, EasyPaisa, SadaPay, and NayaPay are the most prominent mobile wallet applications. Among them, JazzCash has the highest number of registered users. EasyPaisa has been credited with being Pakistan's first-ever mobile money service application. All of these products provide consumers with P2P transfers, utility bill payments, insurance services, and investments. These products are vital for the rising freelancer community of the country.

The Pakistani government has been at the forefront of this growth. The government operates Raast, which handles more than 10 million monthly transactions, proving its usefulness and credibility. It is also a good example of rapidly improving digital infrastructure across the country. Other products, such as Finja and CreditBook, are improving financial inclusion by serving small businesses, especially small merchants. Payoneer and PayPro have emerged as reliable platforms for cross-border payment products, facilitating freelancers. QisstPay has been operating under the category of buy now, pay later, which provides interest-free installment plans for e-commerce through its support of more than 500 retail partners.

Table 1. FinTechs in Pakistan

Category	Product	Key Features	Key Facts
Mobile Wallets	Jazz Cash	P2P transfers, utility bill payments, mobile top-ups, merchant payments, etc.	An estimated 45 million customer base, one of the largest in the country.
	EasyPaisa	Digital payments, remittances, insurance, microloans, etc.	First mobile money service in Pakistan. One of the most popular.
	SadaPay	Digital banking facilities like P2P transfers.	Relatively new in the market and focused on freelancers.
	NayaPay	Digital wallet focusing on freelancers, foreign currency accounts available, etc.	First FinTech to have received the State Bank of Pakistan's Electronic Money Institution license.
Banking/Lending	Raast	Raast is an instant payment system by the State Bank of Pakistan.	Processes some 10 million transactions per month.
	Finja	SME lending, digital wallets, and payment solutions.	Facilitated Rs.11 billion financing to SME's
	CreditBook	Digital Ledger application for small merchants.	Has reached over 1 million micro-small-medium enterprises (MSMEs).
Cross-Border Payments	Payoneer	Global payments solution focusing on freelancers	Has 25+ global offices and is listed on Nasdaq as PAYO.
	PayPro	Global payment solution backed by one of the biggest banking operations in Pakistan, Habib Bank Limited.	-
BNPL (Buy Now, Pay Later)	QisstPay	Interest-free installment plans for e-commerce.	Serves over 500 retailers across Pakistan.

2.3. Consumer Trust in Digital Platforms:

Trust is a very crucial factor for a FinTech platform because, unlike a brick-and-mortar conventional financial institution, there is no physical interaction between the service provider and the consumers. A higher level of trust is required, given the virtual nature of the relationship (Egi Arvian Firmansyah, 2023). A study by Singh, Sahni, & Kovid (2021) also confirms this idea that digital platforms demands a higher level of trust among the consumers because of its virtual nature and this is why trust in FinTech is of utmost importance.

Trust has been regarded as the essential element in crypto adoption (Khan S. &., 2022). Punyatoya (2019) takes this idea a step further by stating that the perceived quality of the platform impacts consumers' behaviour. This consumer behaviour can translate into emotional engagement, which can strengthen both affective and cognitive trust among consumers. Given this paramount importance, FinTech platforms must maintain high standards of security and privacy (Shin, 2018).

A study was conducted by Lian, reviewing research carried out between 2003 and 2021 on mobile payments and banking. Lian (2021) identified four facets of trust.

1. Trust in service providers (i.e., Banks or FinTech companies)
2. Trust in mobile device providers (i.e., Samsung, Nokia, etc.)
3. Trust in mobile network service providers (i.e., telecommunication carriers)
4. Trust in merchants providing mobile payment services

Since trust has been the most important factor in FinTech, trust recovery is an even more sensitive matter, especially in times when attackers and hackers are using innovative techniques to steal data. Trust recovery is crucial if FinTech firms want to improve their reputational image (Yacoub, 2022).

Jurjens (2018) studied the importance of data security and privacy on FinTech adoption in Germany. The author raises serious concerns that only 10% of the respondents from his sample knew about FinTech, while less than 1% had utilized FinTech services. These statistics come from a country where 99% of participants had access to mobile phones. The study shows that around 82% of them don't feel confident enough to share their private information with FinTech firms. These results imply that German consumers have a trust deficit when it comes to using FinTech products, and there is a need to identify the barriers that are stopping them.

To empirically assess these factors, the author studied customer trust, data security, value-added, user design, and FinTech promotion. The research revealed that the biggest barrier stopping users from opting for FinTech is data security, followed by user interface design.

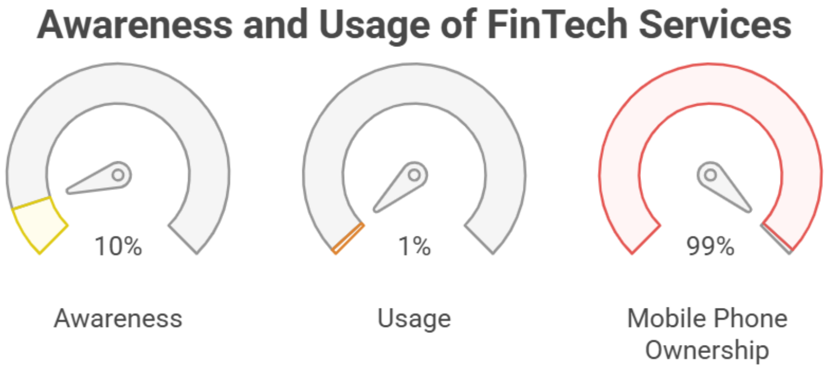


Figure. 10. Awareness & Usage of FinTech Services (Prepared by Author)

The study by Jurjens (2018) reveals consumers' concerns about the security of FinTech products given frequent cyberattacks. They also show concerns about how little has been done to control such incidents in the future. This indicates a lack of visible security updates, as discussed before in this research. Therefore, customers are interested in platforms that satisfy their financial requirements but also fulfill usability standards. From these results, we can say that data security has been of utmost importance, even more than the quality of the product. One can say that a high-quality FinTech application should provide state-of-the-art data protection; therefore, the distinction between the two seems inconsistent.

The study demonstrates that data security significantly improves consumer trust. However, to establish trust, such assurances of data security and privacy need to be effectively conveyed to consumers, as they will promote transparency.

In digital payments, the relationship between the user and the service provider is remote, therefore, it may generate a lot of uncertainties in the B2C (business-to-customer) and B2B (business-to-business) relationships (Chang, 2010). The absence of physical transactions requires a higher level of trust. Maintaining that trust over a long period becomes very precarious because if the consumer's trust in a particular service provider or the national digital payment ecosystem is weak, then even a small event or a single word of mouth can compromise the relationship. A lower level of consumer trust will lead to an even weaker perceived usefulness.

In developed countries, users are typically cognizant of the risks while using FinTech products; as discussed before, trust isn't taking the risk but knowing and accepting it. However, users are always concerned about their data and safety; therefore, when FinTech platforms invest in technology that can counter emerging risks, consumer trust improves automatically (Haritha, 2022). Given the challenges posed by cybersecurity threats, every nation is compelled to implement proactive measures to mitigate risk. Such proactive measures enhance consumer trust in digital payment products and services. It also assures them that national-level digital safeguards will protect them from any possible financial loss, further strengthening their trust in the overall digital infrastructure (Liu, 2019), (Pal, 2021), & (Patil, 2020). Studies show that the mitigation of perceived risk while engaging in one-line transactions by investing in preventive security measures improves consumer trust (Milian, 2019).

2.4. Psychological Drivers and Behavioral Responses to Trust Recovery

The following subchapter investigates psychological elements that affect consumer trust and behavior on FinTech platforms after a data breach occurs. The analysis uses behavioral theory constructs of attitude and subjective norms, and perceived behavioral control to explain consumer platform re-engagement following trust violations and their subsequent disengagement or provider switching. The theoretical framework of behavioral variables receives its conceptual basis from these constructs.

A. Psychological Drivers of Trust Recovery

Attitude

Consumer attitudes largely depend on the effective communication channels that the firm has opened after a data breach has taken place. This communication and transparency can turn consumer attitudes either negative or positive (Jurjens, 2018). Research shows that consumers evaluate the firm's responses by their perceived honesty, timeliness, and fairness. When a FinTech firm is transparent and forthcoming regarding the data breach, then consumers perceive that the firm is being honest and has informed on time. Conversely, if the firm attempts to hide a data breach, then consumers perceive that the firm is being dishonest and unfair. This can turn consumer attitudes negative, resulting in the discontinuation of the services as a result of damaged trust. Such an attitude will then slow down the trust recovery process as well.

Subjective Norms

In collectivist societies, subjective norms are very critical in shaping consumer trust because of the social pressures. In such societies, peer reviews have high weightage and can easily influence the consumer's decision to use a FinTech product or discontinue it. Public perception in Pakistan is also influenced by electronic and social media. Social media influencers have the power to single-handedly move the market. Conversely, a report by the World Bank Group indicates that regulatory authority penalties and new consumer protection policies create positive trust among consumers (World Bank Group, 2021).

Perceived Behavioral Control

Apart from their attitude and subjective norms, consumers also assess their ability to protect themselves from data breaches and digital fraud. For example, how sophisticated security measures are implemented and how easy it is for them to update the password would give consumers a sense of control over their data. It will also reassure the consumer whether the FinTech platform has adequate fraud prevention tools or not. Similarly, in an environment where the regulations are effective and consumers have trust in the state laws, they are more likely to trust FinTech products and continue to do so even after a security breach (World Bank Group, 2021).

B. Behavioral Responses Following a Data Breach

Post-data breach, consumers can respond through different behaviours, such as enhancing their security protections, switching to a competitor with better perceived security, negative word of mouth, etc (Brenner, 2020) (Siddhant Mishra, 2024) (Richins, 1983). These behaviours give us an insight into how consumers' shaken trust can translate into visible actions. The empirical section of this thesis will provide a deeper look into consumer reactions post-data breach.

2.5. Barriers to Trust Recovery in FinTech after a Data Breach:

Consumer trust is the most influential element of FinTech adoption; however, it can also quickly evaporate due to data security issues, user interface design, technical difficulties, and lack of awareness (Abidin, 2019). Stewart (2018) concluded that confidentiality, integrity, authentication, accountability, assurance, privacy, and authorization can influence consumer trust. Since FinTech has been the primary target for data breaches, consumers are very cautious about trusting and using online digital payment platforms.

Pakistan holds the sixth position for the largest population, but a big chunk of that economy is undocumented and cash-based. The country is facing challenges because of an underdeveloped regulatory structure. (Abbass, 2022) says that its economy also suffers from a shortage of capital. However, it is catching up with other countries. Firmansyah (2024) highlights Pakistan's third position in the list of countries that have more citations related to financial innovation, while Hayat (2021) points out that its growing technological landscape is plagued by digital illiteracy. Erum Irfan (2022) also studies how digital literacy rates in Pakistan are a major hindrance in the digital development of Pakistan. Nevertheless, there is a big technological gap between developed countries and Pakistan, which needs to be filled (Khaliq, 2024).

The FinTech landscape of Pakistan is filled with mobile wallets and payment platforms, such as Easypaisa, Nayapay, SadaPay, and JazzCash. According to official sources, around 40 different FinTech companies have been registered in Pakistan (State Bank of Pakistan, 2023) (State Bank of Pakistan, 2023) (Securities and Exchange Commission of Pakistan, 2023). Other sources quote more than 70 FinTech companies to be working in the country. These platforms have greatly revolutionized the financial services industry with their higher reach and lower transaction costs. However, there are significant barriers to trust recovery among consumers, especially after a data breach or a cybercrime incident.

Perceived risk:

Perceived risk refers to a consumer's concern regarding the risk associated with a FinTech platform or industry. We have discussed before that trust means accepting the risk associated with it. However, in the case of a data breach or cybercrime, this perceived risk would rise significantly, creating a ripple effect on consumer trust. Consumers show concerns regarding the enhanced risk associated with the higher frequency of usage of FinTech products and services (Utomo, 2021).

Ali (2021) advocates the role of perceived risks and benefits in FinTech adoption, stating how they impact consumer trust. His findings align with the cognitive dimension of trust because the assessment of these risks & benefits is a result of rational decision-making by the consumer.

Research carried out by PwC states that 87% of consumers were willing to opt for alternatives if they felt their data had not been managed and protected properly. If the company fails to inform them on time or chooses to delay the communication, consumers feel unsafe, and their perceived risk increases, which can damage the trust recovery process (Mamta Kumari, 2014). Hosam Elsaman (2024), shows that perceived risk hurts FinTech adoption, while perceived trust shows a strong positive impact. The study also describes trust propensity as individuals' ability to trust in technology and views it as a critical factor for FinTech adoption forecasting.

A study by Alalwan (2018) aligns with the idea that perceived risk negatively impacts consumer adoption of FinTech. Karjaluoto (2015) also concluded a similar result that perceived risk is a significant barrier to trust in FinTech since it impacts the reliability of the product or service. After falling victim to a data breach, a consumer might continue to fear another similar incident that causes them financial and non-financial loss.

Perceived security:

There has been research on the importance and impact of security on consumer beliefs (Pavlou, 2003). The research by Pavlou suggests that the associated risk with online transactions can only be mitigated by security. The study also proves security as an antecedent of ease of use. Strong security or enhanced security measures post-data breach can help restore trust among consumers.

Data protection concerns among consumers are one of the biggest barriers to trust recovery. In 2020, an estimated 37 billion records were stolen, which was a 141% increase from the previous year (TELUS Digital, 2021). Such concerns then damage the perceived security associated with the FinTech product and service. According to Forbes, 87% of business leaders believed that they are trusted by their consumers in the market, conversely, only 30% of the consumers gave their vote of confidence to the same companies (Segal, 2022). This means there is a big gap between what FinTech companies believe and reality. Such expectation gaps can cause trust recovery to be extremely slow.
Roh (2024) investigated the Chinese FinTech market and studied consumer trust among consumers using models such as the information system success model (ISSM) and the theory of reasoned action (TRA). His findings point out that perceived security and privacy are the two most significant factors that impact trust. In a post-data breach scenario, if perceived security and privacy improve, then consumers can start trusting the product and services again. ISSM, or the IS success model, was developed by DeLone (1992), and it focuses on providing a comprehensive approach to information system success by analyzing several aspects of success, such as system, & information quality. For example, Kim (2021) used the same framework and identified that customer loyalty can be achieved

through information and service quality since it improves consumers' sense of privacy, leading to satisfaction. It will be much easier to restore the trust level of a loyal customer as compared to a normal customer.

TRA is a psychological theory that was developed by Fishbein (1975), it discusses how the intention of a human to perform an act influences their behavior. The theory presents two important factors in this regard: attitude toward behavior and subjective norms. TRA has been used in multidisciplinary fields, such as strategy, marketing, information systems, etc (Roh T, 2024). The idea that perceived security and trust are the critical factors in restoring consumers' trust in FinTech Roh (2024) aligns with the aspect of cognitive trust because when a consumer makes a decision based on their assessment and evaluation of security, it results in a rational behavior of re-establishing trust, thus resulting in cognitive trust.

Regulatory challenges:

FinTech payment mechanisms are not bound by international boundaries; in case of a dispute, one or more countries are probably involved. In such a case, jurisdictional issues can turn out to be very complicated and can damage consumer trust recovery. Every country has its own set of rules and regulations, and it can be challenging to find out which legal framework should be applied (Razmetaeva, 2021).

Krishna (2023) studied how institutional security commitments impact the trust levels of users in digital payments. The study was conducted among digital payment users in India. The author mentions that the users rely on trustworthiness cues to make trust decisions. However, in most cases, users don't have sufficient skills to analyze the security and privacy aspects of a FinTech platform. The authors highlight the term "cognitive heuristic process" that users use to make decisions. This means that users want to protect themselves from cybercrimes and fraud, but they understand that their skills and knowledge are limited; therefore, post-data breaches, they resort to the most prominent and popular FinTech platforms since they have generally positive reviews.

Krishna identifies three key trust heuristics:

- Users place their trust in platforms that central banks endorse or regulate.
- Consistency — prolonged, reliable usage builds trust.
- Expectancy Violation — unmet expectations (e.g., fraud) make trust recovery difficult.

Another interesting aspect of the study is value congruence. It means that the customer expects the platform to share the same goals and preferences as they. This helps restore trust among the customers that the platform will not harm them in any way.

The absence of an efficient governance infrastructure damages FinTech business operations and customers' trust in them (Mertzanis, 2024). The study focuses on mobile financial service providers and what challenges they must face. For example, the regulations that govern the operational aspect of a payment infrastructure might prevent some FinTech companies from providing services or drive the cost high enough to make them uncompetitive in the market. They can also compromise security measures implemented for the safety of consumers. Hence, consumer trust recovery after a data breach because of weak security measures will be difficult.

Cash Culture Barrier:

For low-income developing economies, consumers still prefer to use cash in their daily life transactions. Kshetri (2018), referred to this cash culture as one of the biggest barriers to using FinTech platforms. In the case of cybercrime, a consumer might resort to cash dealing as compared to digital payment solutions, citing the given risk associated with them. According to a World Bank report, a large portion of Pakistan's economy is cash-based, which limits access to finances and hinders economic development (World Bank, 2017).

A report by Saeed (2018) shows that Pakistan can save around 1.5 billion dollars if it makes a complete transition to a cashless economy. This amount can be saved only from one city, i.e., Karachi, which is the most populated metropolitan city of the country. The report shows that currently, 90% of the city is still using cash transactions instead of utilizing FinTech. The main reasons people prefer cash transactions over digital ones are the absence of suitable digital infrastructure, non-user-friendly applications, and cybersecurity concerns. Research shows that around 50% of consumers think that cash payments are better and safer as compared to digital payments (Sania Zafar Awan, 2021). Therefore, after a data breach, when consumer have already suffered a financial or non-financial loss, they will prefer going back to using cash in their daily life instead of exposing themselves to another probable loss in the future.

Other reasons why cash-based transactions are a barrier are that consumers are used to not disclosing their financial history; they believe that while using digital payments, their financial history will be visible to the authorities, and they don't feel comfortable. In most cases, the major reason is tax evasion. Wholesale merchants prefer cash payments because they are settled on the spot, and they don't have to disclose the purpose of payments. It is also considered to be a buffer in case of crisis because cash means liquidity, Independence, and resilience (Sharif, 2025). In our context, after a consumer falls victim to a data breach, they resort to a cash-based economic system because they feel insecure that their data can cause more trouble. Since they have the opportunity to use a less complicated means of transactions, they can stop using FinTech platforms. Switching back to cash is easier than trusting the same FinTech platform again, where the consumer has been cheated or has incurred a financial loss.

Cybersecurity Awareness:

The awareness of cybersecurity comes from digital and financial literacy. Digital literacy is an individual's ability to understand how to safely use the digital landscape by reaping benefits and avoiding potential risks. Financial literacy stands for an individual's ability to understand and manage their finances and achieve their economic goals. Erum Irfan (2022) defines digital literacy as the literacy of the end-users of the digital economy, which includes both individuals and business users.

Research done by Sultana (2021) showed that illiteracy is a major hindrance to trust among consumers. This is because they are unable to understand their benefits and find it difficult to understand how to navigate the FinTech platforms. In such a case, post-data breach, a consumer would not have the knowledge to re-establish their trust in the platform. Similarly, Medhi (2021) also professes that a lack of literacy negatively impacts FinTech adoption.

Important research was done by Avgerou (2013), which concluded that low financial literacy in developing countries was found to be the biggest barrier to trusting Fintech products and services.

Another research by Ouma (2018), researched the Kenyan mobile payment markets and found that a lack of financial literacy is a significant barrier to trust. A less financially literate consumer doesn't understand how to access security measures or analyze regulatory guidelines. So, if they are scammed, they lack the skills to make an educated decision, and hence would make it very tricky for FinTech companies to restore their trust. In other words, their decision to re-establish trust would be based on affective trust rather than cognitive trust.

Perceived usefulness (PU):

The Technology Adoption Model (TAM) defines perceived usefulness as the extent to which a consumer believes that the use of a product or service will be beneficial to them after a negative experience, like a data breach. Earlier research has found that perceived usefulness impacts FinTech adoption; however, its role in trust recovery is also critical and under-researched. Wang (2020) found that perceived usefulness is directly related to the intention to use digital wallets in China. Tan (2016) empirically tested the positive impact of perceived usefulness on the behavioral intentions in mobile banking services and found that it has a net positive effect. Laura Salciuviene (2014) studied the impact of ease of use, usefulness, security, trust, and confidentiality on customers' intention to opt for financial services. We can learn from this research that if a service is useful and easy to use, then it will directly impact the consumer, and it will be much easier to restore trust. The importance of cognitive factors such as security and ease of use in restoring trust in FinTech can also be learned from the research. After a data breach, if it is still beneficial to use the product, then it will justify its usefulness. As a result, trust recovery will be swift. However, perceived usefulness alone cannot do that unless it is paired with other factors such as perceived security, etc. Perceived usefulness has a greater impact on consumers as compared to perceived ease of use (Davis F. D., 1989). Difficulty post data breach in account restorations might discourage a consumer, but if the platform is no longer useful to them, then they are not motivated to trust it again. This can make trust recovery impossible for FinTech companies.

Based on empirical and theoretical research, it has been proven that higher perceived usefulness will improve FinTech adoption. However, its true impact post-data breach is still unclear. For example, after falling prey to cybercrime, consumers would focus more on how to mitigate their losses, so its risk doesn't outweigh its usefulness. Therefore, it is very important to study the impact of perceived usefulness after a data breach.

