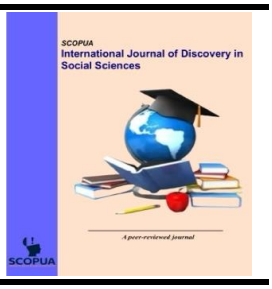
International Journal of Discovery in Social Sciences

Vol.1, Issue 1, August 2025
DOI: https://doi.org/10.64060/IJDSS.v1i1.5



The Impact of Financial Scams on Consumer Trust in the Banking Sector: A Qualitative Analysis

Faisal Akbar [1], Junaid Hussain [1], Babar Usman [1], Jamil Afzal [2*]

[1]Lahore Garrison University, Pakistan

[2]International Islamic University Malaysia

* Corresponding Email: sirjamilafzal@gmail.com

Received: 17 June 2025 / Revised: 06 August 2025 / Accepted: 08 August 2025 / Published online: 10 August 2025

ABSTRACT

The high rate of digitization in Pakistan's banking sector has changed financial habits, but it has also made consumers vulnerable to advanced forms of financial fraud. This paper examines the affective, psychological, and behavioral consequences of banking scams on Pakistan-based consumers, focusing on their experiences and confidence in the banking system. By conducting a qualitative thematic analysis of interview data with 15 people who suffered scams, the study recognizes several scam-type variations, such as OTP phishing, fraudulent online purchases, and impersonation, and analyzes them in terms of their effects on the victim's perception and behavior. Results show that the effects of scam experiences are feelings of deep emotional distress, such as feelings of shame, anxiety, and a loss of self-confidence, and frequently because of cultural stigma. Institutional responsiveness comes out as a key element: compassionate treatment reinforces trust, whereas dismissive or accusatory reactions lead to increased symptoms of distrust and withdrawal. It is discovered that consumer vulnerability varies and is situational and depends on the gaps in digital literacy, manipulation through emotions, and weaknesses in the system as far as the learning of the consumer is concerned. Post-scam behaviors include adaptive caution down to maladaptive avoidance of digital financial services, with implications for financial inclusion objectives. Participants advocate strongly for proactive consumer education, transparent institutional communication, and coordinated regulatory action. The study contributes to both academic literature and practical policy by highlighting the socio-emotional dimensions of scam victimization in Pakistan's digital banking ecosystem. It calls for holistic, consumer-centered strategies to strengthen trust and resilience in the face of evolving financial scams.

Keywords*:* Financial Scams; Consumer Trust; Pakistan; Digital Banking; Thematic Analysis; Consumer Protection; Institutional Response; Financial Literacy

1. Introduction

1.1 Background and Context

Over the past decade, the proliferation of digital banking and online financial services has transformed the way consumers interact with financial institutions worldwide (Bouveret, 2018; (Afzal 2024). While these innovations have enhanced convenience and financial inclusion, they have also exposed consumers to new forms of financial fraud and scams(Afzal, Yongmei et al. 2024). Banking scams, particularly those leveraging social engineering techniques, phishing, and impersonation, have emerged as a significant threat to consumer financial well-being and institutional trust (Button, Lewis, & Tapley, 2014). This threat is not merely a matter of individual financial loss; it represents a systemic risk to the stability of the financial system itself. The Financial Stability Board (2024) has noted that widespread cyber-fraud can undermine confidence in digital payment systems, posing a threat to financial stability, particularly in emerging economies where digital adoption is outpacing

regulatory and educational maturity (Financial Stability Board, 2024). Foundational economic sociology posits that trust is the essential lubricant of any financial system, enabling transactions and investments that would otherwise be paralyzed by risk and uncertainty. Therefore, the erosion of consumer trust by financial scams is not just a customer service issue but a fundamental crisis of social and institutional confidence. The recent digitization of the banking system has done wonders in Pakistan, but the widespread availability of smartphones and mobile wallets has created a fertile breeding ground for financial scams (Yongmei and Afzal 2023, Afzal 2025). As reported by the State Bank of Pakistan (2022), the number of digital banking transactions in Pakistan increased by 57 percent in 2021, which constitutes a larger cashless-online-financial behavior phenomenon. However, this growth has also been accompanied by a notable increase in consumer-targeted scams, with the Federal Investigation Agency (FIA) Cybercrime Wing reporting over 100,000 complaints of financial fraud in 2022 alone (FIA, 2022). These scams range from OTP (one-time password) fraud, online shopping scams, fake investment schemes, to phishing attacks impersonating bank officials.