Perceived ease of use (EU)

Perceived ease of use can be defined as the degree to which a consumer might believe that the platform is free from effort or easy to navigate (Davis F. B., 1989). When consumers find a FinTech platform that is easy to navigate, they are more likely to continue to use it. However, post data breach, the focus shifts to recovery ease. For example, if a user has been locked out of their account as a result of a data breach, how easily and swiftly they can regain control of their account would translate into ease of use.

TAM considers perceived ease of use as an important aspect of explaining perceived usefulness. Therefore, we can say that perceived ease of use has a positive impact on perceived usefulness (Davis F. B., 1989). For example, if a platform isn't easy to use, then it might be less useful for the consumer to use. Therefore, any variance in ease of usefulness can be explained by understanding ease of use.

Davis (1989) linked ease of use with adoption, but in trust recovery, ease of corrective measures becomes critical. When users find the account recovery process to be troublesome, they stop using it, even if they were user-friendly pre-data breach. Similar studies carried out in India also concluded the same results. In line with what we discussed earlier, perceived ease of use alone can't help improve the trust recovery process unless paired with other factors.

2.6. Theoretical Approaches to Trust Recovery

After analyzing various studies on trust in FinTech, barriers, and challenges, what impacts customer trust, and what are the different aspects of trust, we also look at the possible solutions to their barriers and challenges. Early research by Lewicki (1996) recommended a 4-stage process to trust recovery.

1. Acknowledging that a violation has occurred
2. Determine the cause
3. Admit the act was destructive
4. Accept the responsibility for the consequences

Acknowledging a data breach or any other cyberattack is the first step toward restoring trust among consumers. Followed by determining the actual cause of the breach. Consumers are not just interested in the acknowledgement, they also want to know what caused the data breach to happen in the first place. Admitting the destructive nature of data breaches and accepting responsibility for the consequences makes FinTech look firm. A public apology would establish that the company has accepted responsibility, followed by what they are going to do in the future to ensure that such incidents don't happen again. If a company stands strong during adversity, it sends a positive message to all the consumers, which can then help restore trust.

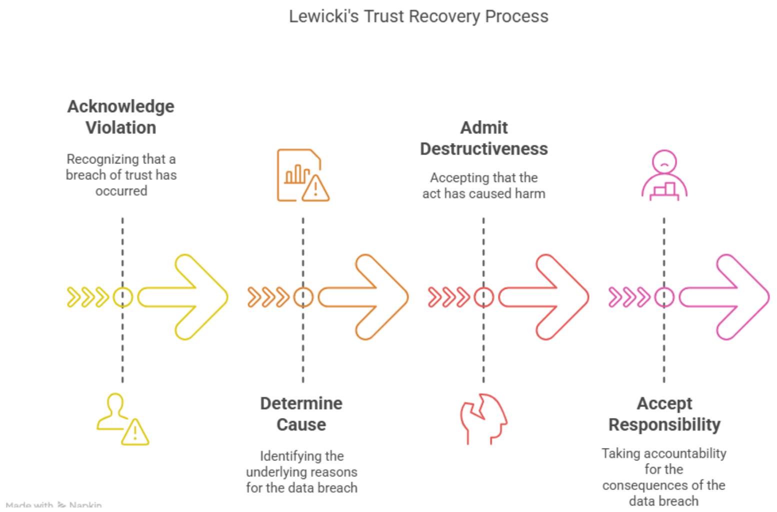

Lewicki's Trust Recovery Process
Acknowledge Violation
Recognizing that a breach of trust has occurred
Determine Cause
Identifying the underlying reasons for the data breach
Admit Destructiveness
Accepting that the act has caused harm
Accept Responsibility
Taking accountability for the consequences of the data breach
Made with Napkin

Figure. 11. Lewicki's Trust Recovery Process (Prepared by Author)

Dietz (2009) carried out research on trust recovery after an organization-level failure. The study can be used to understand what should be done after trust has been damaged in an organization. In our context, a data breach would severely damage the reputation of an organisation, and they have to decide how to handle this precarious situation. The author notes down several important components of trust recovery:

1. Leadership and management practice
2. Culture and climate

3. Strategy
4. Structures, policies, and processes
5. External governance
6. Public reputation

The author suggests that the first thing that needs to be done is to come out as a role model, symbolizing organizational values. Timely communication is critical; for example, trust-enhancing communication can give a positive signal in the market to the consumers. It should be coupled with the assurance that the company will use all the resources necessary to resolve the issue. That includes man-power necessary to find the source of the data breach and money to reimburse consumers for their loss.

For trust recovery, creating a culture that symbolizes trustworthiness is also very important. It will prove that the company is not just communicating positive messages but also creating a necessary climate for consumers to trust the platform again. This also requires a revision to the strategy, which carries trust-based values. Promoting strategies that can foster trust among consumers after a data breach. It also means a revision of old policies. Voluntarily engaging with regulatory bodies, achieving internationally accepted certifications, or licensing can also help restore trust among consumers. For example, a company opts for a license that can serve as proof of enhanced security measures.

Several studies, including Dietz (2009) emphasis on the importance of public apologies and reparations. Communicating with the consumers and focusing on trust-enhancing communication via marketing campaigns and rebranding can also make trust recovery smooth.

The next section will discuss two essential models for trust recovery post-data breach. Lewicki's (1996) presented a 4-stage process for trust restoration, mainly explanation, accountability, and responsibility. Dietz (2009) further develops this model by including leadership, cultural, strategic, regulatory, and communication elements. The thesis will focus on these two models to study trust recovery among consumers in FinTech post-data breach. The main ideas from these models, such as proactive communication, public apology by the CEO, visible security improvements, and effective regulatory framework will be tested in the empirical part of this research.

2.7. Solutions to Barriers

Already established theoretical and empirical research gives some insights on how to overcome barriers to trust recovery in FinTech post-data breach. They include recommendations covering regulatory, technical, organizational, and educational domains.

Regulatory Measures:

A study conducted by Ali (2021) highlights the need for a strong and effective legal framework that can address the problems arising in the modern day. Krishna (2023) and Mazer (2022) focuses more on the importance of consumer protection policies, data control mechanisms, and tokenization to secure digital transactions. In the UK, regulatory sandboxes are being set up that provide legal and financial assurances (Treasury, 2023). Such assurances reinforce trust recovery among consumers of FinTech post-data breach.

Platform-Level Security and Design:

Roh (2024) and Mishra (2024) both emphasize the importance of improving system and service quality. They suggest that it has a strong positive impact on perceived security and user satisfaction among consumers. Dietz (2009) research suggests the need for transparency and proactive communication, which includes informing consumers regarding the data breach and steps needed to avoid such incidents in the future. Some of the security features, such as two-factor authentication, can deliver a clear message of platform reliability.

Staff Training and Communication:

Elsaman (2024) and Abidin (2019) share the opinion on the importance of staff training, and internal audits, focusing especially on data handling and compliance. They are a part of internal monitoring to ensure that staff is adequately informed and educated regarding latest data protection laws and practices. Such practices reduces the percieved risk and improves trust recovery among consumers post-data breach.

Cybersecurity awareness:

Mazer (2022) and Krishna (2023) suggests that FinTech firms should organise educational campaigns regarding cybersecurity, fraud prevention, and digital payment risk. Consumers can be trained on how to adopt behaviours that can ensure maximum protection against online fraud and scams. For exmple, consumers should know how to active security features in their FinTech applicaion, they should also understand the importance of setting up two-factor authentication for logins. During these trainings, fear-appeal messages can also be communicated.

Discouraging Cash culture:

Discouraging cash culture requires changing consumer behaviours and their perception that cash is control. Tax incentives for using digital payment systems could also become a motivational factor for consumers to stop using cash. The UK has implemented effective reimbursement policies that provide consumers with the confidence that their money is safe, and even if they have to face a loss due to any cybercrime, they will be reimbursed. This creates strong trust among consumers, and as a result, discourages cash usage among them.

2.8. Theoretical Framework

In this thesis, the Technology Adoption Model (TAM) proposed by Davis (1989) is selected to be used as it is regarded as the most widely used model, especially for research conducted in the technological world. Jeyaraj (2006) conducted a thorough study of predictors of technology adoption and called TAM one of the widely used technological models. The main reason for its popularity is its simplicity and understandability (Dhagarra D, 2020). It has been used in the field of healthcare services, online system evaluations, telemedicine, and mobile applications. This model presents two determinants:

1. Perceived usefulness: The extent to which consumer believes the product or service to be useful enough to enhance their performance or productivity.
2. Perceived ease of use: The extent to which consumers find using the product easy to navigate.

Singh, Sahni, & Kovid (2021) studied the impact of ease of use and perceived usefulness on the intention to use FinTech services. While Bongomin (2020) found evidence that trust was not only the central concept in enhancing mobile money adoption among individual consumers but also that it impacts financial inclusivity. Patria Laksamana (2023) took this step forward by studying the impact of trust among other variables such as perceived usefulness, ease of use, and risk on customer attitude. A similar study from Waechter (2017) discusses how reliability, competence, and security impact user trust in mobile banking.

Over the years, this framework has been extended by other researchers to include other variables as well. We will be using TAM to understand how consumers respond to data breaches. However, originally TAM can only comprehend stable trust concepts, but a data breach damages the perceived usefulness and ease of use. Therefore, we will extend TAM by adding more variables for better understanding.

Modification to the Technology Adoption Model (TAM): For our research, we will extend the current TAM by incorporating barriers that create friction to trust recovery. These barriers were identified keeping Pakistan's FinTech landscape in mind. For example, cash culture is not a valid barrier or a variable in a developed cashless economy; however, for Pakistan, it is a major barrier. While TAM can help us focus on PU and PEOU as signals for technology adoption, post-data breach trust recovery would require investigating what factors can shape consumers' willingness to trust the FinTech product or service again.

The following conceptual model demonstrates the steps FinTech consumers need to take to rebuild trust after a data breach occurs. The first step in this process leads to trust erosion because consumers experience a breach of their expectations, and their sensitive information becomes exposed. The model shows that trust restoration faces multiple obstacles, including perceived risk and weak regulatory frameworks and cybersecurity concerns and low digital literacy, and cash-based preferences. The barriers create obstacles that prevent consumers from reusing the platform.

The model implements theoretical solutions to overcome these obstacles through improved security protocols and regulatory changes and user training, and proactive communication approaches. The implemented interventions work to reduce the adverse effects of each barrier while helping to rebuild trust. The model reaches its conclusion with trust restoration when consumers develop confidence about the safety and reliability, and value of the FinTech platform.

If the perceived risk is higher, then it would be difficult for the consumers to trust the FinTech product or service again. Similarly, if the regulatory challenges are higher and consumers believe that he is vulnerable in the current data breach scenario, then trust recovery will be much slower. A strong cash culture will also contribute to slowing down the re-establishment of trust in FinTech products. Post-data breach, weaker cybersecurity awareness will hinder the trust recovery process.

On the other hand, if the FinTech platform implements stronger security measures, then it would help increase the perceived security. This will help consumers regain their trust in the platform much faster. Another important aspect is that the product is still useful for the consumer and easy to use after a data breach. Make sure it is easy for consumers to regain control of their accounts after a data breach or cyberattack. Transparency, as discussed in the theoretical solutions, is of utmost importance. Effective, timely communication with consumers, data breach reports, and clear communication of security and prevention measures can significantly contribute to trust recovery. All these identified barriers directly affect perceived trust recovery, which will help consumers re-establish their trust in FinTech products and services.

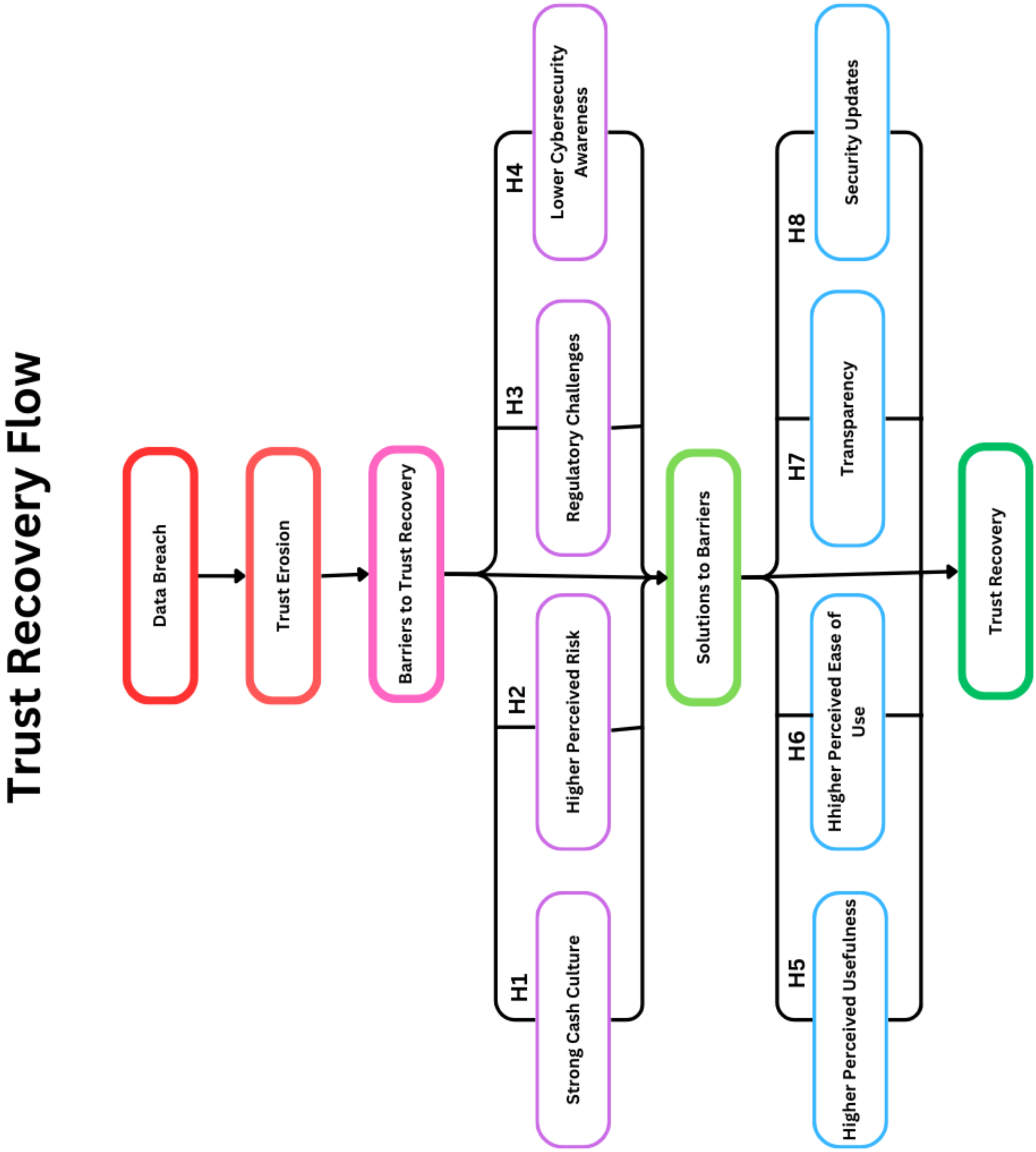


Figure. 12. Conceptual Model for Trust Recovery (Prepared by Author)

2.8.1 Hypothesis

Based on the conceptual model and barriers discussed in the previous section, we can now develop hypotheses to understand the most impactful and important barriers to re-establishing trust in FinTech consumers.

H1: A strong cash culture contributes to delayed trust recovery among consumers (Sania Zafar Awan, 2021) (Saeed, 2018).

H2: Perceived risk has a negative impact on trust recovery post-data breach (Ali M, 2021) (Hosam Elsaman, 2024).

H3: Weak regulatory structure slows down trust recovery (Krishna, 2023) (Melnyk, 2024).

H4: Lower Cybersecurity awareness damages trust recovery post-data breach (Krishna, 2023) (Erum Irfan, 2022).

H5: Higher perceived usefulness fosters trust recovery among consumers (Ali M, 2021) (Wang, 2020).

H6: Higher perceived ease-of-use accelerates trust recovery post-data breach (Davis F. B., 1989) (Yang, 2012).

H7: Proactive transparency after a data breach helps speed trust recovery among consumers. (Dietz, 2009)

H8: Visible security updates enhance trust recovery post-data breach (Roh T, 2024) (Pavlou, 2003).

3. Research Methodology

The theoretical analysis performed in this study helped determine the main constructs that influence consumer trust recovery in FinTech services following a data breach. The model has its roots in the TAM, and it includes constructs such as perceived risk, perceived security, regulatory challenges, cybersecurity awareness, cash culture, and transparency. The theoretical findings from the previous chapters helped in determining the variables and in designing the questionnaire. The research will help find a visible link between behavioural theories and actual issues related to trust in FinTech post-data breach.

Quantitative research design was used to analyse barriers to trust recovery in FinTech post-data breach in the Pakistani FinTech market. The major objective of this research was to understand what the key barriers to trust recovery are once initial trust has been damaged due to cybercrime, and then how that trust can be recovered.

The Aim and Objectives:

The research aims to understand barriers to trust recovery in FinTech for customers in Pakistan after digital fraud and data breaches. This research will also suggest solutions to overcome those barriers.

For the above-stated aim, the objectives of the research are as follows:

- To perform a situational analysis of trust in FinTech post-data breach and financial fraud in Pakistan.
- To theoretically substantiate existing barriers to trust in FinTech.
- To substantiate research methodology for managerial actions to overcome key barriers to trust recovery in FinTech platforms in Pakistan.
- To propose managerial solutions and recommendations for overcoming key barriers to consumer trust recovery in FinTech platforms in Pakistan.

3.1. Research Design

Research Method

According to Creswell (2014), quantitative research is most suitable when the goal is to examine cause-effect relationships and generalize findings to a larger population. The hypotheses designed in the previous section were required to be statistically tested to establish clear relationships. The research design enabled the application of statistical methods, including regression and factor analysis, to test the theoretical model in a structured and replicable manner. Therefore, quantitative methods were used to standardize data and then analysed using statistical tools.

Research Sample

A total of 187 valid responses were collected from the consumers of FinTech. The sample size was good enough to perform statistical analyses such as regression and factor analysis. However, if we consider the total number of complaints received by the FIA of cybercrimes, for generalization, the sample should have been more than this. Therefore, we will proceed with exploratory research. Non-probability sampling methods were used to avoid sample size calculations. For valid statistical analysis, the minimum sample size was 150 respondents, therefore, 187 responses were enough to perform the required statistical analysis.

Research Process

The questionnaire was circulated between 12th April and 22nd April. A total of 193 responses were received, but 187 responses were accepted. Given the specific nature of the research, the snowball sampling method was used. Participants of the survey were contacted through professional networks, such as LinkedIn, social media groups of FinTech, and FinTech activists in Pakistan via WhatsApp.

Research Ethics

Utmost care was practiced to maintain ethical research standards during the data collection period. All the participants of the survey were informed about the objectives of the research and were also given the choice to complete the questionnaire voluntarily. It was explicitly mentioned that their data will not be stored and nor be used to ensure anonymity. The respondents had the option to leave the questionnaire at any point. This informed consent was taken from every participant before the beginning of the survey. The research study implemented standard ethical protocols for social science research while maintaining complete transparency and respect for all participants.

Research Instrument

A standardized questionnaire was used to collect the data from the consumers. The questionnaire had sections for both consumers who suffered a data breach and those who didn’t, to have a more holistic view of trust recovery. In total, there were three sections: section A covers general FinTech users, section B for those who experienced a data breach, and section C to identify the top three trust diminishers and builders.

Section A: General FinTech Usage (All Respondents). This part of the questionnaire investigated what FinTech products consumers use, and what kind of fraud or scam they have suffered.

FinTech Usage: The first questions were asked if the respondent uses FinTech applications or not. If they do, then they were asked to mention what FinTech applications respondents are using, for example, mobile banking applications, JazzCash, EasyPaisa, NayaPay, SadaPay or any other application.

Respondents were asked if they have suffered some kind of cybercrime. If they didn’t suffer any cybercrime, then the questionnaire will take them to Section C. If they did, then they were asked, what kind of cybercrime they had faced which resulted in any financial or nonfinancial loss. After which they were allowed to proceed to Section B of the questionnaire.

Section B: Respondents who experienced some kind of scam or fraud were asked to select from the list of cybercrimes. The possible fraud incidents were:

- Unauthorized transactions
- Impersonation scams via phone calls
- Personal data breaches
- Fraudulent FinTech service providers
- Other (open response)

Further in this questionnaire, responses from the respondents were measured on a 5-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree). The list of constructs is as follows.

- Cash Culture (adapted from (Sania Zafar Awan, 2021) (Saeed, 2018))
- Perceived Risk (K. Gupta, 2023) (Lee, 2009)
- Regulatory Challenges (Sohail, 2024) (Ahmad Fraz, 2021)
- Cybersecurity Awareness (Tick, 2021)
- Perceived Usefulness (Cheng TCE, 2006)
- Perceived Ease of Use (Cheng TCE, 2006)
- Transparency (Dietz, 2009)
- Security Updates (Jia Qi, 2024) (Patria Laksamana, 2023)
- Perceived Trust Recovery (Awad, 2008)

Three questions were asked for each construct to have an enriched insight into consumers' behaviours.

Section C: Organizational Trust Recovery Measures (All Respondents). As discussed below, this section was meant for all respondents, regardless of whether they suffered a data breach or not. These included:

- Public disclosure of breaches
- CEO's apology and responsibility
- Reimbursements
- Security upgrades (e.g., biometric login)
- Regulatory partnerships and audits
- Consumer education programs
- Staff training
- 24/7 fraud support in local languages

Trust Builders and Trust Diminishers:

The respondents chose their top three Trust Builders (e.g., instant refunds and notifications, multi-factor authentication, government approval, privacy policies, awareness campaigns, and 24/7 support) and Trust Diminishers (e.g., customer support deficiencies and unreported breaches and app failures and delayed notifications and complicated interfaces and unauthorized data transfers and invisible security enhancements).

Research Data Analysis:

The data was exported to Excel directly from Google Forms. The data was then cleaned and formatted in Excel before being analysed in SPSS. The data was imported into SPSS, and statistical tests were performed on the data for analysis purposes. The types of statistical analysis carried out on this data are as follows:

1. Descriptive analysis
2. Correlations
3. Regression
4. Factor Analysis (7 Factors)
5. Reduced Model
6. Organizational Responses

7. Crime type ANOVA
8. Trust builders Regression
9. Trust Diminishers Regression

Limitations of the research:

Given the current exploratory nature of the research, valuable insights were revealed into trust recovery. However, the number of cases reported to the Banking Mohtaisb of cybercrimes, and the FIA, the ideal sample size for generalization would have been more than 300 respondents. Keeping in mind that such cases are underreported. Due to time and budget constraints, only 187 valid responses were collected. The snowball sampling methods helped reach cybercrime victims, but it also introduced sampling bias, limiting the diversity of the data set.

Another limitation of the research is that it only focuses on statistical analysis and fails to capture the emotional and contextual depth of qualitative analysis. Factors like shame, fear, and social pressure are not possible to quantify in quantitative statistical analysis. Also, understanding cash culture requires a deeper qualitative analysis of society.

The discarded responses showed that some of the respondents were not aware of the term FinTech, or what comes under this umbrella. Therefore, there is a possibility that some of the responses received were either misunderstood or exaggerated. Regardless of these limitations, the study revealed valuable insights into understanding trust recovery factors among consumers of FinTech in Pakistan post-data breach.

4. Results of the Statistical Analysis

Descriptive Analysis:

The following research is based on statistical findings based on the responses received from FinTech consumers of Pakistan who suffered cybercrimes. Descriptive analysis was conducted on the data to summarize consumer perception of trust recovery. A correlation analysis was then performed to find relationships between the variables. Then, a multiple regression analysis was applied, followed by factor analysis to find what the key factors influencing trust recovery in FinTech post-data breach are. Based on the factors identified in the factor analysis, a reduced model analysis was carried out to grade the three top variables. Organizational responses were analysed separately, along with the top three trust builders and trust diminishers. The analysis confirmed some of the hypotheses, while some failed to be statistically significant.

Descriptive analysis:

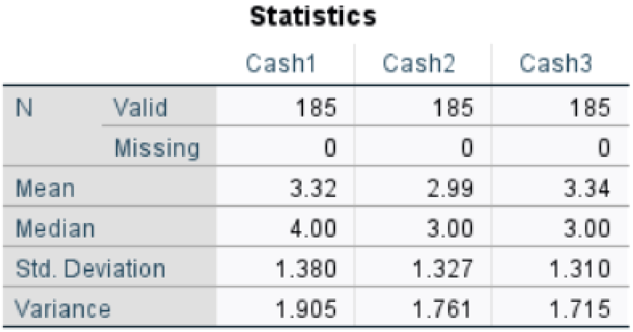
The research applied descriptive analysis to examine cash culture and perceived risk and regulatory challenges and cybersecurity awareness and perceived usefulness and ease of use and transparency and perceived security, and perceived trust because these variables emerged from the literature as essential factors that affect consumer trust in FinTech platforms, particularly in post-cybercrime contexts. The research expanded the Technology Acceptance Model (TAM) through the addition of trust-related and culturally relevant constructs to enhance understanding of trust recovery. The analysis reveals how participants felt about each factor following their FinTech cybercrime experience.

Cash Culture:

Cash culture as a whole showed neutral to mildly positive perceptions, while responses varied among the respondents. The deeper analysis confirms this pattern because some consumers have a clear tilt towards cash, whereas others still prefer FinTech to some extent. It also highlights the fact that cash culture needs an even deeper qualitative investigation for better understanding. Later in the study, we will see how important cash culture is and how big an impact it can create in trust recovery post-data breach.

For a deeper understanding of how cash culture impacts consumer trust recovery post-data breach, we carried out item-level analysis. In the table below, Cash1, Cash2, and Cash3 are the three questions asked of consumers under the category of cash culture.

Table 2. Item-level mean scores of cash culture



Statistics

		Cash1	Cash2	Cash3
N	Valid	185	185	185
	Missing	0	0	0
Mean		3.32	2.99	3.34
Median		4.00	3.00	3.00
Std. Deviation		1.380	1.327	1.310
Variance		1.905	1.761	1.715

Cash is more convenient (Cash1):

The respondent of the questionnaire shows moderate behavior when asked if they find cash more convenient as compared to cash (mean = 3.32). The standard deviation of 1.380 shows that the responses were highly varied. This is possible due to respondents having different social classes, income levels, and FinTech awareness. Consumers who belong to a lower social class usually carry out purchasing on buying in public markets, where people prefer to use cash due to its high level of acceptability. Whereas consumers who belong to a higher social class usually transact online or in shopping malls, where digital payments are acceptable. Therefore, based on their background, cash can be convenient for one but not for the other, even after they have suffered a data breach.

Responses were scaled on a 5-point Likert scale; therefore, the above table shows the frequency each point was selected. For example, the highest percentage of respondents (27%) strongly agree with the statement that cash is more convenient. 23% of the respondents agreed using 4 on the scale, followed by 21% choosing 2, showing they don't perceive cash as more convenient. We can say that almost half of the respondents who suffered some kind of cybercrime perceive cash as more convenient.

Avoiding FinTech after Data Breach (Cash2):

The descriptive analysis of the questions about whether consumers have started avoiding FinTech post-data breach shows neutrality (mean = 2.99, SD = 1.33). This means that while some consumers have indeed started avoiding FinTech after the data breach, others still use FinTech with caution. The frequency table below also shows that the responses are almost evenly distributed. But we can still say that consumers still use FinTech since almost 25% of them disagree with the statement, and nearly 24% of them were neutral.

Cash is simpler than Digital Payments (Cash3):

A similar pattern can be observed in the third question, whether cash is simpler to use as compared to digital payments. The question was asked to see if consumers feel cash is simpler than FinTech, where there is a probability of data breach or cybercrime. The responses were widely spread, with a mean of 3.34 and a standard deviation of 1.31. These figures explain that for some consumers, cash is more intuitive and familiar than FinTech post-data breach.

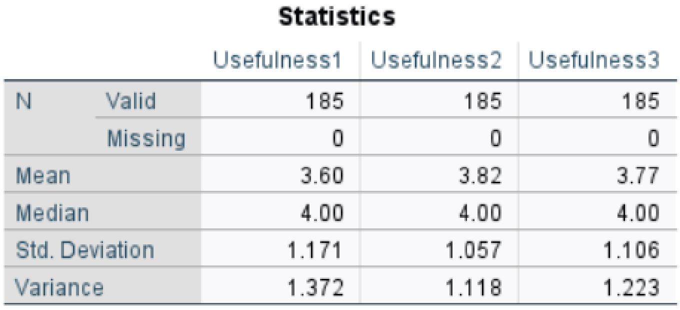
The frequency table also shows a somewhat similar pattern as before, nearly 25% of the respondents show neutrality, whereas 26.5% strongly agree with the statement. We can say that nearly half of the consumers agree that cash is simpler than FinTech. This frequency distribution also supports the mean score, showing a slight tilt towards agreement on this statement.

The analysis reveals that cash preference was not absolute; some consumers prefer cash over digital payments post-data breach, but the avoidance of FinTech was found to be weak. This is a positive sign, FinTech firms can still retain consumers and restore their trust by offering reimbursements, cybersecurity education, active communication, security updates, etc. However, this requires a deeper analysis of the cultural nuances in Pakistan. In order to address this, FinTech firms need to understand the cultural aspect of this construct.

Perceived Usefulness:

Perceived usefulness means how much a consumer considers the FinTech platform beneficial and efficient, even post-data breach. The descriptive analysis of perceived usefulness shows that consumers still perceive FinTech platforms as convenient and useful (mean = 3.73). Post-data breach, consumers believe that FinTech is still playing a positive role in their payment requirements. This analysis highlights that even though data breach damages consumer trust in FinTech, the functional value of digital payments can still be identified by the consumer. This could be a positive sign for trust recovery since it can serve as a balancing force. If the consumer still believes that FinTech products are useful, then it is easier for the FinTech firms to regain their trust.

Table 3. Item-level mean scores of usefulness



Statistics

		Usefulness1	Usefulness2	Usefulness3
N	Valid	185	185	185
	Missing	0	0	0
Mean		3.60	3.82	3.77
Median		4.00	4.00	4.00
Std. Deviation		1.171	1.057	1.106
Variance		1.372	1.118	1.223

Using online banking is still useful after cybercrime (Usefulness1):

An in-depth analysis of perceived usefulness was also carried out to understand consumer perception. When the consumers were asked whether online banking is still useful to them after the data breach, around 56% of them either agreed or strongly agreed with the statement. Only a minimal percentage of just over 4% disagreed with the statement. These results show that consumers still believe that FinTech products are useful for them even after they have suffered from data breach or other cybercrimes.

Online banking provides significant benefits (Usefulness2):

When consumers were asked about the benefits of FinTech products post-data breach, more than 67% of them either agree or strongly agree with the statement. This shows that even after a data breach, consumers still acknowledge and understand the benefits of FinTech products. The consumers are not letting their bad experience with a product ruin their perception of how beneficial using FinTech can be in their daily life. This can be very positive for the FinTech firms as well in their journey of restoring consumer trust in their products.

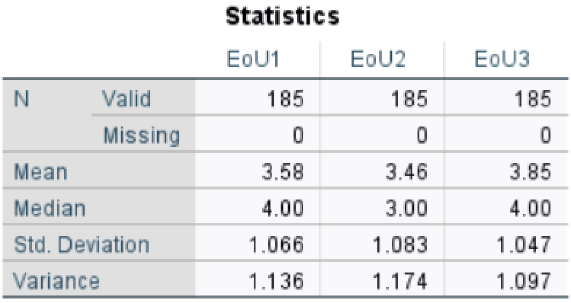
Online banking saves a lot of time (Usefulness3):

A large population of consumers believes that using FinTech products can save a lot of time. Around 65% of them either agree or strongly agree with this statement. Just over 2% of the respondents strongly disagree with the statement, which is negligible. These results show that consumers do understand that FinTech products can save them a lot of time, as traditional payment methods are very slow and time-consuming. The acknowledgment of its usefulness shows that consumers might still want to use FinTech products, or will do so in the future, given that their trust has been fully restored.

Perceived Ease-of-Use:

Ease of use construct measures how effortlessly consumers can use FinTech products while carrying out their routine tasks. The descriptive analysis of ease-of-use shows a mean value of 3.63, which is nearly the same as perceived usefulness. Both core elements of the TAM show a similar pattern among consumers post-data breach. The consumers still consider FinTech products to be easy to use. Given the case with cash convenience, ease-of-use can be of significant importance. The moment consumers feel that FinTech products are not easy to use, they will resort to using cash, damaging FinTech adoptability. Similarly, in our case, if the consumers feel like they were scammed or suffered a data breach, the FinTech product has to be at least easy to use. However, we will do an item-level analysis of this variable as well to better understand how consumers feel FinTech products are easy to use.

Table 4. Item-level mean scores of ease of use



Statistics

		EoU1	EoU2	EoU3
N	Valid	185	185	185
	Missing	0	0	0
Mean		3.58	3.46	3.85
Median		4.00	3.00	4.00
Std. Deviation		1.066	1.083	1.047
Variance		1.136	1.174	1.097

FinTech products are easy to use after security updates (EoU1):

When the consumers of FinTech were asked if FinTech products were easy to use after security updates, 53% of them either agreed or strongly agreed with the statement (mean = 3.58, SD = 1.07). Only 15% of the respondents strongly disagreed or disagreed with the statement. These results show that post-data breach consumers believe that FinTech products are easy to use. At times, enhanced security measures make FinTech products complicated to navigate. Therefore, understanding whether these products are still easy to use is of crucial importance. In this case, most of the consumers agreed to this statement.

Periodic security updates make digital services easier (EoU2):

With the lowest mean value in this construct, 49% of the respondents either agreed or strongly agreed with this statement (mean = 3.46, SD = 1.08). These results show that consumers agree that security updates have made their digital experience easier. However, since it has the lowest mean among all others, it shows that security updates are not always considered as improvements in their utility.

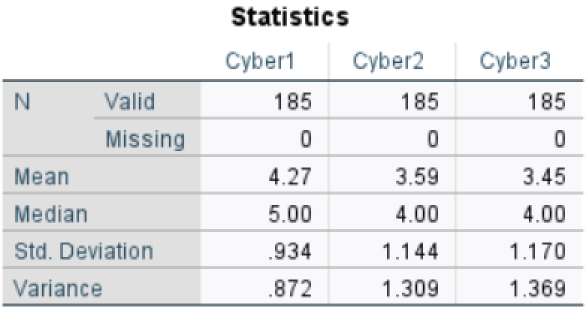
Making online transactions is simpler (EoU3):

Having a mean value of 3.85, around 67% of the respondents agreed that making online transactions is simpler using FinTech products. This means that post-data breach, consumers still consider that online payment mechanisms are simpler to use, keeping the credibility of the overall fabric. This can be used by the FinTech firms in their trust recovery journey, highlighting that consumers' experience in using FinTech products is simpler.

Cybersecurity Awareness:

Cybersecurity awareness measures how informed a consumer is regarding protecting themselves from online threats. The overall mean score for cybersecurity awareness in our descriptive analysis was 3.77, showing consumers became very conscious regarding their cybersecurity after experiencing a data breach. Consumers become more alert and cautious once they have suffered a loss in a data breach. Our analysis shows that cybersecurity awareness plays a very significant role in understanding post-data breach consumer behavior.

Table 5. Item-level mean scores of cybersecurity awareness



Statistics

		Cyber1	Cyber2	Cyber3
N	Valid	185	185	185
	Missing	0	0	0
Mean		4.27	3.59	3.45
Median		5.00	4.00	4.00
Std. Deviation		.934	1.144	1.170
Variance		.872	1.309	1.369

I wouldn't reveal any information (cyber1):

An item-level analysis of the cybersecurity awareness construct was conducted to understand consumer trust levels post-data breach. When respondents were asked if they wouldn't reveal any information to unknown sources, 79% of them agreed or strongly agreed with the statement. The mean score was found to be 4.27, which was the highest among all constructs. This shows that a majority of consumers understand the importance of keeping their information safe. It also shows that they understand online threats and what methods are commonly used to cheat consumers online.

Aware of the latest online threats (cyber2):

Regarding awareness of online threats, nearly half of the correspondents agreed that they can identify threats. The mean score was found to be 3.59, which is slightly lower than the first one, showing a positive sign. Only 17% of the consumers disagreed with the statement, showing slightly lower cybersecurity awareness. Overall, we can say that consumers were largely aware of online threats, which confirms our earlier analysis that consumers become conscious after a data breach.

How to activate security features (cyber3):

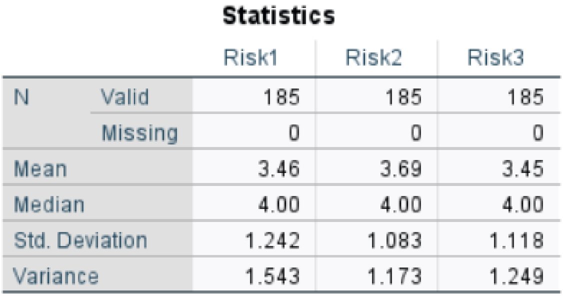
This question was asked to understand if consumers understand how to activate security features in their FinTech products. The overall score was found to be neutral, with 3.45, showing that consumers were indifferent. Approximately 50% of the respondents either agreed or strongly agreed with the statement that they know how to activate security features. But a good percentage of 27% were found to be neutral, with 22% disagreeing with the statement. It shows that not all consumers are aware of how to use the application properly or to their best advantage. FinTech firms need to educate consumers to ensure that they understand how to protect themselves from online threats.

The initial analysis shows that consumers do understand online threats. FinTech firms should also understand that cybersecurity awareness goes beyond fear messages and occasional alerts. They should ensure that consumers are properly aware of the prevailing frauds and scams.

Perceived Risk:

Perceived risk measures the level of uncertainty among consumers, or the risk that is associated with using FinTech products. The mean score of perceived risk was found to be moderate at 3.53. Which means that consumers were rather moderate in perceiving risk post-data breach. This risk can include the risk of financial loss, data leakages, etc. A deeper analysis of the perceived risk will give us insight into this construct.

Table 6. Item-level mean scores of perceived risk



Statistics

		Risk1	Risk2	Risk3
N	Valid	185	185	185
	Missing	0	0	0
Mean		3.46	3.69	3.45
Median		4.00	4.00	4.00
Std. Deviation		1.242	1.083	1.118
Variance		1.543	1.173	1.249

Online banking is extremely risky (Risk1):

When consumers were inquired if they believe online banking is extremely risky as compared to physical transactions. The mean score was found to be 3.46, showing mixed responses. The standard deviation was found to be 1.24, which shows a wide variability. Around 53% of them agreed to it. However, a quarter of respondents disagree with the statement as well, showing that some consumers believe that online banking is a very risky post-data breach.

Fear of not getting a reimbursement for financial loss (Risk2):

With a mean score of 3.69, this item had the highest value among others. Around 56% of the consumers either agree or strongly agree with the statement that consumers fear they will not be reimbursed if they suffer a financial loss. These results show consumers' fear of losing money, indicating the need for clear reimbursement policies in FinTech companies. This is not a positive sign for FinTech firms, but also provides an opportunity to address this issue for trust recovery. Later in the thesis, we will analyse if this construct has any significant impact on trust recovery.

Worry that personal data can be misused (Risk3):

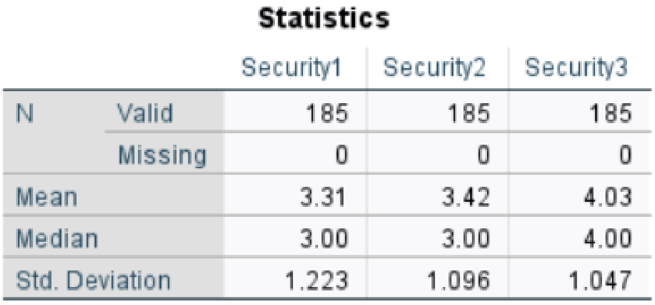
The worry of personal data being misused by someone had a mean score of 3.45. Following a similar pattern, around 51% of the respondents either agreed or strongly agreed with the statement. However, a sizeable percentage of 26.5% of respondents showed neutral behavior. It is possible that consumers don't understand the privacy policies or how data is handled by FinTechs.

It should be a FinTech firm's top priority to remove all ambiguities from the mind of their consumers by giving guarantees, security updates, transparency etc. These actions will bring perceived risk levels down among consumers, which can eventually improve the trust recovery process. Without addressing all the issues, or addressing some of them, might not provide useful results.

Perceived Security:

Perceived security means how consumers evaluate security improvements in trust recovery. From our theoretical analysis, we know that security updates are only useful when they are explicitly seen by the consumers. The overall trend was found to be positive, however, we ran an item-level analysis of the items included in this construct.

Table 7. Item-level mean scores of perceived security



Statistics

		Security1	Security2	Security3
N	Valid	185	185	185
	Missing	0	0	0
Mean		3.31	3.42	4.03
Median		3.00	3.00	4.00
Std. Deviation		1.223	1.096	1.047

Payment transaction information is secure (Security1):

The mean score of this item was found to be 3.31, which shows a moderate trend. 48% of the respondents agree with this statement that their payment transaction information is secure despite the data breach. 26% of them disagree that their payment transaction information is secure, which shows a breach of trust. A quarter of them choose to be neutral. This analysis shows that most consumers are skeptical about the platform's security post-data breach.

Noticed visible security improvements after breach (Security2):

The second-highest mean score of this construct was for the item about noticing visible security improvements. The analysis shows that 56% of the consumers agreed that they have noticed a visible security post-data breach; conversely, only 19% disagreed with it. Consumers tend to trust more when they notice visible security measures being taken.

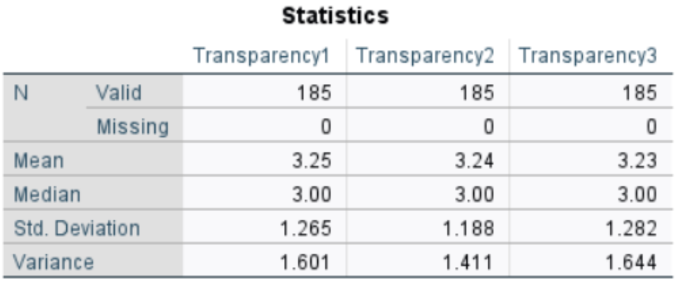
Two-way authentication makes FinTech more secure (Security3):

With the highest mean score of 4.03, 72% of the respondents agreed that two-way authentication makes a FinTech application more secure. This means that two-way authentication is perceived as a symbol of trustworthiness and safety. Other features like biometric login is also part of visible security cues, which help improve trust recovery post-data breach.