1.2 Rise of Financial Scams Globally and in Pakistan

Globally, financial scams represent a multibillion-dollar industry. The Federal Trade Commission (FTC) in the United States reported that consumers lost over $8.8 billion to scams in 2022, a 30% increase from the previous year (FTC, 2023). Similarly, the UK's Financial Conduct Authority (FCA) has identified online banking fraud and authorized push payment (APP) scams as among the most prevalent financial threats (FCA, 2023). These trends underscore a global epidemic of digital financial crime. The International Monetary Fund has warned that such trends can have macroeconomic consequences, reducing consumer spending and savings rates as trust in financial intermediaries' wanes (IMF, 2022). Pakistan mirrors these trends but faces unique contextual challenges. The country's financial literacy rate remains low, with only 26% of adults demonstrating basic financial knowledge (SBP, 2021). Coupled with increasing mobile phone penetration and aggressive marketing of digital financial services, this environment leaves consumers particularly vulnerable to sophisticated scams (Hasan & Ali, 2020). The FIA Cybercrime Wing reports that phishing scams targeting Pakistani bank customers have increased by 47% in the past two years (FIA, 2022). OTP fraud, wherein scammers impersonate bank staff and trick consumers into sharing their authentication codes, has emerged as a particularly damaging tactic (PTA, 2023).

1.3 Digital Banking & Scam Ecosystem in Pakistan

Pakistan's digital banking landscape is rapidly evolving. With over 125 million mobile phone subscribers and growing internet penetration (PTA, 2023), the country is experiencing a digital financial revolution. Mobile wallets such as Easypaisa and JazzCash, alongside traditional banks' digital platforms, now serve millions of consumers. The COVID-19 pandemic further accelerated this shift, pushing more transactions online (World Bank, 2021). However, this transformation has also expanded the attack surface for scammers. Online shopping scams, fake investment opportunities, lottery fraud, and phishing attacks are rampant across social media platforms (Ali & Ahmed, 2022). A recent survey by Karandaaz Pakistan (2022) found that 32% of Pakistani digital banking users had encountered or narrowly avoided a scam attempt. The fragmented regulatory landscape and lack of consistent consumer awareness initiatives exacerbate the problem (SBP, 2022). Moreover, institutional responses to scam reports are often perceived as inadequate, contributing to declining consumer trust in banks (Interview Transcripts 6-18). This study aims to fill a critical gap in understanding the lived experiences of Pakistani consumers affected by bank-related scams, exploring the emotional, behavioral, and trust-related impacts of such incidents.

1.4 Emotional, Psychological, and Social Impact of Scams

The emotional and psychological toll of financial scams on victims is profound. Numerous studies indicate that beyond financial losses, scam victims often experience intense feelings of shame, guilt, anxiety, and depression (Cross, Richards, & Smith, 2016; Whitty, 2018). The sense of personal violation and perceived naivety associated with falling victim to a scam can result in long- lasting emotional trauma (Button et al., 2014). Victims frequently report self-blame, social withdrawal, and erosion of self-confidence (Cross et al., 2016). These patterns are illustrated in the interviews carried out in this research. It is emphasized that after understanding they have been scammed, many participants shared the feelings of being embarrassed, angry, and helpless (Interview Transcripts 6-18). One of them interviewed said: I was unable to sleep several days, wondering how I managed to be that stupid (Interview 3). Another would describe that he suffered intense anxiety which did not go away even when the financial problem was solved. This kind of emotional strain does not only create problems

on an individual level, but also impacts the way people will interact with the digital banking ecosystem in the future. Moreover, social stigma connected with getting scammed is likely to prevent the victim of the event to seek help or file a report (Button & Cross, 2017). This stigma can be especially strong in the case of Pakistani context where finances tend to coincide with family and community honor (Hasan & Ali, 2020). It emphasizes the relevance of favorable institutional reactions and social awareness campaigns that normalize the reporting of victims and decrease shame.