Perceived Transparency:

Perceived transparency in our context means how effectively a FinTech firm communicates the causes of the data breach and steps to prevent such breaches in the future. We learned from the theoretical review that firms that openly communicate with consumers are considered to be more trustworthy. Perceived transparency showed mixed responses from consumers of FinTech post-data breach. Transparency is indeed a crucial factor for trust recovery, however, not every consumer might feel that their firm has been transparent with them. Our analysis highlights the importance and the need to establish a crisis communication cell and guidelines to handle consumers in case of a data breach.

Table 8. Item-level mean scores of perceived transparency



Statistics

		Transparency1	Transparency2	Transparency3
N	Valid	185	185	185
	Missing	0	0	0
Mean		3.25	3.24	3.23
Median		3.00	3.00	3.00
Std. Deviation		1.265	1.188	1.282
Variance		1.601	1.411	1.644

The company communicated the cause of the breach (Transparency1):

The purpose of asking these questions was to see the level of transparency consumers perceived from their FinTech products. The mean score in descriptive analysis was found to be 3.25. Around 46% of the consumers who responded to the questionnaire either agreed or strongly agreed that their company communicated the cause of the data breach. However, more than a quarter of respondents remained neutral. These results show varying levels of transparency across FinTech platforms.

Received timely updates about the breach (Transparency2):

When respondents were asked if they received timely updates about the data breach, 47.6% of them either agreed or strongly agreed (mean = 3.24). A quarter of respondents also disagreed with the statement that their firms did not provide timely updates. Our analysis shows that many firms need to be vigilant in this area and ensure that consumers receive timely updates.

Communicated steps to prevent breach in the future (Transparency3):

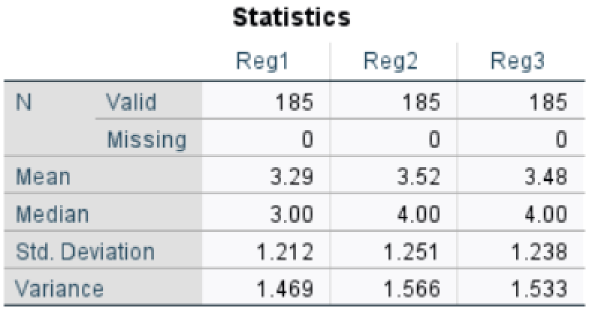
The analysis shows that nearly 45% of the respondents were informed of what measures to take to ensure safety in the future (mean = 3.23). While 30% disagreed with the statement, showing questionable behavior by the FinTech firms post-data breach, by not informing consumers on what steps should be taken. Such behavior could become a major barrier to trust recovery efforts by the FinTech firm. It also confirms the earlier analysis, highlighting the importance of effective communication.

Transparency has been one of the most powerful tools that a FinTech firm can use to restore consumer trust post-data breach. However, our analysis shows that FinTech firms might not be using this tool very effectively. Effective communication during crisis periods is more important than having a strong infrastructure or security protocols. Consumers want to communicate their concerns and want some kind of response. When they are unable to do so, they feel frustrated, damaging trust recovery.

Regulatory Challenges:

Regulatory challenges measure the effectiveness of the regulatory framework in trust recovery. From our theoretical analysis, we understand that when consumers believe that the regulatory framework is strong enough to protect their rights, trust recovery is strong. Conversely, regulatory challenges weaken trust recovery in FinTech. An in-depth analysis of regulatory challenges was carried out to understand how consumers of FinTech post-data breach perceived regulatory effectiveness.

Table 9. Item-level mean scores of regulatory challenges



Statistics

		Reg1	Reg2	Reg3
N	Valid	185	185	185
	Missing	0	0	0
Mean		3.29	3.52	3.48
Median		3.00	4.00	4.00
Std. Deviation		1.212	1.251	1.238
Variance		1.469	1.566	1.533

FinTech regulations in Pakistan are not well developed (Reg1):

Respondents were asked if they believe the Pakistani FinTech regulations to be well developed. The analysis shows that 47% of them either agreed or strongly agreed that the FinTech regulations are not well developed in the country. A significant portion of 28% disagree with the statement, showing their trust. Differing views based on personal experiences and news could be an explanation of these results (mean = 3.29).

Victims of data breaches don’t get justice (Reg2):

With the highest mean score of 3.52, this question shows whether consumers trust that they will get justice or not. The analysis shows that 54.6% of the respondents agree that victims don’t receive justice in the case of a loss or data breach. These results are worrisome since a large majority lack confidence in regulatory effectiveness. This can greatly damage trust recovery post-data breach, consumers will feel vulnerable and exposed to any threats without any protection.

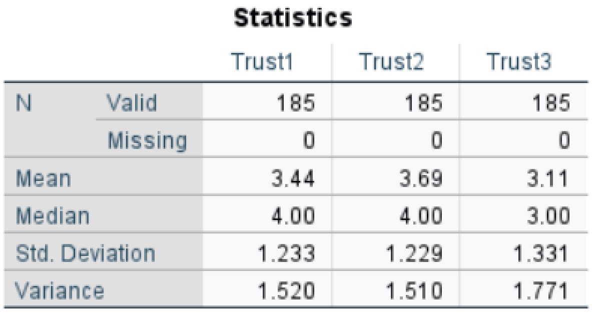
Current regulations need to adopt current innovation (Reg3):

Following a similar pattern, 54% of the respondents show that the prevailing regulations are outdated and don't address the modern-day challenges. These results call for regulations that are better suited to address the issues posed by current innovations. These regulations might not directly impact trust recovery but would impact the process.

Perceived Trust Recovery:

Perceived trust recovery measures the extent to which consumers can trust their FinTech products post-data breach. The whole purpose of this study was to understand trust recovery after a consumer has suffered losses. The analysis shows that the trust has not been fully restored among the consumers post-data breach. We will analyse them in depth to understand if consumers would be willing to recommend the FinTech product to someone else, and if they believe their problems can be solved in time by their service provider.

Table 10. Item-level mean scores of perceived trust



Statistics

		Trust1	Trust2	Trust3
N	Valid	185	185	185
	Missing	0	0	0
Mean		3.44	3.69	3.11
Median		4.00	4.00	3.00
Std. Deviation		1.233	1.229	1.331
Variance		1.520	1.510	1.771

Trusting a digital service provider post-data breach (Trust1):

This item was asked to see whether consumers still trust their FinTech products, or not, especially after a data breach. The analysis showed that nearly 52% of the respondents agreed that they do trust their service provider. However, nearly a quarter of them disagree with the statement as well, showing trust has not fully recovered among all consumers. This highlights the need to understand trust recovery factors, which is the purpose of this study.

I would recommend using FinTech despite the data breach (Trust2):

With the highest mean score of 3.69, nearly 59.4% of the respondents agree that they would be willing to recommend FinTech despite the data breach. These results confirm our previous analysis that, despite a data breach, consumers still acknowledge that FinTech products are useful and save time. Knowing the functional value of FinTech products, consumers are willing to recommend others to utilize these products.

Confident that a digital service provider can solve problems in time (Trust3):

Opposite to the last item, this has the lowest mean score of 3.11. This item shows if consumers are confident that their digital service provider can solve their problems in case of a data breach. Around 40% of the respondents either agreed or strongly agreed to this statement, but over 34% disagreed, while a quarter remained neutral. Overall, our analysis shows a weak trust in the service provider from the consumers post-data breach. This also presents an opportunity for FinTech firms to address these issues for a swift trust recovery.

The analysis shows that even though consumers still believe FinTech firms are useful and easy to use, they still don't trust their service providers to help them in case of need. In order to develop this trust, FinTech providers need to demonstrate that they are competent enough to handle a data breach maturely and openly. Problem resolution post-data breach is of utmost importance, it comes along with transparency.

(Refer to Appendix 2 for details.)

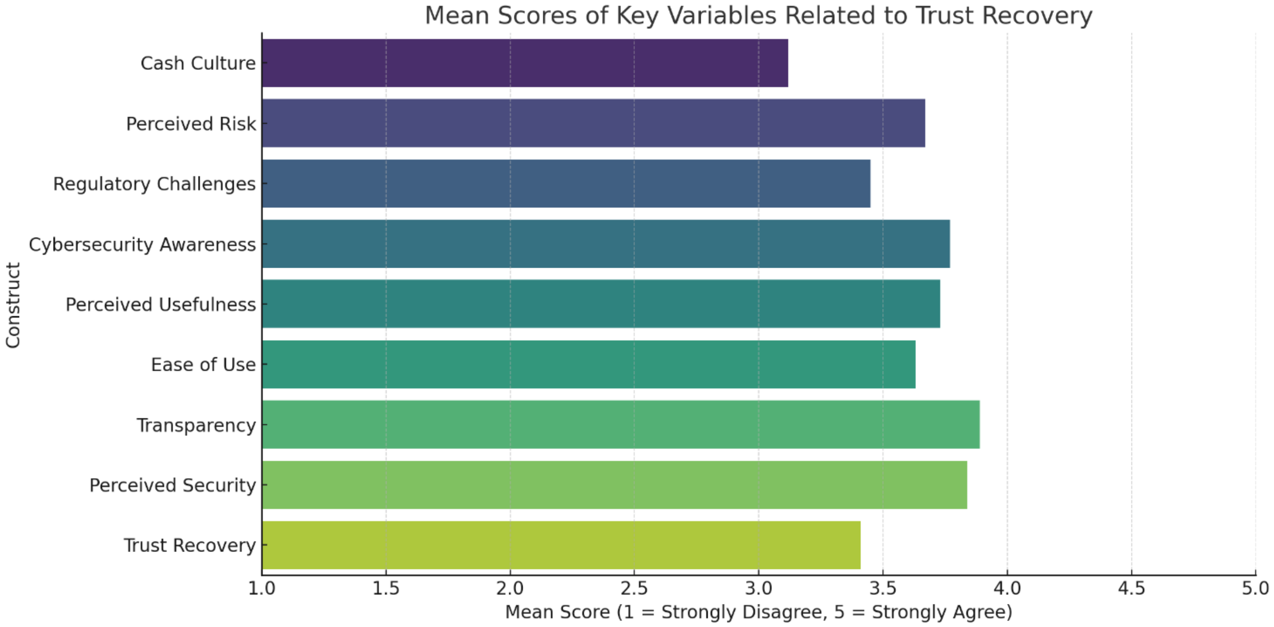


Figure. 13. Consumer perceptions of FinTech security and benefits (Prepared by Author)

Correlation analysis

To study how these variables relate to trust recovery, Pearson's correlation analysis was conducted. This test will help analyse which factors are moving with trust recovery levels.

At the significant level of $p < 0.001$, correlation analysis ($n = 185$) indicated that trust recovery was positively related to transparency (r=0.397) and visible security updates (r=0.398). This suggests that when a company remains transparent regarding the data breach and introduces visible security updates, the level of trust improves among consumers. These findings empirically support hypotheses that transparency H7 and security measures H8 enhance consumer trust recovery.

Conversely, trust recovery was found to be negatively related to cash culture (r=-0.382) and perceived risk (r=-0.321). The results imply that a strong cash preference will hinder trust recovery along with higher risk. If consumers prefer cash over digital payments and believe that the probability of cybercrime is high, then they will not trust FinTech products. These findings empirically support hypotheses regarding cash convenience H1 and higher perceived risk H2, which lowers the trust recovery process. The consumers who prefer cash are less likely to trust FinTech post cybercrime, and a higher perceived risk would lower the trust. (Refer to Appendix 2.)

In conclusion, correlation analysis showed that transparency and visible security updates are strong trust boosters, whereas cash preference and risk perception are trust dampeners. Higher transparency and strong security from the FinTech product will boost trust recovery and cash preference, and high risk regarding possible cybercrime will lower the trust recovery. A more in-depth analysis will require regression to understand which factors matter the most when considered together.

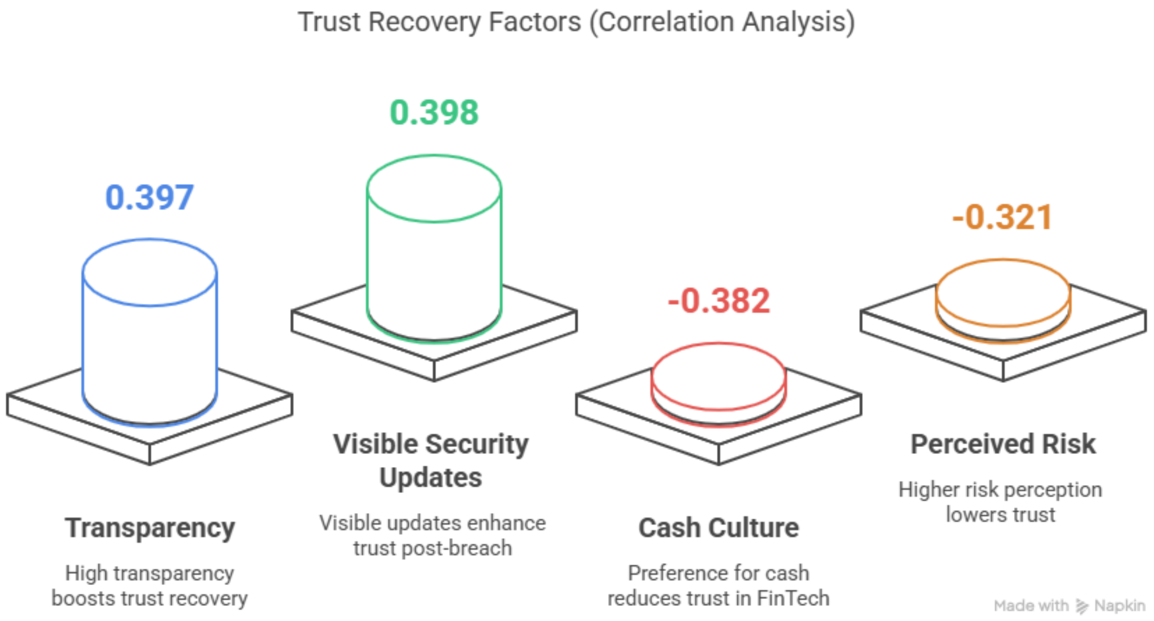


Figure. 14. Trust Recovery Factors (Correlation Analysis) (Prepared by Author)

Regression Analysis

A multiple regression model including all eight factors was run to determine which factors significantly impact trust recovery. The regression model was statistically significant ($R^2 = .345$, F(8, 176) = 11.59, $p < .001$), explaining 34.5% of the total variance in Perceived Trust. A model explaining 34.5% of the variance is substantial for a complex behavior such as trust.

The regression analysis highlighted three major factors that predict trust recovery post-data breach, i.e., cash preference, security, and transparency. The analysis explains that consumers who prefer cash are less likely to trust FinTech post data breach ($\beta = -.203$, $p = .003$). This finding validates our earlier results from correlation that consumers who prefer cash over FinTechs are less likely to trust FinTech post-data breach. This highlights a cultural barrier since consumers who consider cash as more convenient and safer, resort back to using it after becoming a victim of cybercrime.

Similarly, security was also found to be a significant predictor of trust recovery ($\beta = .210$, $p = .003$). This means that when consumers notice visible security updates in the FinTech product, they tend to trust its services. Improved security fosters the trust recovery process post-data breach.

One of the strongest predictors of trust recovery was transparency ($\beta = .273$, $p < .001$). Transparency has the highest beta value among all the factors, making it the most critical predictor of trust recovery among all the others. This implies the importance of open and honest communication by the FinTech companies. It is more critical in the times of cybercrimes. When a FinTech company promptly intimate its consumers about the causes of the data breach, and what steps they are taking to ensure it will not happen in the future, it helps rebuild trust among consumers.

Other variables, such as risk, regulations, and core factors from the Technology Acceptance Model (TAM), ease of use, and usefulness, remain conceptually relevant but failed to reach statistical significance during the analysis. It means that once the consumer trust is breached, ease of use and usefulness alone are insufficient to rebuild trust. Similarly, perceived risk remains important, but its effect is overshadowed when we analyse it with transparency, security, and cash preference. (Refer to Appendix 3.)

Factor Analysis

Factor analysis was conducted to analyse the underlying patterns among different trust-related constructs. It also helps to reduce any possible overlap among the factors. Principal Component Analysis with Varimax rotation was used for this purpose. The main idea was to reduce the number of variables into meaningful components.

Kaiser-Meyer-Olkin (KMO) value was found to be 0.733, which indicates that the data structure was suitable for identifying latent factors. Additionally, Bartlett's Test of Sphericity was also significant, confirming that the correlations between the variables were large enough to run factor analysis (χ^2 = 1166.122, df = 276, p < .001).

Factor analysis found 8 distinct factors based on eigenvalues. These factors explain 64% of the total variance. These factors represent intended independent variables. The scree plot shows an elbow after the 8th factor, which confirms that there are no additional major factors beyond this to explain the data's variance. The names of the factors are: (Refer to Appendix 4.)

- Factor 1 – Transparency
- Factor 2 – Cash Culture
- Factor 3 – Regulations
- Factor 4 – Perceived Risk
- Factor 5 – Cybersecurity Awareness
- Factor 6 – Perceived Usefulness
- Factor 7 – Ease of Use
- Factor 8 – Perceived Security

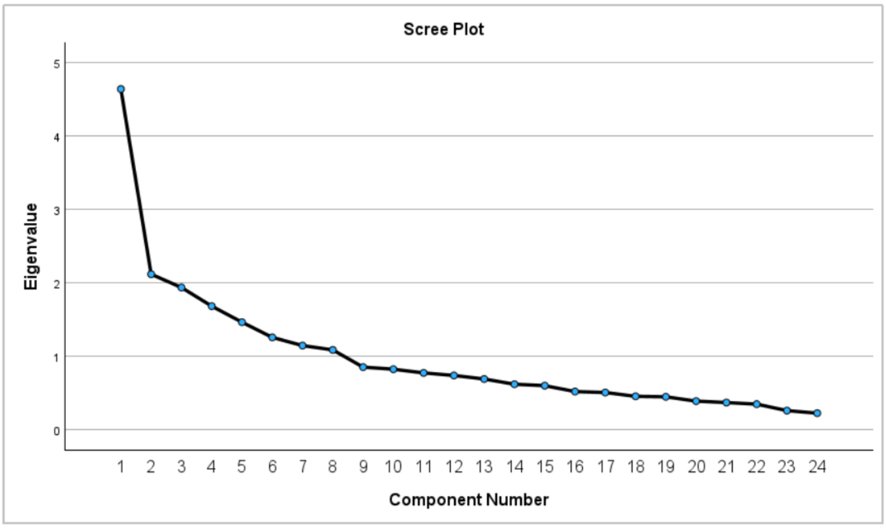


Figure. 15. Scree Plot showing component eigenvalues (Prepared by Author)

Regression Analysis using Extracted Factors

Multiple regression analysis was carried out using composite variables derived from factor analysis to minimize collinearity. The model explains 34.5% of the total variance in trust recovery ($R^2 = .345$). The model was found to be statistically significant (F(8, 176) = 11.594, p < .001). Variance Inflation Factors (VIF) were all below 1.3, therefore, no multicollinearity was found in the model, so each factor contributed independently.

The regression analysis found that transparency (β = .273, p < .001) and perceived security (β = .224, p = .003) had a statistically significant and positive impact on trust recovery. Conversely, cash (β = –.203, p = .003) had a statistically significant but negative impact on trust recovery. These findings reinforce our earlier analysis that, regardless of the statistical method used, the results are always the same. It provides additional assurance about the robustness of these results. (Refer to Appendix 5.)

Reduced Model Regression

To simplify the model and focus on only the strongest predictors, a reduced regression model was tested using only three factors, i.e, Transparency, Security, and Cash culture. The idea was to narrow down to three major predictors of trust recovery. The reduced model retained most of the explanatory power of the full model, 31.7%. All predictors remained statistically significant. Among these, Transparency was found to have the strongest positive effect on trust (β = 0.285). The second most crucial factor was visible security features (β = 0.262). Conversely, cash preference hurt trust recovery (β = -0.261). These findings show that even if we analyse focusing on only these three factors, we can still capture most of what influences trust recovery. It also highlights that FinTech firms should focus on these three factors to accelerate trust recovery post-data breach, and other factors such as perceived usefulness and ease of use wouldn't make any significant difference.

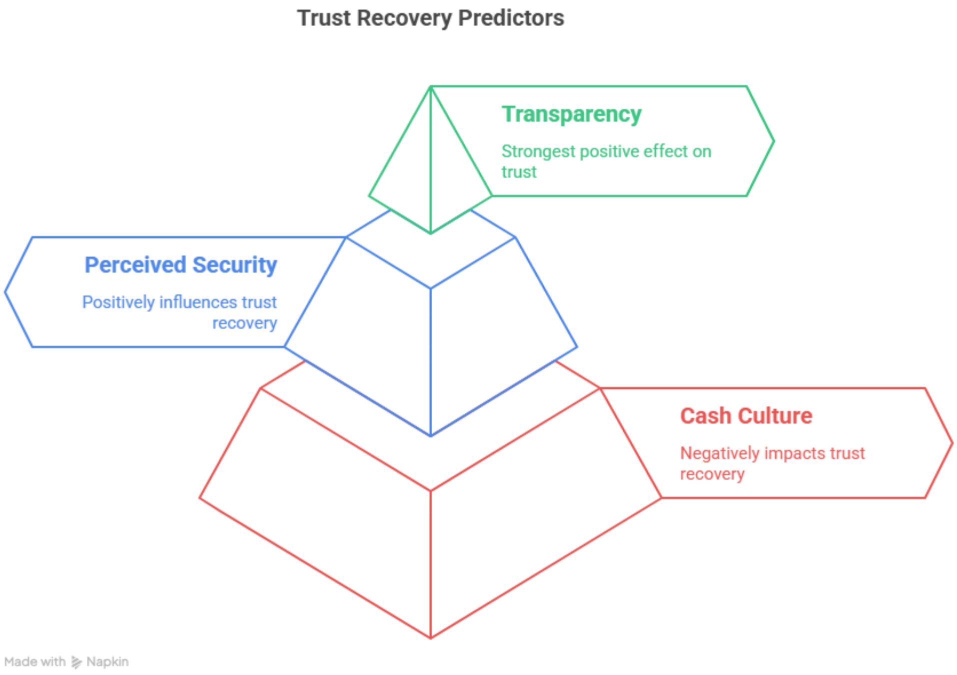

Trust Recovery Predictors
Transparency
Strongest positive effect on trust
Perceived Security
Positively influences trust recovery
Cash Culture
Negatively impacts trust recovery
Made with Napkin

Figure. 16. Top 3 Trust Recovery Predictors (Prepared by Author)

Organizational Recovery Actions

The research also applied statistical models to organizational recovery actions post-data breach. For example, offering compensation to the victims, public apology, staff training, consumer educational initiatives, etc. A regression analysis was conducted on this data.

The analysis revealed that all the organizational recovery action plans were statistically insignificant in predicting trust recovery post-data breach. Which means that none of these organizational actions can restore trust among consumers once it has been breached due to a cybercrime. Such results can be a result of a smaller sample size of the data. It is also possible that consumers want to see all or most of these actions together rather than individually.

The analysis showed that staff training had a statistically significant and net positive impact on trust recovery ($p < .05$). These results show that when staff are trained on how to prevent data breaches or enhance cybersecurity awareness, consumers tend to trust the firm more. It means that they are satisfied to some extent that a similar breach will not occur in the future since FinTech firm has taken appropriate actions.

The study also focused on understanding the top three trust-building and trust-diminishing factors among consumers. The data was analyzed separately using statistical techniques, but similar to the last results, none of the trust diminishers or builders proved to be statistically significant. However, a lack of customer support was found to have had some significant negative impact on trust recovery. The importance of customer support can be highlighted by the fact that the presence of 24/7 customer support in multiple languages was also found to be closer to statistical significance. So, we can say that the presence of a responsive customer support and the lack thereof were found to be important in both trust builders and diminishers. All the other factors were not significant individually; however, they can have a strong combined effect on trust recovery given their theoretical significance.

Summary of the empirical data analysis:

The multiple regression analysis was found to be statistically significant and explained 34.5% of the variance in perceived trust recovery ($R^2 = 0.345$). Three of the eight hypothesized predictors were found to have a statistically significant effect on trust recovery in the context of FinTech-related cybercrime: transparency, perceived security, and cash culture.

Transparency ($\beta =.273$, $p <.001$) was found to be the strongest positive predictor of trust recovery, confirming H7. This finding suggests that consumers are more likely to trust FinTech firms that openly disclose the causes of a data breach, provide timely updates, and clearly communicate future prevention measures.

Perceived security ($\beta =.224$, $p = 0.003$) was also found to be positively related to trust recovery and thus also supports H8. This is because consumers are more likely to trust a FinTech provider if they can observe improvements in security measures, for instance, two-factor authentication or biometric login, following a breach.

Cash culture ($\beta = -0.203$, $p = 0.003$) was found to be negatively related to trust recovery, thereby supporting H1. This shows that customers who prefer cash are even more opposed to digital platforms after a cybercrime, which hampers trust restoration.

The remaining hypotheses were not statistically supported by the regression model:

H2 (Perceived Risk): Not supported. Although there was a negative relationship between risk and trust, it did not achieve statistical significance in the presence of predictors like transparency and security.

H3 (Regulatory Challenges): Not supported. Weak or underdeveloped regulatory frameworks were not found to be a significant predictor of trust recovery.

H4 (Cybersecurity Awareness): Not supported. Although consumers were more aware post-breach, awareness alone did not make a significant contribution to the rebuilding of trust.

H5 (Perceived Usefulness): Not supported. The perceived utility of FinTech platforms, although still rated as positive, was not enough to predict trust recovery post-breach.

H6 (Ease of Use): Not supported. The simplicity of using FinTech platforms was not a significant factor when trust had already been broken.

In addition, separate regression models analysing organisational recovery actions revealed that customer support was the only factor with a significant effect on trust. It was found that reliable and responsive customer service is not only a top trust builder but also the greatest trust diminisher when absent. This reveals that Hypothesis H9 (organizational response quality), which was not part of the original TAM framework, turns out to be an important factor in trust recovery in practice.

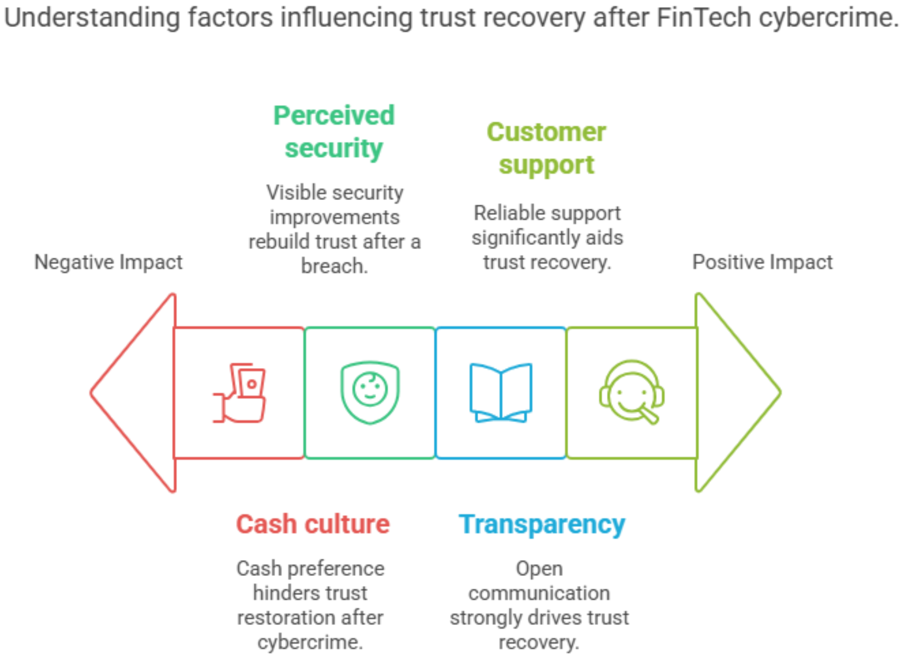

Understanding factors influencing trust recovery after FinTech cybercrime.
Perceived security
Visible security improvements rebuild trust after a breach.
Customer support
Reliable support significantly aids trust recovery.
Negative Impact
Positive Impact
Cash culture
Cash preference hinders trust restoration after cybercrime.
Transparency
Open communication strongly drives trust recovery.

Figure. 17. Factors Influencing Trust Recovery (Prepared by Author)

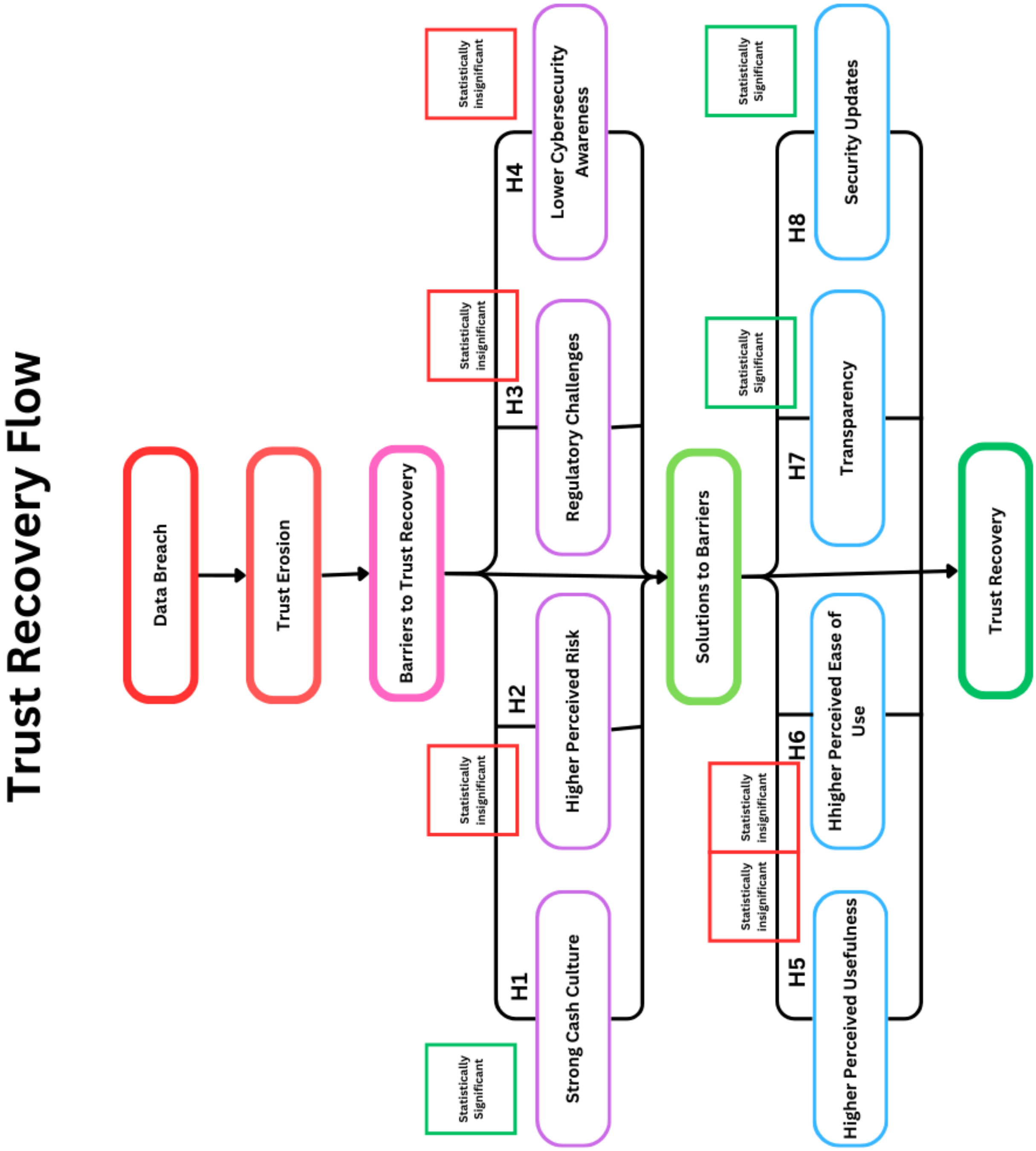

Trust Recovery Flow
Data Breach
Trust Erosion
Barriers to Trust Recovery
H1
Strong Cash Culture
Statistically Significant
H2
Higher Perceived Risk
Statistically insignificant
H3
Regulatory Challenges
Statistically insignificant
H4
Lower Cybersecurity Awareness
Statistically insignificant
Solutions to Barriers
H5
Higher Perceived Usefulness
Statistically insignificant
H6
Hhigher Perceived Ease of Use
Statistically insignificant
H7
Transparency
Statistically Significant
H8
Security Updates
Statistically Significant
Trust Recovery

Figure. 18. Trust Recovery Flow After Empirical Analysis (Prepared by Author)

4.1. Discussion

The research was conducted to identify barriers to trust recovery in FinTech post-data breach among consumers of the Pakistani FinTech market. An extended version of the Technology Acceptance Model (TAM) was used in this research, including perceived ease of use and usefulness being the core TAM elements, among cybersecurity awareness, regulatory framework, cash culture, perceived risk, perceived transparency, and trust recovery. As discussed above, these factors were adopted from already established theoretical models in the study of trust in FinTech. Extended TAM proved to be statistically significant in predicting trust recovery post-data breach. Three hypothesized elements were found to be statistically significant, and the rest were rejected. These three were transparency, perceived security, and cash culture.

The analysis showed that transparency is the strongest predictor of trust recovery among consumers of FinTech post-data breach. Consumers prefer to trust firms that have active communication channels with their customers and disclose the causes of the breach in a timely manner. It shows that the firm is not hiding the causes and taking responsibility. This act of integrity then helps consumers trust the firm more as compared to others. It improves their institutional credibility as well. The results of our analysis closely align with Dietz (2009), who proposed that transparency can positively affect the trustworthiness of an organization.

Transparency has dual benefits; it enhances the cognitive trust of the consumers, showing that the FinTech firm is competent enough to handle the difficult situation. It also improves the affective trust because the consumers feel valued and cared for. These results clearly show that factors that can enhance or establish initial trust are different from the post-data breach trust recovery factors. the consumers' focus shifts from the usability of the product to how secure and competent the firm is and how it treats the consumers. Therefore, the FinTech firms must remain transparent and forthcoming with the consumers. We have already discussed the importance of responsive customer support and the positive impact it has on trust recovery.

These results align closely with Dietz (2009), who stressed the importance of transparency, public apology, and firms taking responsibility for the data breach. However, Dietz study focused on organisational crisis, but in our context, we have refined it to focus on trust recovery among consumers of FinTech post-data breach. Our findings showed that transparency was indeed an important factor in trust recovery process.

The second most critical factor was perceived security. Perceived security measures the perception of how secure consumers perceive the FinTech product. Stronger security protocols support in trust recovery process. These results align with Pavlou (2003), who emphasized that perceived risk can only be mitigated by introducing visible security updates that can improve the perceived security. Roh (2024) also reported that perceived security and privacy are the two most important factors that can affect trust.

Mayer (1995) believes that trust is a function of the perceived likelihood of negative outcomes and the ability to mitigate those outcomes. Perceived security serves the same purpose by providing the ability to resist online threats and keep consumers safe. Our analysis also shows that post-data breach consumers become more conscious regarding their online security and protection. The visible security updates provide consumers with the peace that the FinTech firm is working to keep them protected. These security updates can include two-factor authentication or biometric login, etc (Beg, 2022).

However, it is important to note that security updates alone are not enough to restore consumer trust. The key term is that such security updates need to be visible to the consumers. It is important for consumers to visibly notice security updates post-data breach (Siddhant Mishra, 2024). A FinTech firm can develop a strong backend security, but unless it is properly communicated to the consumers, it might not have any significant impact on trust recovery. Once again, the importance of effective and useful communication is highlighted here.

Pavlou (2003) used TAM to study e-commerce adoption among consumers. His study identified perceived usefulness, ease of use, and security as the key factors of establishing trust. This research extends Pavlou's model by shifting the focus to trust recovery after a data breach. The results of our analysis also align with his study since perceived security was found to be a key indicator of trust in both studies. However, our research shows that perceived ease of use and usefulness, the key elements of TAM, lose their importance and significance in the post-data breach scenario. This implies the need to expand TAM constructs to analyse trust recovery in post-data breach.

The study shows that cash convenience was found to be negatively impacting the trust recovery process. These results align with the study of Kshetri (2018), who found cash to be a barrier to FinTech use. In our context, consumers who prefer cash tend to rely more on cash and prefer it rather than using FinTech products. Especially, post-data breach, when their trust has been breached, they feel like cash is more secure as compared to digital payments. It also implies that cultural elements emerge once trust has been breached. The analysis showed that consumers don't avoid FinTech products post-data breach, but still consider cash as more convenient. We know from the theoretical analysis that non-tangible forms of payments require a higher degree of trust from the consumers, which is then difficult to restore once damaged. Zafar Awan (2021) found that almost half of the consumers in Pakistan still prefer using cash over digital payments. His findings also align with the results of our statistical analysis.

The findings of this research support the social-cultural trust model, which suggests that trust is not the same everywhere (Ferrin, 2010). People from different backgrounds and cultures perceive trust differently. What one perceives from trust in one society or culture will be different from what someone from a different culture. Which means that trust is not a rational phenomenon, it's a deeply rooted one in the culture and background of the society it's being studied. Cash in Pakistani culture means control and safety; consumers have been using it for a long period and feel comfortable using it in the future as well. When consumers' trust is breached due to a data breach or some scam, their concerns and fear regarding intangible FinTech products turn into a reality, making trust recovery more complicated. We can concur that trust recovery is a technical matter, but some aspects require a deeper analysis of the cultural aspects of the society.

The analysis found that reliable customer support was the most important trust builder among all the organisational trust recovery actions. The data shows that an active and responsive customer support that can provide support in multiple languages was found to be a strong indicator of trust recovery. While analysing trust diminishers, the data shows that lack of reliable customer support was the leading trust diminisher among consumers post-data breach. All the other organisational actions failed to be statistically significant. However, it doesn't reduce their theoretical significance in the trust recovery process.

The analysis showed the lowest mean for the item if FinTech is still useful after the data breach. The highest mean score was for accepting the benefits of FinTech products. A majority of respondents also agreed that digital payments save them a lot of time. We can say that a data breach may have shaken the emotional trust among consumers, but the functional utility of FinTech products remained intact even post-data breach. This means that even if the trust is breached, the perceived usefulness remains intact, which provides FinTech an opportunity to retain consumers and work on trust recovery.

Regarding ease of use, 67% of consumers believe that digital transactions are simpler to use. Like usefulness, ease of use also remained intact post-data breach. Transparency remained a strong predictor of trust recovery in all other statistical analyses, but in descriptive analysis, the score was low. All three items under this construct showed neutral or low agreement. The analysis revealed a gap between the consumer's expectations and the firm's performance.

Consumers agreed with cash convenience on a larger scale, however, they remained nearly neutral on avoiding FinTech products post data breach. This highlights the cultural aspect of Pakistani society, where cash is translated into control and ease. Strong cash preference needs to be addressed by carrying out a qualitative analysis. On the positive end, the consumers are not avoiding FinTech post-data breach, which means the FinTech firms can still retain their consumers and work on trust recovery. It may include fraud insurance, guarantees, highlighting the risk of carrying cash, especially in big cities with a higher rate of street crimes.

Perceived trust recovery was also analysed on an item level. Consumers showed that they would recommend FinTech to others even after suffering a data breach. However, consumers don't trust their service providers, they can help them solve their issues in case of a data breach. This shows that whilst consumers still understand the functional utility of FinTech products on a rational basis, their trust on an emotional level is more damaged and requires more effort.

Our analysis showed that perceived security was a predictor of trust recovery in the regression model. However, a closer look at the construct reveals even more details. All three items in the construct scored positively during the analysis. The most crucial driver of trust recovery was the question if consumers noticed visible security improvements post-data breach. This confirms our analysis of the need for visible security updates in trust recovery. This is important for cognitive trust. The second important item was about the importance of two-way authentication. These results confirm our analysis that trust recovery is based on visible security updates, much like two-way authentication, security alerts, etc. They serve a dual purpose by not only providing security but also a sense of protection for the consumers as well.

5. Conclusions and Recommendations

Based on this research's findings, we can make recommendations for FinTech companies and policymakers.

Recommendations for FinTech Companies

The study revealed that transparency and active communication are critical predictors of trust recovery among consumers of FinTech post-data breach. It is highly recommended that FinTech establish active communication channels with consumers and design crisis management protocols. This enables the staff to know exactly what to do in the event of a data breach or a cyberattack. These protocols should also discuss the procedure to disclose the reasons for data breaches to the consumers. Our analysis shows that such communications should be timely to have any impact on consumers' trust. FinTech companies should also utilize these communications channels and educate consumers on what steps should be taken to avoid such incidents in the future. As discussed before, FinTech should also communicate the progress that has been made to improve the product's security. These visible security updates will then improve trust recovery among consumers.

Dietz's (2009) in his study discussed the impact of public apology and active communication. Our recommendations are based on the analysis, aligning with Dietz's study. However, the data doesn't show that consumers were interested in a public apology from the firm's CEO, and it was to be statistically significant. Therefore, the firm should focus on establishing responsive 24/7 customer support, promoting active communication, and being transparent with the consumers regarding the cyberattack.

Customer support, as discussed above, is a very important factor in both restoring trust and its absence hinders trust recovery. FinTech companies should train their customer support staff to handle difficult situations, especially where consumers are afraid and stressed about their loss. The staff should be trained to handle data breach queries in an "empathetic and rational manner".

In a post-data breach scenario, prompt, helpful, and resourceful customer support can turn a bad consumer experience into a pleasant one. These actions touch both the cognitive and affective trust. The resourcefulness and prompt response make consumers feel that the firm is competent enough to handle the situation. It also shows that the firm is giving proper response, importance, and respect to the consumer. Chatbots and AI agents can be used for general questions, but live agents are very important so that consumers can explain their problem and be heard. Similarly, follow-up calls can also leave a good impression on the consumers.