1.5 Institutional Response & Consumer Trust Issues

The response of the institution to a bank scam is important in determining the confidence of the consumers and the integrity of the banking system. It has been found that consumer trust can be maintained and, in some cases, even enhanced when financial institutions take swift, transparent, and emotional responses to reports of scams (Lee & Turban, 2001; Lichtenstein & Williamson, 2006). On the other hand, institutional reactions that are ineffective worsen the suffering of the victim and the loss of confidence (Cross et al., 2016). In Pakistani banking, the sources in this study have mixed feelings on the response of the institutions. Other respondents said that the responses were dismissive or unhelpful or that bank staff was very professional. One participant shared: "I reported it to my bank immediately, but they just told me there's nothing they can do" (Interview 8). Another noted: "They [the bank] were polite but offered no real support, just advised me to be more careful next time" (Interview 12). Such experiences contribute to a climate of distrust toward financial institutions. According to a 2022 survey by Gallup Pakistan, 37% of respondents reported low or no trust in banks to protect their personal data (Gallup Pakistan, 2022). This distrust is further fueled by perceptions that banks prioritize their liability minimization over customer protection (Interview Transcripts 6-18). Strengthening institutional responses to scams, including clear communication, victim support mechanisms, and proactive fraud prevention, is essential to restoring and maintaining consumer trust.

1.6 Vulnerability and Risk Factors

Understanding the factors that render consumers vulnerable to scams is critical for effective prevention. Prior research identifies several risk factors, including low financial literacy, limited digital literacy, social isolation, and personality traits such as trustfulness or impulsivity (DeLiema, 2018; Whitty, 2018). In Pakistan, these vulnerabilities are compounded by rapid digitalization outpacing consumer education and regulatory oversight (Hasan & Ali, 2020). The present study's findings corroborate these insights. Participants frequently cited a lack of awareness about scam tactics and over-reliance on perceived institutional authority as contributors to their victimization. One respondent stated: "I thought it was really my bank calling me… I didn't know they [banks] would never ask for OTP" (Interview 5). Another reflected: "I trusted the online store because it looked professional, but I had no idea it was fake" (Interview 10). Many participants described feeling "rushed" or "pressured" during scam interactions, impairing their ability to evaluate the situation critically (Interview Transcripts 6-18). These findings highlight the urgent need for targeted consumer education and behavioral interventions that address both cognitive and emotional dimensions of scam susceptibility.

1.7 Post-Scam Behavior and Consumer Protection

The behavior of victims after the scams has valuable lessons in the process of recovery, as well as the potential to enhance consumer protection. Studies indicate that victim's resort to increased caution and new security routines and promote increased awareness (Button & Cross, 2017; DeLiema, 2018). Nonetheless, behavioral changes do not always benefit the illegal proprietary network, as some victims can refuse digital banking completely, and their role in the financial system becomes restricted (Cross et al., 2016). According to the interviews in this study, there was a range in the response after the scam. Several participants said that they became more alert: "I now scrutinize every message: I never click a non-familiar link" (Interview 6). The other participants incorporated new security practices like two-factor authentication, frequent change of passwords, and source verification before undertaking financial transactions. One respondent stated: "After this happened, I installed antivirus software and started using secure browsers" (Interview 11). At the same time, several participants expressed lingering anxiety and reduced trust in online banking: "I avoid using mobile banking now, only go to the branch" (Interview 14). The avoidance behavior may derail financial inclusion initiatives, especially among populations that have low physical proximity to the banking facilities (Hasan & Ali, 2020). This highlights the fact that it is essential not only to empower the consumers on the aspect of protective knowledge but also to reconstruct trust thanks to the role of institutional transparency and support. From a policy perspective, results indicate that there is a need to have complete consumer protection systems. Directions on how to prevent digital fraud have been published by the State Bank of Pakistan

(2022), but the enforcement thereof and the general awareness thereof lack uniformity. More cooperation between banks, regulators, and consumer advocacy movements is needed to establish solid post-scam protection mechanisms and resilience in digital financial environments.

1.8 Rationale for the Study

Despite the growing prevalence of bank-related scams in Pakistan, empirical research on their consumer-level impacts remains scarce. Most existing studies focus on technical aspects of fraud detection or aggregate economic costs, with limited attention to the human experiences behind the statistics (Hasan & Ali, 2020; Ali & Ahmed, 2022). Understanding how scams affect individuals emotionally, psychologically, and behaviorally is crucial for designing effective prevention and response strategies. This study addresses this gap by exploring the lived experiences of Pakistani consumers affected by bank scams. Through in-depth interviews, it examines how scams shape victims' emotions, trust in institutions, and financial behaviors. Specifically, this study will analyze the dynamics of trust erosion and potential restoration through the established theoretical lens of Mayer, Davis, and Schoorman's (1995) model of organizational trust, which posits that perceptions of a trustee's Ability, Benevolence, and Integrity are the core antecedents of trust. This provides a clear analytical roadmap to move beyond description and toward a theoretically grounded explanation of the phenomenon. The insights generated aim to inform both academic discourse and practical interventions, contributing to a more holistic understanding of financial consumer protection in Pakistan's digital economy. Moreover, the study aligns with global research priorities emphasizing consumer-centered approaches to financial crime prevention (DeLiema, 2018; Whitty, 2018). By foregrounding victim perspectives, it advocates for empathetic and inclusive responses that go beyond technological solutions to address the socio-psychological dimensions of scam vulnerability and resilience.

Research Objectives and Questions Objectives

To examine the impact of financial scams on consumer trust in banking institutions.
To explore the psychological and emotional consequences of financial scams on affected consumers.
To identify the key factors that contribute to consumer vulnerability to financial scams in the banking sector.
To investigate the role of financial institutions' response mechanisms in rebuilding consumer trust after a scam incident.
To evaluate the effectiveness of consumer education programs in reducing vulnerability to financial scams.
To develop a theoretically grounded set of recommendations for financial institutions and regulators based on the principles of organizational trust and crisis communication.

The study seeks to answer the following research questions

How do financial scams affect consumer perceptions of banking institutions?
What psychological and emotional effects do financial scams have on consumer perceptions of financial institutions?
What factors make consumers more vulnerable to financial scams within the banking environment?

2. Literature Review

The banking industry's digital evolution has infused financial transactions with record levels of convenience and efficiency(Afzal 2024, Afzal 2024). Mobile and internet banking have become an indispensable part of contemporary finance, allowing customers to check their accounts, shift funds, and avail services with just a click or a tap. This digital ease has also provided new opportunities for cybercriminals to target vulnerabilities, causing financial scams to rise at a critical rate. These deceptive practices have a significant effect on customer confidence, which is the bedrock of the bank-customer relationship. Financial fraud occurs in numerous forms, ranging from phishing, identity theft, credit card scams, social engineering schemes, and deepfake impersonation. In line with Waliullah et al. (2025), the most common cyber threats in online banking are phishing attacks and malware attacks, which involve personal and financial data breaches. The writers note that consumers are fast becoming susceptible as these scams are becoming very sophisticated and easily found on digital platforms. The economic loss sustained because of these scams is huge. For example, in the UK alone, fraud loss was over £1.17 billion in 2024, representing one of the highest levels ever (The Times, 2025). In the US, the Federal Trade Commission (FTC) stated that Americans lost more than $10 billion to fraud in 2023, up 14% from the previous year (FTC, 2024). Across the world, cybercrime syndicates have been taking advantage of global payment systems to drain funds through mule accounts, layering schemes, and unauthorized crypto wallets. The Financial Action Task Force (FATF, 2023) alerts that money laundering using digital fraud routes is becoming more advanced. These cross-border trends not only suck out money but