The analysis shows that perceived security improves trust recovery among consumers post-data breach. However, it was also noted that security improvements need to be visible. For example, post-data breach, if the FinTech firm decides to introduce two-factor authentication for login, then they should properly communicate this feature to the consumers. It is also the FinTech firm's responsibility to adequately educate consumers about the security features, so they should know how to activate these in their accounts. These suggestions are closely aligned with Pavlou (2003) and Roh (2024), who suggests that perceived risk can be mitigated by improving perceived security and stresses the importance of privacy and security for trust.

During research, we asked consumers regarding fear-motivated messages, and the analysis found that they were statistically not significant. It doesn't mean that the firm should not warn its consumers regarding the prevailing online threats and frauds. It is imperative to note that consumers should be kept informed regarding the techniques, especially social engineering, so that they can stay vigilant. These actions will keep consumers safe in case they face a similar scenario. It will also communicate that the firm is ahead of the ongoing frauds, scams, and data breach techniques.

While discussing the barriers to trust recovery, cash culture was found to have a sizeable impact on the Pakistani consumers. FinTech firms need to first acknowledge that cash is considered a symbol of safety, conformity, and convenience in the market. Acknowledging this behavior will enable FinTech firms to then devise strategies to counter this narrative. One possible way is to offer fraud protection guarantees or insurance, up to a specific amount, that can serve as proof of security that will mimic the sense of control consumers feel in having cash. Consumers can opt for this insurance and ensure that in case of any data breach or unauthorized transactions, they will not lose all their money. Similarly, some banks in Pakistan have a maximum online transaction limit on accounts, so in case of data breach or unauthorized access to accounts, the damage can be curtailed. These actions can reassure them that their money is safe in their accounts.

FinTech firms can run educational campaigns to educate consumers to understand how safe their money is in their digital accounts as compared to cash. Especially in Karachi, which is the biggest city in Pakistan by population, the street crimes reported in 2024 were around 18,213 (Khan F.). These statistics can be used in campaigns, and over time, consumers will see consistent performance and understand that protection is in place using digital payment methods. This transition will take time, but slowly, consumers will start to embrace FinTech products.

Most of the FinTech firms, such as NayaPay, EasyPaisa, SadaPay, etc, all market their products as being "easy to use," and highlight their "usefulness" to the consumers. However, our research shows that post-data breach, consumers shift their focus from utility to safety. Therefore, if the firm continues to focus on the utility aspect of its products, it will not be able to recover trust among the consumers. For example, if pre-data breach the firm was marketing with the slogan that "how easy it is to pay your utility bills", post-data breach, this marketing should shift to focusing on "look how secure your transactions are with us." It simply means that post-data breach, consumers apply a different evaluation criterion to trust FinTech products than they did during initial adoption.

Recommendation for Policymakers

This study found that trust recovery isn't merely a rational process, but it's deeply rooted in the culture as well. Much like FinTech firms, the policymakers should also keep in mind the cultural aspects of the market, such as cash preference. Once policymakers acknowledge this behavior, they can introduce initiatives that can gradually guide consumers towards opting for digital payments. For example, policymakers can give incentives to pay taxes and other governmental duties via digital payment systems. The incentives will act as a motivating factor for the consumers, and payments made to governments can add a sense of security. The policy should speak to people's comfort zones.

These strategies can shift the focus of consumers from cash reliance to digital payments. Policymakers can use the help of social media influencers to spread the idea of using FinTech products, and steer it as a patriotic activity, since virtual payments can significantly reduce the operational cost for the government.

Along with these, the policymakers should focus on introducing mandatory data breach insurance for FinTech companies, offering tax incentives for investments in improving cybersecurity. By doing so, FinTech firms will be incentivized to enhance their cybersecurity beyond minimum requirements. It will decrease the perceived risk among consumers and foster trust. Policymakers can also make it mandatory for FinTech firms to have customer support teams to specifically handle data breach queries. FinTech firms can also set up a centralized warning system where consumers are timely updated regarding data breaches and other cybercrimes. This early warning mechanism will make consumers feel well informed. All of these actions collectively can help restore trust among consumers.

The purpose of the above-mentioned recommendations is to turn the findings of this research into actionable strategies. FinTech firms can focus on designing their post-data breach protocols, improving their overall transparency, and having open channels with consumers. Whereas policymakers can provide a sustainable FinTech ecosystem to the firms and make it mandatory to have insurance, and teams that can handle data breaches with sensitivity and rationality. Both FinTech firms and policymakers should acknowledge the cultural aspect of trust recovery and avoid using one solution fit for all formula.

References

1. Abbasi, K. A. (2021). FinTech , SME efficiency & national culture: evidence from OECD countries. *Technological Forecasting and Social Change, 163*, 1-9. doi:10.1016/j.techfore.2020.120454.
2. Abbasi, S. (2022, October 12). SIM swap fraud: How scammers are stealing millions from bank accounts. Karachi, Sindh, Pakistan. From https://www.dawn.com/news/1764628
3. Abbasi, S. (2023, July 16). Pakistan's Web of Cyber Scammers. *DAWN.COM*. Karachi, Sindh, Pakistan. From https://www.dawn.com/news/1764628
4. Abbass, K. B. (2022). Fresh insight through a Keynesian theory approach to investigate the economic impact of the COVID-19 pandemic in Pakistan. *Sustainability, 14*(3), 1054.
5. Abidin, M. A. (2019). Customer data security and theft: A Malaysian organization's experience. *Information and Computer Security, 27*(1), 81-100. doi:https://doi.org/10.1108/ICS-04-2018-0043
6. Ahmad Fraz, A. U. (2021). FinTech in Pakistan. *Policy and research, 2*(8).
7. Ahmad, I. I. (2021). A systematic literature review of e-banking frauds: current scenario and security techniques. *Linguistica Antverpiensia*.
8. Ahmed Shuhaiber, K. S.-O. (2023, October 13). Investigating trust and perceived value in cryptocurrencies: do optimism, FinTech literacy, and perceived financial and security risk matter? *Kybernetes*, na. doi:https://doi.org/10.1108/K-03-2023-0435
9. Alalwan, A. A. (2018). Consumer adoption of mobile banking in Saudi Arabia: An empiricial analysis. *International Journal of bank Marketing, 36*(3), 545-566.
10. Ali M, R. S. (2021). How perceived risk, benefit and trust determine user Fintech adoption: a new dimension for Islamic finance. *Foresight, 23*, 403-420. doi:DOI 10.1108/FS-09-2020-0095
11. Arli, D. v. (2020). "Do consumers really trust?". *Marketing Intelligence and Planning,, 39*(1), 74-90.
12. Arshad, R. (2023, November 5). Phone scams to data leaks securing Pakistan s digital frontier. Lahore, Punjab, Pakistan: The Express Tribune. From https://tribune.com.pk/story/2444854/phone-scams-to-data-leaks-securing-pakistans-digital-frontier
13. Avgerou, C. &. (2013). Information systems in developing countries: A critical research review. *Journal of Information Techonology, 28*(4), 556-582. doi:https://doi.org/10.1057/jit.2013.28
14. Awad, N. a. (2008). Establishing trust in electronic commerce through online word of mouth: an examination across genders. *Journal of Management Information Systems, 24*(4), 101-121.
15. Ayllón, S. B.-K. (2020). ICT usage across Europe. A literature review and an overview of existing data. *(Digi- Gen - working paper series No. 2).*
16. Ayman Mansour Khalaf Alkhazaleh, H. H. (2021). How does the Fintech services delivery affect customer satisfaction: A scenario of Jordanian banking sector. *Strategic Change, 30*, 405-413. doi:DOI: 10.1002/jsc.2434
17. Ayse Demir, V. P.-C. (2022). Fintech, financial inclusion and income inequality: a quantile regression approach. *The European Journal of Finance, 28*(1), 86-107. doi:10.1080/1351847X.2020.1772335
18. aysonline. (n.d.). From aysonline.pk: https://www.aysonline.pk/qisstpay-pakistan/
19. Baber, H. (2020). FinTech, Crowdfunding & Customer Retention in Islamic Banks. *Vision: The Journal of Busniess Perspective, 24*(3), 260-268. doi:https://doi.org/10.1177/0972262919869765

20. Ballaji, N. (2024). Consumers Protection in the era of Digitial Payments: Legal challenges and solutions. *Beijing Law Review*, 1268-1290. doi:https://doi.org/10.4236/blr.2024.153076

21. Banking Mohtasib Pakistan. (2023). *Annual Report 2023.* Islamabad: Banking Mohtasib Pakistan. From https://www.bankingmohtasib.gov.pk/Documents/Annual_Report_2023.pdf

22. BCG and QED. (2024, June). *Global FinTech 2024: Prudence, Profits, and Growth.* Boston: Boston Consulting Group & QED. From https://www.bcg.com/publications/2024/global-fintech-prudence-profits-and-growth

23. Beg, S. S. (2022). Data usage-based privacy and security issues in mobile app recommendation (MAR). *A systematic literature review*, 725-49.

24. Bhatti, E. (2018, October 29). BankIslami becomes victim of $6.5 million cyber-attack. Lahore, Punjab, Pakistan: Profit by Pakistan Today. From https://profit.pakistantoday.com.pk/2018/10/29/bankislami-becomes-victim-of-6-5-million-cyber-attack/

25. Boehm, J. G. (2022). *Why digital trust truly matters.* NA: McKinsey & Company. From https://www.mckinsey.com/capabilities/quantumblack/our-insights/why-digital-trust-truly-matters

26. Bongomin, G. O. (2020). Trust: Mediator between mobile money adoption and usage and financial inclusion. *Social Responsibility Journal, 16*(8), 1215-1237. doi:10.1108/SRJ-01-2019-0011

27. Brenner, L. M. (2020). Consumer fraud victimization and financial well-being. *Journal of Economic Psychology, 76*, 102243.

28. Bryan Zheng Zhang, A. A. (2021). Do FinTech and financial incumbents have different experiences and perspectives on the adoption of artificial intelligence? *Strategic Change, 30*(3), 223-234. doi:https://doi.org/10.1002/jsc.2405

29. Buckley, R. a. (2016). FinTech in developing countries: charting new customer journeys. *Journal of Financial Transformation, 44*, 1-19.

30. C., C. (2018). Expectations vs reality: responding to online fraud across the fraud justice network. *International Journal of Law, Crime and Justice, 55*, 39.

31. Chakraborty, D. S. (2022). Mobile payment apps filling value gaps: integrating consumption values with initial trust and customer invovlement. *Journal of Retailing and Consumer Services, 66*, 1-16. doi:10.1016/j.jretconser.2022.102946.

32. Chang, H. a. (2010). Adoption of e-procurement and participation of e-marketplace on firm performance: trust as a moderator. *Information and Management, 47*(5-6), 262-270. doi:10.1016/j.im.2010.05.002

33. Cheng TCE, L. D. (2006). Adoption of internet banking: an empirical study in Hong Kong. *Decis Support syst*, 1558-72.

34. Chervany, D. H. (2001). Trust and Distrust Definations: One Bite at a Time. *Trust in Cyber-societies: Integrating the Human and Artificial Perspectives*, 27-54. doi:10.1007/3-540-45547-7_3

35. Cisco. (2025, March 21). *The future of ransomware: Inside Cisco Talos threat hunters*. From cisco.com: https://www.cisco.com/site/us/en/learn/topics/security/what-is-phishing.html

36. Cook, S. G. (2023). Fear of economic cybercrime across Europe: a multilevel application of routine activity theory. *The British Journal of Criminology, 63*(2), 384-406.

37. creditbook. (n.d.). *About us*. From creditbook.pk: https://www.creditbook.pk/about

38. Creswell, J. W. (2014). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. Thousand Oaks,: Sage Publications.

39. Cross, C. a. (2022). Exploring fear of crime for those targeted by romance fraud. *Victims and Offenders, 17*(5), 735-755. doi:doi: 10.1080/15564886.2021.2018080

40. Davis, F. B. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management Science, 35*(8), 982-1003.

41. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 319-340.

42. DAWN. (2022, September 23). Fintech fraud is not really uncommon. Khairpur Mirs, Sindh, Pakistan. From https://www.dawn.com/news/1711578

43. DAWN. (2023, January 22). Amid rising fraud, telecom watchdog lays out cyber risks. Islamabad, Punjab, Pakistan. From https://www.dawn.com/news/1732919/amid-rising-fraud-telecom-watchdog-lays-out-cyber-risks

44. DeLone, W. H. (1992). Information system success: The quest for the dependent variable. *Information system research, 3*(1), 60-95.

45. Dhagarra D, G. M. (2020). Impact of Trust and Privacy Concerns on Technology Acceptance in Healthcare: An Indian Perspective. *Int J Med Inform*. doi:doi: 10.1016/j.ijmedinf.2020.104164

46. Dietz, N. G. (2009). Trust repair after an organization level failure. *Academy of Management Review*, 127-145. doi:DOI: 10.5465/AMR.2009.35713319

47. Douglas Arner, J. B. (2015). The evolution of FinTech: A new post-crisis paradigm? *University of Hong Kong Faculty of Law Research Paper no. 2015/047*. doi:http://dx.doi.org/10.2139/ssrn.2676553

48. Egi Arvian Firmansyah, M. M. (2023). Factors Affecting Fintech Adoption: A Systematic Literature Review. *FinTech, 2*, 21-33. doi:https://doi.org/10.3390/fintech2010002

49. Erum Irfan, Y. A. (2022). Analysing role of businesses' investment in digital literacy: A case of Pakistan. *Technological Forecasting and Social Change, 176*, 121484. doi:doi.org/10.1016/j.techfore.2022.121484

50. Eurostat. (2024, Feburary 22). Digital skills in 2023: impact of education and age. From https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20240222-1

51. Ferrin, D. a. (2010). Trust Differences Across National-Societal Cultures: Much to Do, or Much Ado about Nothing? From https://ink.library.smu.edu.sg/lkcsb_research/3142

52. Financial Stability Board. (2017). *Financial Stability Implications from FinTech: Supervisory & Regulatory issues that Merit Authorities' Attention.* Financial Stability Board.

53. Financial Stability Board. (n.d.). Financial Innovation. From https://www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/financial-innovation/

54. Finja. (2023, October 2). *Finja Sells Its Payments License to Opay and Doubles Down on Its Lending Business!* From finja.pk: https://finja.pk/pressDetail/24

55. FinTech Magazine Article. (2025). 4 Common cyber security challenges for fintechs. From https://www.fintechweekly.com/magazine/articles/4-common-cyber-security-challenges-for-fintechs

56. Firmansyah, E. M. (2024). Innovation in finance: a bibliometric and content-analysis study. *Nankai Business Review International,, 15*(4), 578-594. doi:https://doi.org/10.1108/NBRI-08-2023-0071

57. Fishbein, M. &. (1975). Belief, attitude, intention, and behaviour: An introduction to theory and research. *Addison-wesley*.

58. Gupta, A. a. (2022). Long-term changes in consumers' shopping behavior post pandemic: an exploratory study. *International Journal of Retail & Distribution Management, 50*(12), 1518-1534. doi:doi: 10.1108/IJRDM-04-2022-0111

59. Haritha, P. (2022). Mobile payment services adoption: understanding customers for an application of emerging financial technology. *Information and Computer Security, 31*(2), 145-171.

60. Hayat, S. R. (2021). Understanding the usability issues in contact management of illiterate and semi-literate users. *PloS One, 16*(12), e0259719. doi:https://doi.org/10.1371/journal.pone.0259719

61. Hentzen, J. H. (2022). Artificial intelligence in customer-facing financial services: a systematic literature review and agenda for future research. *International Journal of Bank Marketing, 40*(6), 1299-1336. doi:https://doi.org/10.1108/IJBM-09-2021-0417

62. Hosam Elsaman, R. D. (2024). Navigating fintech innovation: Performance, trust, and risk factors in UAE's Banking sector. *Journal of Eastern European and Central Asian Research, 11*(2), 332-341. doi:DOI: https://doi.org/10.15549/jeecar.v11i2.1569

63. Huang, S. a. (2022). Prediciting continuance intention to fintech chatbot. *Computers in Human Behavior, 129*, 1-8. doi:doi: 10.1016/j.chb.2021.107027

64. Jaspers, E. &. (2022). Consumers' acceptance of domestic Internet-of-Things: the role of trust & privacy concerns. *Journal of Business Research*, 255-265. doi:10.1016/j.jbusres.2021.12.043

65. JazzCash. (n.d.). *Introducing BookMe in your JazzCash App*. From jazzcash.com.pk: https://www.jazzcash.com.pk/bookme-cashback-campaign/

66. Jeyaraj, A. R. (2006). A review of the predictors, linkages and biases in IT innovation adoption research. *Journal of Information Technology, 21*(1), 1-23.

67. Jia Qi, S. C. (2024). Using an extended post-acceptance framework to examine consumer adoption of fintech. *International Journal of Bank Marketing, 42*(3), 642-668. doi:DOI 10.1108/IJBM-10-2022-0448

68. Joubert, J. a.-P. (2013). The role of trust and risk in mobile commerce adoption within South Africa. *International Journal of Business, Humanities and Technology, 3*(2), 27-38.

69. Jurjens, H. S. (2018). Data security and consumer trust in FinTech innovation in Germany. *Information and Computer Security, 26*(1), 109-128. doi:10.1108/ICS-06-2017-0039

70. K. Gupta, A. W. (2023). Determinants of continuous intention to use FinTech services: the moderating role of COVID-19. *Journal of Financial Services Marketing*, 1-17.

71. Karjaluoto, H. M. (2015). Factors underlying attitude formation towards mobile banking services. *Journal of Marketing Communications, 21*(2), 117-133.

72. Khan, F. (n.d.). Karachi saw over 72,000 street crime incidents in 2024. karachi, Sindh, Pakistan. From https://www.thenews.com.pk/print/1267450-karachi-saw-over-72-000-street-crime-incidents-in-2024

73. Khan, S. &. (2022). In-depth analysis of blockchain, cyrptocurrency and sharia compliance. *Internatioanl Journal of Business Innovation and Research, 29*(1), 1-15.

74. Kim, Y. W. (2021). Do information and service quality affect perceived privacy protection, satisfaction and loyalty? Evidence from a Chinese 020-based mobile shopping application. *Telematics and Informatics, 56*, 101483.

75. KPMG. (2023). *Global fintech investment drops to five-year low in 2023*. From KPMG: https://kpmg.com/xx/en/our-insights/value-creation/pulse-of-fintech-h2-2023-global-insights.html

76. Krishna, B. K. (2023). Understanding the process of building institutional trust among digital payment users through national cybersecurity commitment trustworthiness cues: a critical realist perspective. *Information Technology & People*. doi:10.1108/ITP-05-2023-0434

77. Kshetri, N. &. (2018). Factors affecting adoption of mobile money by micro and small enterprises (MSEs). *Journal of Business Research, 86*, 272-280.

78. Kumar, D. P. (2023). Filling the SME credit gap: a systematic review of blockchain-based SME finance literature. *Journal of Trade Science, 11*(2/3), 45-72. doi:https://doi.org/10.1108/JTS-06-2023-0003

79. Laura Salciuviene, V. A. (2014). Key Drivers Affecting Customer Intention to Purchase Financial Services Online. *Eingeering Economics, 25*(2), 194-202. doi:10.5755/j01.ee.25.2.6427

80. Lee, M.-C. (2009). Factors influencing the adoption of internet banking: an integration of TAM and TPB with perceived risk and percieved benefit. *Electronic Commerce Research and Application*, 130-141.

81. Leong, C. T. (2017). Nurturing a FinTech ecosystem: the case. *Int. J. Inf. Manag, 37*(2), 92-97. doi:http://dx.doi.org/10.1016/j.ijinfomgt.2016.11.006

82. Leukfeldt, E. a. (2020). Cybercrimes on the streets of The Netherlands? An exploration of the intersection of cybercrimes and street crimes cybercrimes on the streets.... *Deviant Behavior,, 42*(11), 1-12. doi:doi: 10.1080/01639625.2020.1755587

83. Lewicki, R. &. (1996). Developing and maintaining trust in work relationships. *Trust in organizations: Frontiers of theory and research* (pp. 114-139). Thousands Oaks, CA: Sage.

84. Lewis, J. D. (1985). Trust as a Social Reality. *Social Forces, 63*(4), 967-985. doi:https://doi.org/10.2307/2578601

85. Lian, J. a. (2021). The dimension of trust: an investigation of mobile payment services in Taiwan. *Technology in Society, 67*, 1-14. doi:10.1016/j.techsoc.2021.101753

86. Liu, Z. B. (2019). Factors affecting consumers mobile payment behavior: a meta analysis. *Electronic Commerce Research, 19*, 575-601.

87. Mamta Kumari, P. C. (2014). The impact of data breach on consumer trust in e-commerece. *IJCSPUB, 4*(4).

88. Mark A Chen, Q. W. (2019). How Valuable Is FinTech Innovation? *The Review of Financial Studies, 32*(5), 2062-2106. doi:https://doi.org/10.1093/rfs/hhy130

89. Market Data Forecast. (2022). *Global Fintech Market Research Report.* Hyderabad: Market Data Forecast. From https://www.marketdataforecast.com/market-reports/fintech-market

90. Mazer, R. &. (2022). *Consumer protection in digital finance: Innovations to address emerging risks.* Centre for Financial Regulation and Inclusion (CENFRI). From https://cenfri.org/wp-content/uploads/Consumer-Protection-in-Digital-Finance_August-2022.pdf

91. McKinsey & Company. (2022, May 31). *What's fueling Pakistan's emerging start-up ecosystem*. From McKinsey & Company: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/whats-fueling-pakistans-emerging-start-up-ecosystem

92. Medhi, D. D. (2021). Adoption of fintech by SMEs in India: A theoretical framework. *International Journal of Business and Globalisation, 26*(2), 228-245.