also undermine the integrity of cross-border banking alliances. The Asia-Pacific area, in general, has experienced an upsurge in e-business and mobile payment cons, particularly in high-density countries with low levels of financial literacy (ADB, 2024). The psychological effect of financial cons is yet another essential aspect shaping customer trust. Alashwali et al. (2024) discovered that victims of financial fraud are usually afflicted with anxiety, stress, and feelings of helplessness. These psychological effects are not necessarily dependent on the amount of loss incurred; instead, they are a result of the violation of trust in a financially secure institution. Chawla et al. (2023) also observes that the loss of trust is particularly acute with elderly and lower-income individuals with lower financial literacy, who are less confident in dealing with sophisticated digital platforms and identifying scams. The victims also suffer from reputational loss, social isolation, and heightened distrust of subsequent digital interactions (Marwick & Lewis, 2022). These emotional consequences are compounded when victims become ignored or blamed by banks. A study by Rosenzweig et al. (2023) highlights that banks with little empathy in their response to fraud tend to suffer irreparable harm to customer relationships. Post-incident engagement with emotional intelligence is increasingly being seen as a key driver in averting fallout and restoring confidence. Trust in banking organizations is founded on perceived benevolence, competence, and integrity. If customers are scammed, these pillars are greatly damaged. A study by Gupta and Shukla (2024) points out that consumers' perception of the security of a bank's online platform has a noteworthy impact on their trust. According to their qualitative investigation, when security is compromised, customers doubt the institution's competency and its intent to safeguard their interests. In addition, if the bank does not do the right thing about it openly and does not do enough to help, the image of benevolence is undermined as well. Research by Kim et al. (2021) points out that even if the attack had been caused by external cyberattackers, customers tend to blame the bank's poor security architecture.

2.1 Theoretical Perspective

To systematically analyze the complex dynamics of consumer trust in the wake of financial scams, this study adopts a multi-layered theoretical perspective, integrating seminal models from organizational behavior, information systems, and crisis communication.

The Core Framework: Mayer, Davis, and Schoorman's (1995) Integrative Model of Organizational Trust

The foundational framework for this study is the integrative model of organizational trust proposed by Mayer, Davis, and Schoorman (1995). This model is one of the most widely cited in trust research and defines trust as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (Mayer et al., 1995, p. 712). This definition is particularly salient in the context of banking, where consumers (trustors) make themselves financially vulnerable to banks (trustees) with the expectation that their assets will be protected. The model posits that this willingness to be vulnerable is a function of the trustor's perception of the trustee's trustworthiness, which is composed of three distinct, yet interrelated, factors (Schoorman, Mayer, & Davis, 2007):

Ability: This refers to the group of skills, competencies, and characteristics that enable the trustee to have influence within a specific domain (Mayer et al., 1995). In the banking context, Ability encompasses the bank's perceived competence in securing customer data, providing reliable digital platforms, processing transactions accurately, and effectively preventing fraud. A consumer's belief in a bank's Ability is a belief that the bank *can* fulfill its protective duties.

Benevolence: This is the extent to which the trustee is believed to want to do good for the trustor, aside from any egocentric profit motive (Mayer et al., 1995). It is the perception that the bank genuinely cares about the customer's well-being, will act in their best interests, and will not exploit their vulnerability. Benevolence is about perceived motives and is crucial for building a relational, rather than purely transactional, bond.

Integrity: This involves the trustor's perception that the trustee adheres to a set of principles that the trustor finds acceptable, such as honesty and fairness (Mayer et al., 1995). For banks, this means being seen as acting consistently, keeping promises, being transparent in communications, and taking responsibility for failures. Integrity is about the alignment of the bank's actions with its stated values and the customer's ethical expectations. These three factors are not merely additive; they interact to form a holistic perception of trustworthiness. For instance, a bank may have high Ability (strong technology) but be perceived as lacking Benevolence (uncaring customer service) and Integrity (opaque fee structures), resulting in low overall trust. This model provides a powerful analytical lens to deconstruct *why* trust erodes after a scam, moving beyond the financial loss to examine how the incident and the bank's response impact perceptions of its Ability, Benevolence, and Integrity.

2.2 A Multi-Layered View of Trust in Digital Finance

While the Mayer et al. (1995) model addresses trust in the institution, the digital context introduces another critical layer: trust in the technology itself. Information Systems (IS) research makes a valuable distinction between interpersonal/organizational trust and technology trust (McKnight, Carter, Thatcher, & Clay, 2011).

Trust in Technology: IS scholars argue that users can develop trust in a technology based on their perceptions of its core attributes, independent of the organization providing it (Thielsch, Meeßen, & Hertel, 2018). Key components of technology trust include its perceived reliability (consistent and error-free performance), functionality (possessing the necessary features to accomplish a task), and helpfulness (providing effective user support) (Müller et al., 2020). A customer might lose trust in their bank's mobile app because it is unreliable or confusing, even while maintaining trust in the bank as an institution. Conversely, a seamless and secure app can bolster overall trust.