93. Meena Akileswaran, D. S. (2024). Cyber security and its importance with special reference to FinTech companies in Chennai. *Educational Administration: Theory and Practice, 30*(4), 9262-9265. doi:Doi: 10.53555/kuey.v30i4.3476

94. Melnyk, V. (2024). Transforming the nature of trust between banks and young clients: from traditional to digital banking. *Qualitative Research in Financial Markets, 16*(4), 618-635. doi:https://doi.org/10.1108/QRFM-08-2022-0129

95. Memon, S. M. (2015). Prospects and challenges for social media in Pakistan. *International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), London, UK*, 1-5. doi:https://doi.org/10.1109/CyberSA.2015.7166124

96. Mertzanis, J. P. (2024). The adoption of digital payments in emerging economies: challenges and policy response. *Digital Policy, Regulation & Governance, 26*(5), 476-500. doi:10.1108/DPRG-06-2023-0077

97. Milian, E. S. (2019). FinTechs: a literature review and research agenda. *Electronic Commerce Research and Applications, 34*, 100833.

98. Nicoletti, B. (2017). *The Future of FinTech – Integrating Finance and Technology in Financial Services.* Rome: Palgrave Macmillan.

99. Ouma, S. A. (2018). Mobile money and financial inclusion in Kenya: The role of accessibility and financial literacy. *International Journal of Business and Emerging Markets, 10*(2), 157-175.

100. Pakistan Telecommunication Authority. (2021, April 18). PTA Cautions public of fraud calls and SMS. Islamabad, Islamabad, Pakistan. From https://www.pta.gov.pk/category/pta-cautions-public-of-fraud-calls-sms-845777240-2023-06-01

101. Pakistan Telecommunication Authority. (2022). *Advisory on social engineering attacks.* Islamabad: National Telecom Computer Emergency Response Team (NTCERT). From https://ntcert.pta.gov.pk/2022/Advisories/pdf/157.pdf

102. Pal, A. H. (2021). Why do people use mobile payment technologies and why would they continue? An examination and implication from India. *Research Policy, 50*(6), 104-228.

103. Patil, P. T. (2020). Understanding consumer adoption of mobile payment in India: extending meta-UTAUT model with personal innovativeness, anxiety, trust, and grievance redressal. *International Journal of Information Management, 54*, 102-144.

104. Patria Laksamana, &. S. (2023). Determining factors of continuance intention in mobile payment: fintech industry perspective. *Asia Pacific Journal of Marketing and Logistics, 35*(7), 1355-5855. doi:DOI 10.1108/APJML-11-2021-0851

105. Pavlou, P. (2003). Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce, 7*(3), 101-134.

106. Payoneer. (n.d.). *About*. From payoneer.com: https://www.payoneer.com/about/

107. Punyatoya, P. (2019). Effects of cognitive and affective trust on online customer behavior. *Marketing Intelligence and Planning, 37*(1), 80-96. doi:10.1108/MIP-02-2018-0058

108. R. Sabillon, V. C.-R. (2016). Cybercriminals, cyberattacks and cybercrime. *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF), Vancouver, BC, Canada* (pp. 1-9). Vancouver,: IEEE. doi:doi: 10.1109/ICCCF.2016.7740434

109. Rahman, S. N.-V. (2024). Promoting fintech: driving developing country consumers' mobile wallet use through gamification and trust. *International Journal of Bank Marketing, 42*(5), 841-869. doi:https://doi.org/10.1108/IJBM-01-2023-0033

110. Razmetaeva, Y. P.-S. (2021). Jurisdictional Issues in the Digital Age. *Law Journal, 10*, 167-183.

111. Remitly. (2023). *11 Popular mobile wallets from around the world.* Retrieved 12 25, 2024 from Remitly.com: https://blog.remitly.com/finance/popular-mobile-wallets-around-world/

112. Richins, M. L. (1983). Negative word-of-mouth by dissatisfied consumers: A pilot study. *Journal of Marketing, 47*(1), 68-78. doi: https://doi.org/10.2307/3203428

113. Roger C. Mayer, J. H. (1995). AN INTEGRATIVE MODEL OF ORGANIZATIONAL TRUST. *Academy of Management Review, 20*(3), 709-734.

114. Roh T, Y. Y. (2024). What makes consumers trust and adopt fintech? An empirical investigation in China. *Electronic Commerce Research, 24*(3), 3-35. doi:10.1007/s10660-021-09527-3

115. Ruhland, P. a. (2023). FinTechs and the financial industry: partnerships for success. *Journal of Business Strategy, 44*(4), 228-237. doi:https://doi.org/10.1108/JBS-12-2021-0196

116. Saeed, T. (2018, August 7). *Cashless payments estimated to save Rs182 billion a year for Karachi: Visa*. From The News: https://www.thenews.com.pk/print/351548-cashless-payments-estimated-to-save-rs182-billion-a-year-for-karachi-visa.

117. Sania Zafar Awan, S. R. (2021). Conducting the cashless revolution in Pakistan using enterprise integration. *International Journal of Education and Management Engineering*. doi:DOI: 10.5815/ijeme.2021.04.02

118. Securities and Exchange Commission of Pakistan. (2023). *Digital lending apps being run and administered by duly licensed lending NBFCs.* From Securities Exchange Commission of Pakistan: https://www.secp.gov.pk/document/digital-lending-apps-being-run-and-administered-by-duly-licensed-lending-nbfcs/?wpdmdl=46367&refresh=67c9e9948df381741285780

119. Segal, E. (2022, Jun 21). *Customer dont trust businesses as much as executives think they should, PwC study finds*. From Forbes: https://www.forbes.com/sites/edwardsegal/2022/06/21/new-survey-shows-a-big-gap-in-trust-between-companies-and-consumers/?sh=7e2758e96811

120. Setiawan, K. S. (2024). Determinants of FinTech adoption: Evidence from SMEs in Indonesia. *LBS Journal of Management and Research, 22*(1), 55-65. doi:DOI 10.1108/LBSJMR-11-2022-0076

121. Shahzad, M. (2023). Emerging Cyber Crimes in Pakistan: A Case Study of Online Fraud through Digital Microloan Apps. *Global Digital & Print Media Review, 6*(2), 411-421. doi:https://doi.org/10.31703/gdpmr.2023(VI-II).30

122. Sharif, O. (2025, January 24). *Cash is King: The Case of Pakistan in a Fintech Revolution*. From The Express Tribune: https://tribune.com.pk/story/2524269/cash-is-king-the-case-of-pakistan-in-a-fintech-revolution

123. Shin, I. L. (2018). Fintech: Ecosystem, business models, investment decisions, and challenges. *Business Horizons, 61*(1), 35-46. doi:https://doi.org/10.1016/j.bushor.2017.09.003

124. Siau, K. S. (2003). Development of a framework for trust in mobile commerce. *Proceedings of the Second Annual Workshop on HCI Research in MIS*, (pp. 85-89). Washington, Seattle.

125. Siddhant Mishra, M. G. (2024). Investigate how data breaches affect consumer trust in companies and their willingness to share personal information. *International Journal of Creative Research Thoughts, 12*(7), 867-883.

126. Singh, S., Sahni, M. M., & Kovid, R. K. (2021). Exploring trust and responsiveness as antecedents for intention to use FinTech services. *International Journal of Economics and Business Research, 21*(2), 254-268. doi:10.1504/IJEBR.2021.113152

127. Šmahel, D. M. (2020). EU Kids online 2020: survey results from 19 countries. From https://www.eukidsonline.ch/files/Eu-kids-online-2020-international-report.pdf

128. Sohail, I. B. (2024). *The Regulatory Landscape for Fintech in Pakistan.* Islamabad Policy Research Institute (IPRI).

129. State Bank of Pakistan. (2023). *List of electronic money institutions (EMIs).* From Statebank of Pakistan: https://www.sbp.org.pk/ps/PDF/List-of-EMIs.pdf

130. Stewart, H. a. (2018). Fintech and trust: A qualitative study of customers' attitudes towards fintech and their data protection concerns. *Journal of Financial Services Marketing*, 225-237. doi:10.1108/ICS-06-2017-0039

131. Sultana, N. R. (2021). Factors affecting the adoption of fintech in developing countries: A review of the literature. *Journal of Asian Finance, Economics and Business,, 8*(6), 65-77.

132. Sung, K. L. (2018). FinTech (Financial Technology): What is it and how to use technologies to create busines value in FinTech way? *International Journal of Innovation, Management and Technolgoy, 9*(2), 74-78. doi:doi:10.18178/ijimt.2018.9.2.791

133. Swammy, S. T. (2019, January 25). A vision for the future: the Bermuda FinTech story. *Crypto Uncovered: The Evolution of Bitcoin and the Crypto Currency Marketplace*, pp. 173-181.

134. Tade, O. a. (2020). Dimensions of electronic fraud and governance of trust in Nigeria's cashless ecosystem abstract Oludayo Tade and Oluwatosin Adeniyi". *International Journal of Offender Therapy and Comparative Criminology, 64*(16), 1-15.

135. Tahir, N. (2023, June 11). Despair in digital age online scams shake Pakistan s financial scene. Karachi, Sindh, Pakistan: The Express Tribune. From https://tribune.com.pk/story/2421209/despair-in-digital-age-online-scams-shake-pakistans-financial-scene

136. Tan, E. a. (2016). Behavioural intention to adopt mobile banking among the millennial generation. *Young Consumers, 17*(1), 18-31.

137. TELUS Digital. (2021, July 22). *Bridging the trust gap in FinTech*. From telusdigital.com: https://www.telusdigital.com/insights/trust-and-safety/article/bridging-the-fintech-trust-gap

138. Tick, P. T. (2021). Cyber Seucrity Awareness and Beahvior of Youth in Smartphone Usage: A comparative study between... *Acta Polytechnica Hungarica, 18*, 67-89. doi:10.12700/APH.18.8.2021.8.4

139. Treasury, H. (2023). *Future of Payments Review report.* UK Government. From https://assets.publishing.service.gov.uk/media/6557a1eb046ed400148b9b50/Future_of_Payments_Review_report.pdf

140. Utomo, P. K. (2021). The effects of performance expectancy, effort expectancy, facilitating condition, and habit on behavior intention in using mobile healthcare application. *International Journal of Community Service & Engagement, 2*(4), 183-197.

141. Verizon Business. (2024). *Data Breach Investigation Report.* Verizon Business.

142. Waechter, L. G. (2017). Examining the role of initial trust in user adoption of mobile payment services: an empirical investigation. *Information Systems Frontiers, 19*, 525-548. doi:DOI 10.1007/s10796-015-9611-0

143. Wang, D. L. (2020). What affects the intention to use digital wallets? A study of the theory of reasoned actions and trust. *Journal of Consumer Behaviour, 19*(5), 496-508.

144. Whitman, M. a. (2009). In *Principles of Information Security.* Course Technology.

145. World Bank. (2017). *Pakistan Development Update Growth: A shared responsibility, World Bank Group, Washington DC.* World Bank.

146. World Bank Group. (2021). *Consumer Risk in FInTech.* World Bank Group and Foreign Ministry of The Netherland. From https://documents1.worldbank.org/curated/en/515771621921739154/pdf/Consumer-Risks-in-Fintech-New-Manifestations-of-Consumer-Risks-and-Emerging-Regulatory-Approaches-Policy-Research-Paper.pdf

147. Xiao Xiang, Z. L. (2017, December 23). *China's Path to FinTech Development*. From European Economy: https://european-economy.eu/2017-2/chinas-path-to-fintech-development/

148. Xin H, T. A. (2015). Antecedents of consumer trust in mobile payment adoption. *J Comput Inform Syst, 55*(4), 1-10. doi:https:// doi. org/ 10. 1080/ 08874 417. 2015. 11645 781

149. Xiongfei Cao, L. Y. (2018). Understanding mobile payment users' continuance intention: a trust transfer perspective. *Internet Research, 28*(2), 456-476. doi:DOI 10.1108/IntR-11-2016-0359

150. Yacoub, G. a. (2022). Blockchain in your grocery basket: trust and traceability as a strategy. *Journal of Business Strategy, 43*(4), 247-256.

151. Yang, K. C. (2012). A two-factor theory for website analysis and redesign for mobile compatibility. *Decision Support Systems, 53*(3), 583-593. doi:https://doi.org/10.1016/j.dss.2012.04.009

152. YOUSAFZAI, A. R. (2020, December 24). Scammers rob Rs5.6 billion in online investment fraud in Pakistan's northwest. Peshawar, KPK, Pakistan. From https://www.arabnews.com/node/1782216/amp

153. Zhang, Y. L. (2003). Intrusion detection techniques for mobile wireless networks. *Wireless Networks*, 545-556.

154. Zhenning Wang, Z. G. (2019). What determines customers continuance intention of FinTech? Evidence from YuEbao. *Industrial Management and Data Systems, 119*(8), 1625-1637. doi:10.1108/IMDS-01-2019-0011

Appendices

Appendix 1. Questionnaire

Section A: General FinTech Usage (For all respondents)

Are you a FinTech user? For example, mobile banking, EasyPaisa, JazzCash, NayaPay or SadaPay, etc.

Which FinTech products do you use?

- Mobile banking applications (e.g., HBL, UBL, Meezan, etc)
- JazzCash
- EasyPaisa
- NayaPay
- SadaPay
- Other:________________________

Have you ever experienced a fraud or scam or financial loss while using any of these FinTech applications? If you answered "Yes" to question 3, then please continue to section B. Otherwise, skip to section C directly.

Section B: For those who experienced FinTech Fraud or scam.

- What kind of fraud or financial/non-financial loss did you experience?
- Unauthorized transactions
- Scammed by someone impersonating over a phone call
- Personal data breach
- Scammed by a fraudulent FinTech service provider
- Other:

(Scale: 1 = Strongly Disagree, 5 = Strongly Agree)

Cash Culture H1: (Sania Zafar Awan, 2021) (Sharif, 2025)
1. I feel cash payments are convenient compared to digital payments.
2. I avoid FinTech after the data breach because cash feels secure.
3. I think cash payments are simpler than digital payments.

Perceived Risk H2: (K. Gupta, 2023) (Lee, 2009)
1. I find online banking and applications to be extremely risky to use after a scam or data breach.
2. I am afraid that online banking applications will not reimburse me if I lose money after a scam or fraud.
3. I worry that my personal data can be misused by FinTech companies.

Regulatory Challenges H3: (Sohail, 2024) (Ahmad Fraz, 2021)
1. I think FinTech regulations in Pakistan are not well developed.
2. I believe victims of data breaches or fraud don't get justice in Pakistan.
3. I think current regulations need to adopt current innovations.

Cybersecurity Awareness H4: (Tick, 2021)

1. I wouldn't reveal any confidential information under any circumstances to unknown sources.
2. I am aware of and able to identify the latest online banking scams.
3. I know how to activate security features on my FinTech application.

Perceived usefulness H5: (Cheng TCE, 2006)

1. I think using online banking is still useful for me even after the scam/fraud.
2. Online banking can still provide significant benefits despite previous security breaches.
3. I think online banking saves a lot of time for me to carry out my routine tasks.

Perceived ease of use H6: (Cheng TCE, 2006)

1. I think it is easy to use online banking services after security updates.
2. Periodic security updates have made digital banking services easier.
3. I think making transactions using online banking is simpler.

Transparency H7: (Dietz, 2009)

1. My company communicated the cause of the data breach.
2. I received timely updates about the data breach.
3. I was communicated the steps taken to prevent such data breaches in the future.

Security Updates H8: (Jia Qi, 2024) (Patria Laksamana, 2023)

1. I think my mobile payment transaction information is secure despite the data breach.
2. I noticed visible security improvements after the data breach.
3. I believe 2-factor authentication makes FinTech applications more secure.

Perceived Trust Recovery: (Awad, 2008)

1. I trust my digital banking service provider even after the fraud/scam.
2. I would recommend using FinTech to others despite scams and fraud.
3. I am confident that my digital banking provider can solve my problems in time.

Section C: All Respondents

(**Scale: 1 = Strongly Disagree, 5 = Strongly Agree)**

I would be more likely to use FinTech again if the companies implement:

1. Full public disclosure of the breach and steps taken to avoid a similar situation in the future. (Lewicki, 1996)
2. A public apology from the CEO, taking responsibility. (Lewicki, 1996) (Dietz, 2009)
3. Full or partial reimbursement for the losses caused by the data breach. (Dietz, 2009)
4. Visible security upgrades, for example, 2-factor authentication, biometric login, etc. (Dietz, 2009)
5. Regulatory partnerships with regulators or accredited independent audits. (Dietz, 2009)
6. Educational programs for consumers on identifying scams and avoiding breaches. (Mazer, 2022) (Krishna, 2023)
7. The company provides adequate staff training to secure leakage of sensitive information. (Abidin, 2019)
8. Set up a 24/7 fraud support hotline (English & Urdu) that guarantees immediate response to minimize the damage.

Insights on Trust in FinTech Products:

Please choose the top three features that would increase and diminish your trust in FinTech products like JazzCash, Easypaisa, digital banking applications, NayaPay, SadaPay, etc.

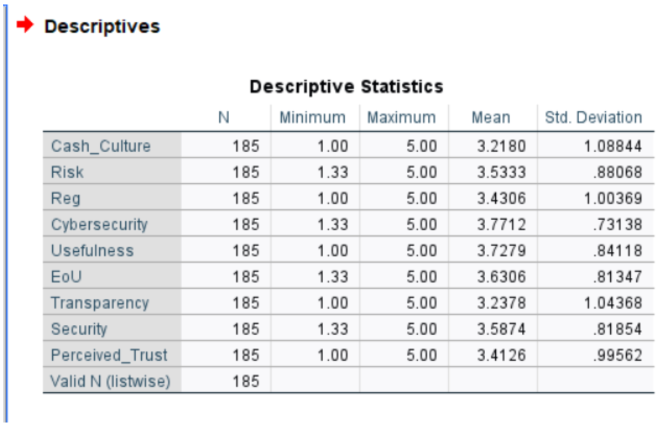
Trust Builders: What makes you trust FinTech products? **Choose the top 3.**

1. Quick refunds in case of financial loss.
2. Instant notifications for every transaction.
3. Easy login with multi-factor authentication or bio-metric login options.
4. Government-approved applications.
5. Clear privacy policy with no third-party data-sharing requirements.
6. Periodic fear-centric messages on rising frauds, scams, and data breaches.
7. Active 24/7 customer support.

Trust Diminishers: What makes you stop trusting FinTech products? **Choose the top 3**

1. No reliable customer support.
2. No disclosures from the company on data breaches.
3. Frequent app crashes while processing payments.
4. Delayed or slow transactions alerts.
5. Difficulty recovering passwords, accounts, payment processing & confusing menus.
6. Data sharing without clear user consent.
7. No visible security improvements in the product after the scam/fraud/data breach.

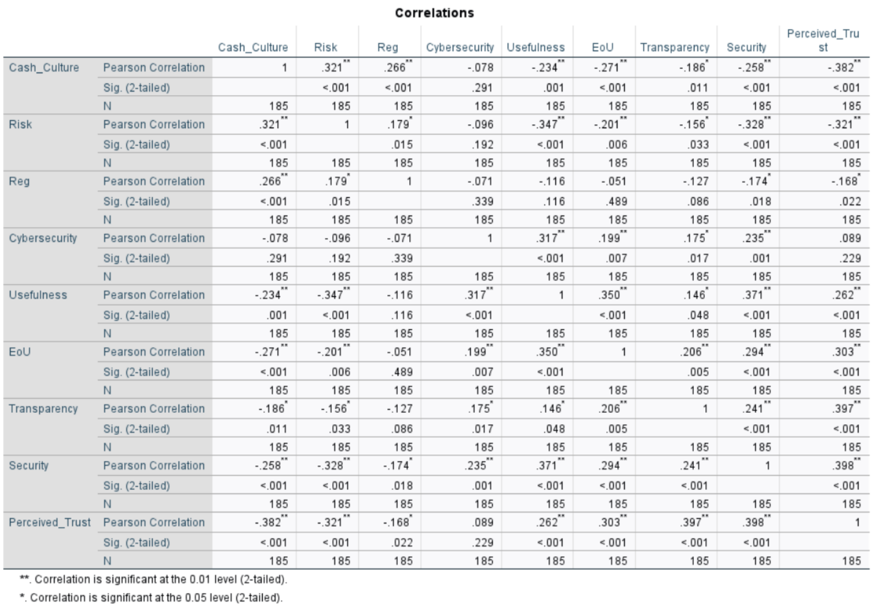
Appendix 2. Descriptive and Correlation Analysis



Descriptives

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Cash_Culture	185	1.00	5.00	3.2180	1.08844
Risk	185	1.33	5.00	3.5333	.88068
Reg	185	1.00	5.00	3.4306	1.00369
Cybersecurity	185	1.33	5.00	3.7712	.73138
Usefulness	185	1.00	5.00	3.7279	.84118
EoU	185	1.33	5.00	3.6306	.81347
Transparency	185	1.00	5.00	3.2378	1.04368
Security	185	1.33	5.00	3.5874	.81854
Perceived_Trust	185	1.00	5.00	3.4126	.99562
Valid N (listwise)	185				



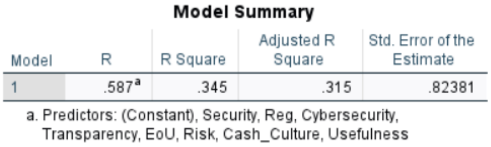
Correlations

		Cash_Culture	Risk	Reg	Cybersecurity	Usefulness	EoU	Transparency	Security	Perceived_Trust
Cash_Culture	Pearson Correlation	1	.321**	.266**	-.078	-.234**	-.271**	-.186*	-.258**	-.382**
	Sig. (2-tailed)		<.001	<.001	.291	.001	<.001	.011	<.001	<.001
	N	185	185	185	185	185	185	185	185	185
Risk	Pearson Correlation	.321**	1	.179*	-.096	-.347**	-.201**	-.156*	-.328**	-.321**
	Sig. (2-tailed)	<.001		.015	.192	<.001	.006	.033	<.001	<.001
	N	185	185	185	185	185	185	185	185	185
Reg	Pearson Correlation	.266**	.179*	1	-.071	-.116	-.051	-.127	-.174*	-.168*
	Sig. (2-tailed)	<.001	.015		.339	.116	.489	.086	.018	.022
	N	185	185	185	185	185	185	185	185	185
Cybersecurity	Pearson Correlation	-.078	-.096	-.071	1	.317**	.199**	.175*	.235**	.089
	Sig. (2-tailed)	.291	.192	.339		<.001	.007	.017	.001	.229
	N	185	185	185	185	185	185	185	185	185
Usefulness	Pearson Correlation	-.234**	-.347**	-.116	.317**	1	.350**	.146*	.371**	.262**
	Sig. (2-tailed)	.001	<.001	.116	<.001		<.001	.048	<.001	<.001
	N	185	185	185	185	185	185	185	185	185
EoU	Pearson Correlation	-.271**	-.201**	-.051	.199**	.350**	1	.206**	.294**	.303**
	Sig. (2-tailed)	<.001	.006	.489	.007	<.001		.005	<.001	<.001
	N	185	185	185	185	185	185	185	185	185
Transparency	Pearson Correlation	-.186*	-.156*	-.127	.175*	.146*	.206**	1	.241**	.397**
	Sig. (2-tailed)	.011	.033	.086	.017	.048	.005		<.001	<.001
	N	185	185	185	185	185	185	185	185	185
Security	Pearson Correlation	-.258**	-.328**	-.174*	.235**	.371**	.294**	.241**	1	.398**
	Sig. (2-tailed)	<.001	<.001	.018	.001	<.001	<.001	<.001		<.001
	N	185	185	185	185	185	185	185	185	185
Perceived_Trust	Pearson Correlation	-.382**	-.321**	-.168*	.089	.262**	.303**	.397**	.398**	1
	Sig. (2-tailed)	<.001	<.001	.022	.229	<.001	<.001	<.001	<.001	
	N	185	185	185	185	185	185	185	185	185

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

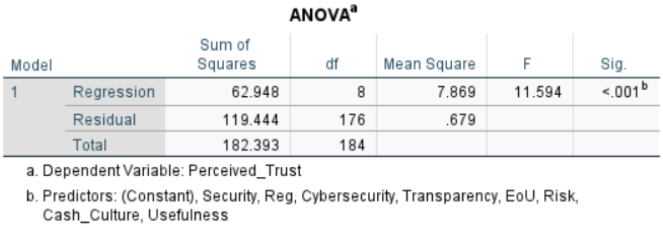
Appendix 3. Regression Analysis



Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.587[a]	.345	.315	.82381

a. Predictors: (Constant), Security, Reg, Cybersecurity, Transparency, EoU, Risk, Cash_Culture, Usefulness

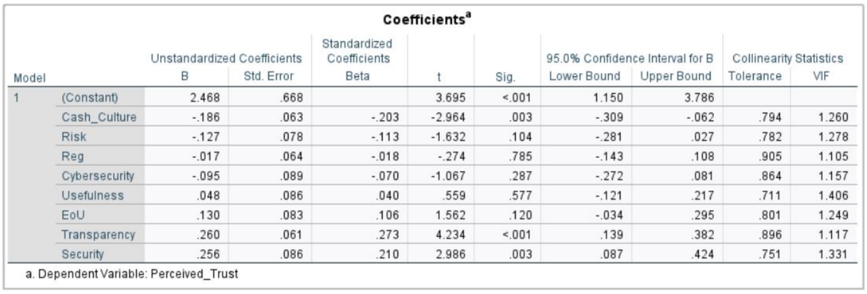


ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	62.948	8	7.869	11.594	<.001[b]
	Residual	119.444	176	.679		
	Total	182.393	184			

a. Dependent Variable: Perceived_Trust

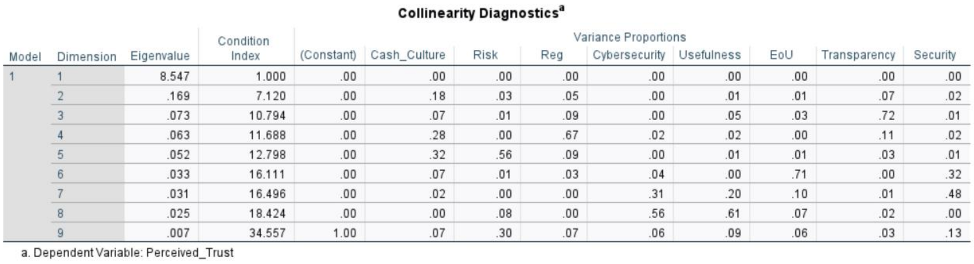
b. Predictors: (Constant), Security, Reg, Cybersecurity, Transparency, EoU, Risk, Cash_Culture, Usefulness



Coefficients[a]

		Unstandardized Coefficients		Standardized Coefficients			95.0% Confidence Interval for B		Collinearity Statistics	
Model		B	Std. Error	Beta	t	Sig.	Lower Bound	Upper Bound	Tolerance	VIF
1	(Constant)	2.468	.668		3.695	<.001	1.150	3.786		
	Cash_Culture	-.186	.063	-.203	-2.964	.003	-.309	-.062	.794	1.260
	Risk	-.127	.078	-.113	-1.632	.104	-.281	.027	.782	1.278
	Reg	-.017	.064	-.018	-.274	.785	-.143	.108	.905	1.105
	Cybersecurity	-.095	.089	-.070	-1.067	.287	-.272	.081	.864	1.157
	Usefulness	.048	.086	.040	.559	.577	-.121	.217	.711	1.406
	EoU	.130	.083	.106	1.562	.120	-.034	.295	.801	1.249
	Transparency	.260	.061	.273	4.234	<.001	.139	.382	.896	1.117
	Security	.256	.086	.210	2.986	.003	.087	.424	.751	1.331

a. Dependent Variable: Perceived_Trust

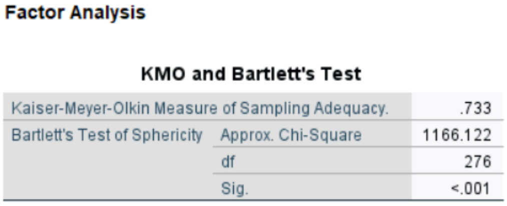


Collinearity Diagnostics[a]

				Variance Proportions								
Model	Dimension	Eigenvalue	Condition Index	(Constant)	Cash_Culture	Risk	Reg	Cybersecurity	Usefulness	EoU	Transparency	Security
1	1	8.547	1.000	.00	.00	.00	.00	.00	.00	.00	.00	.00
	2	.169	7.120	.00	.18	.03	.05	.00	.01	.01	.07	.02
	3	.073	10.794	.00	.07	.01	.09	.00	.05	.03	.72	.01
	4	.063	11.688	.00	.28	.00	.67	.02	.02	.00	.11	.02
	5	.052	12.798	.00	.32	.56	.09	.00	.01	.01	.03	.01
	6	.033	16.111	.00	.07	.01	.03	.04	.00	.71	.00	.32
	7	.031	16.496	.00	.02	.00	.00	.31	.20	.10	.01	.48
	8	.025	18.424	.00	.00	.08	.00	.56	.61	.07	.02	.00
	9	.007	34.557	1.00	.07	.30	.07	.06	.09	.06	.03	.13

a. Dependent Variable: Perceived_Trust

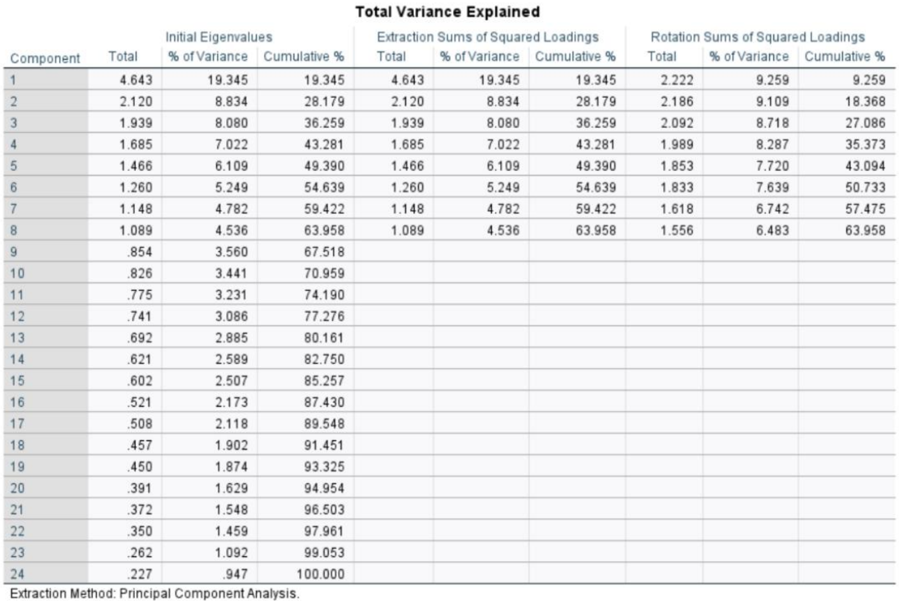
Appendix 4. Factor Analysis



Factor Analysis

KMO and Bartlett's Test

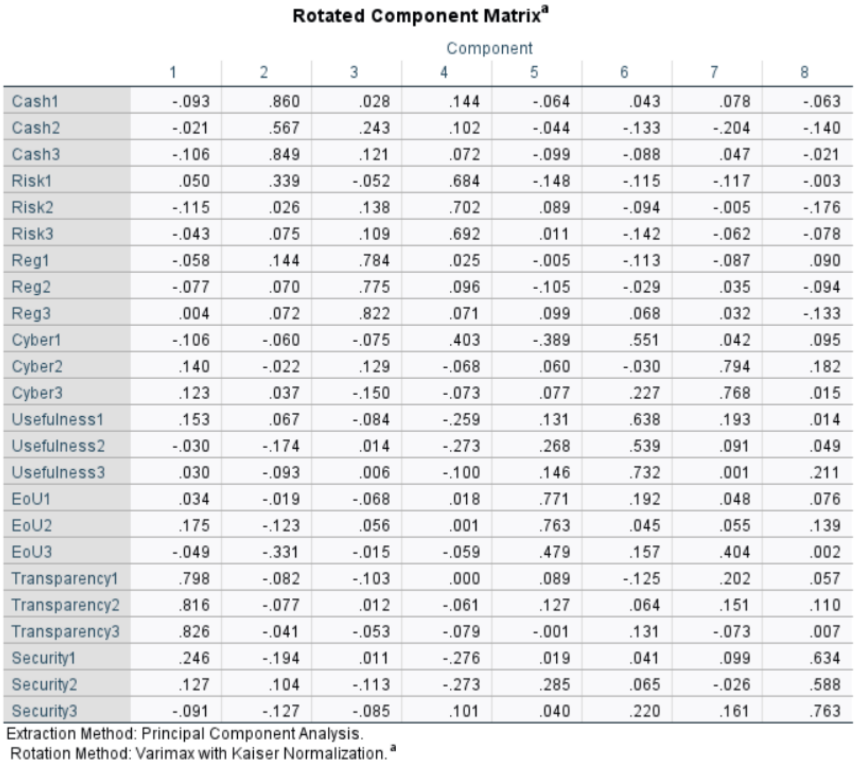
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.733
Bartlett's Test of Sphericity	Approx. Chi-Square	1166.122
	df	276
	Sig.	<.001



Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	4.643	19.345	19.345	4.643	19.345	19.345	2.222	9.259	9.259
2	2.120	8.834	28.179	2.120	8.834	28.179	2.186	9.109	18.368
3	1.939	8.080	36.259	1.939	8.080	36.259	2.092	8.718	27.086
4	1.685	7.022	43.281	1.685	7.022	43.281	1.989	8.287	35.373
5	1.466	6.109	49.390	1.466	6.109	49.390	1.853	7.720	43.094
6	1.260	5.249	54.639	1.260	5.249	54.639	1.833	7.639	50.733
7	1.148	4.782	59.422	1.148	4.782	59.422	1.618	6.742	57.475
8	1.089	4.536	63.958	1.089	4.536	63.958	1.556	6.483	63.958
9	.854	3.560	67.518						
10	.826	3.441	70.959						
11	.775	3.231	74.190						
12	.741	3.086	77.276						
13	.692	2.885	80.161						
14	.621	2.589	82.750						
15	.602	2.507	85.257						
16	.521	2.173	87.430						
17	.508	2.118	89.548						
18	.457	1.902	91.451						
19	.450	1.874	93.325						
20	.391	1.629	94.954						
21	.372	1.548	96.503						
22	.350	1.459	97.961						
23	.262	1.092	99.053						
24	.227	.947	100.000						

Extraction Method: Principal Component Analysis.

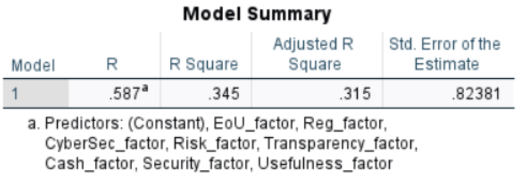


Rotated Component Matrix[a]

	Component							
	1	2	3	4	5	6	7	8
Cash1	-.093	.860	.028	.144	-.064	.043	.078	-.063
Cash2	-.021	.567	.243	.102	-.044	-.133	-.204	-.140
Cash3	-.106	.849	.121	.072	-.099	-.088	.047	-.021
Risk1	.050	.339	-.052	.684	-.148	-.115	-.117	-.003
Risk2	-.115	.026	.138	.702	.089	-.094	-.005	-.176
Risk3	-.043	.075	.109	.692	.011	-.142	-.062	-.078
Reg1	-.058	.144	.784	.025	-.005	-.113	-.087	.090
Reg2	-.077	.070	.775	.096	-.105	-.029	.035	-.094
Reg3	.004	.072	.822	.071	.099	.068	.032	-.133
Cyber1	-.106	-.060	-.075	.403	-.389	.551	.042	.095
Cyber2	.140	-.022	.129	-.068	.060	-.030	.794	.182
Cyber3	.123	.037	-.150	-.073	.077	.227	.768	.015
Usefulness1	.153	.067	-.084	-.259	.131	.638	.193	.014
Usefulness2	-.030	-.174	.014	-.273	.268	.539	.091	.049
Usefulness3	.030	-.093	.006	-.100	.146	.732	.001	.211
EoU1	.034	-.019	-.068	.018	.771	.192	.048	.076
EoU2	.175	-.123	.056	.001	.763	.045	.055	.139
EoU3	-.049	-.331	-.015	-.059	.479	.157	.404	.002
Transparency1	.798	-.082	-.103	.000	.089	-.125	.202	.057
Transparency2	.816	-.077	.012	-.061	.127	.064	.151	.110
Transparency3	.826	-.041	-.053	-.079	-.001	.131	-.073	.007
Security1	.246	-.194	.011	-.276	.019	.041	.099	.634
Security2	.127	.104	-.113	-.273	.285	.065	-.026	.588
Security3	-.091	-.127	-.085	.101	.040	.220	.161	.763

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.[a]

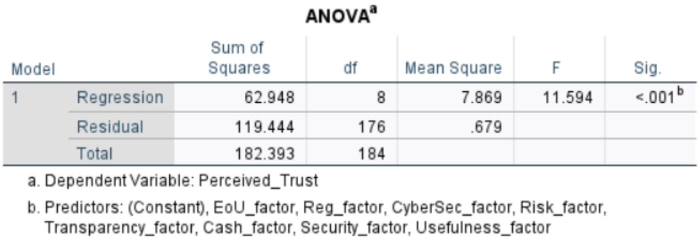
Appendix 5. Regression Analysis on Factors



Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.587[a]	.345	.315	.82381

a. Predictors: (Constant), EoU_factor, Reg_factor, CyberSec_factor, Risk_factor, Transparency_factor, Cash_factor, Security_factor, Usefulness_factor

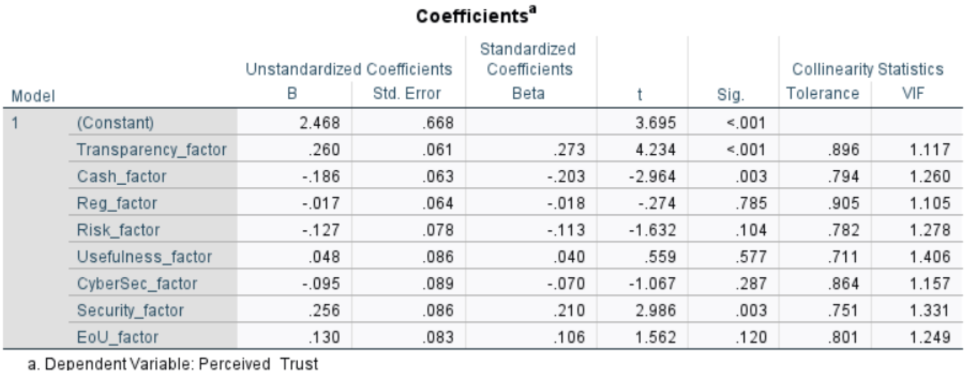


ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	62.948	8	7.869	11.594	<.001[b]
	Residual	119.444	176	.679		
	Total	182.393	184			

a. Dependent Variable: Perceived_Trust

b. Predictors: (Constant), EoU_factor, Reg_factor, CyberSec_factor, Risk_factor, Transparency_factor, Cash_factor, Security_factor, Usefulness_factor

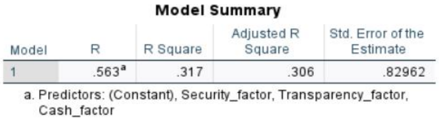


Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	2.468	.668		3.695	<.001		
	Transparency_factor	.260	.061	.273	4.234	<.001	.896	1.117
	Cash_factor	-.186	.063	-.203	-2.964	.003	.794	1.260
	Reg_factor	-.017	.064	-.018	-.274	.785	.905	1.105
	Risk_factor	-.127	.078	-.113	-1.632	.104	.782	1.278
	Usefulness_factor	.048	.086	.040	.559	.577	.711	1.406
	CyberSec_factor	-.095	.089	-.070	-1.067	.287	.864	1.157
	Security_factor	.256	.086	.210	2.986	.003	.751	1.331
	EoU_factor	.130	.083	.106	1.562	.120	.801	1.249

a. Dependent Variable: Perceived_Trust

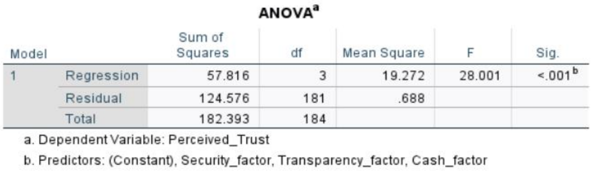
Appendix 6. Reduced Model Regression Analysis



Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.563[a]	.317	.306	.82962

a. Predictors: (Constant), Security_factor, Transparency_factor, Cash_factor

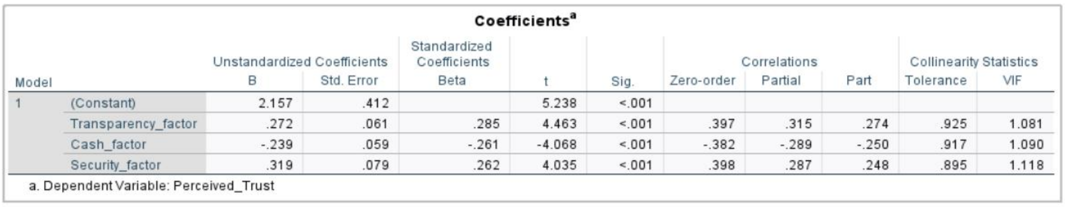


ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	57.816	3	19.272	28.001	<.001[b]
	Residual	124.576	181	.688		
	Total	182.393	184			

a. Dependent Variable: Perceived_Trust

b. Predictors: (Constant), Security_factor, Transparency_factor, Cash_factor



Coefficients[a]

		Unstandardized Coefficients		Standardized Coefficients			Correlations			Collinearity Statistics	
Model		B	Std. Error	Beta	t	Sig.	Zero-order	Partial	Part	Tolerance	VIF
1	(Constant)	2.157	.412		5.238	<.001					
	Transparency_factor	.272	.061	.285	4.463	<.001	.397	.315	.274	.925	1.081
	Cash_factor	-.239	.059	-.261	-4.068	<.001	-.382	-.289	-.250	.917	1.090
	Security_factor	.319	.079	.262	4.035	<.001	.398	.287	.248	.895	1.118

a. Dependent Variable: Perceived_Trust