The 5Cs Model of Trust in Financial Services: Complementing these frameworks, a model developed specifically for financial services identifies five core dimensions of trust: Character-Competence, Congruence, Communication, Commitment, and Context (Ennew, Sekhon, & Kharouf, 2021). This model's dimensions of 'Character-Competence' and 'Congruence' (shared values) map closely onto Mayer et al.'s concepts of Integrity/Ability and Benevolence, respectively, reinforcing the validity of these core constructs in the financial domain.

2.3 Institutional Response and Crisis Communication

The bank's response after a scam is a critical moment that can either repair or shatter trust. To analyze this interaction, this study incorporates Situational Crisis Communication Theory (SCCT) (Coombs, 2020). Rooted in attribution theory, SCCT posits that the effectiveness of a crisis response depends on matching the communication strategy to the nature of the crisis and the degree of responsibility attributed to the organization (Coombs, 2007). SCCT identifies three crisis clusters based on perceived organizational responsibility: the *Victim Cluster* (minimal responsibility, e.g., natural disaster, product tampering), the *Accidental Cluster* (low responsibility, e.g., technical error), and the *Preventable Cluster* (strong responsibility, e.g., human error, organizational misconduct) (Coombs, 2020). In response, organizations can choose from four primary strategies:

Deny: Rejecting any connection to the crisis.

Diminish: Minimizing the organization's responsibility or the perceived damage.

Rebuild: Taking responsibility and offering apology and/or compensation to victims.

Bolster: Reminding stakeholders of the organization's past good works.

When a customer is scammed by a third party impersonating a bank, the bank is technically in the *Victim Cluster*. However, if the bank's response is perceived as dismissive or blaming, it can create a *second, preventable crisis* of customer relations. Analyzing the bank's response through the SCCT lens allows for a nuanced assessment of why certain communication strategies fail to rebuild trust and may, in fact, cause more reputational damage than the original scam. The implementation of emerging technologies like artificial intelligence (AI) and machine learning (ML) for the detection of fraud has been suggested as a measure to reduce the risk of scams and restore trust. Vieras et al. (2025) show that real-time fraud detection systems can greatly improve a bank's reputation and customer trust if properly implemented.

These technologies allow banks to identify anomalous patterns of transactions and act in time, hence avoiding possible losses. Nevertheless, these systems have to be supplemented by human monitoring in order to cope with shortcomings in contextual intelligence, according to Business Insider (2025). By contrast, ineffective use of AI instruments—lacking appropriate openness—may end up producing distrust through algorithmic blackboxing and false alarms (Zarsky, 2020). The financial sector has also tried predictive analytics and behavioral biometrics. The Deloitte Global Financial Services Report (2024) suggests that banks using these technologies experience 32% fewer customer churning due to fraud. Behavioral biometric software uses keyboard patterns, mouse activity, and device behavior to identify impostors in real time, which helps build greater trust. However, data privacy and surveillance ethical issues need to be carefully weighed to maintain the confidence of the masses. Not all customers react in the same manner to financial frauds. There have been demographic differences in trust reactions in terms of age, gender, income, and computer literacy. According to one report from the American Bankers Association (2025), one in five Americans have been a victim of a financial scam, and older adults are most likely to be victims with long-term loss of trust. This is corroborated by recent industry research, such as the Thales (2025) Digital Trust Index, which found that while banking is the most trusted sector overall, trust levels plummet to just 32% among Gen Z consumers, indicating a significant generational divide in perceptions of digital safety (Thales, 2025).

Younger customers, though also impacted, are more resilient and are more likely to claim compensation or change the service provider. Gender differences were also noted in a study conducted by Mahmood and Malik (2023), where female customers indicated more loss of trust and more perceived vulnerability due to scam experiences.

Cultural and geographical differences also add to the complexity of trust dynamics. In collectivist cultures, public revelation of scams creates stigma at a societal level, aggravating psychological and financial harm (Hofstede Insights, 2022). In contrast, in more individualistic cultures, customers would be more likely to go to war legally and claim compensation, transferring the onus to institutional responsibility. High-profile case studies offer significant insights into the implications of financial scams on institutional trust. The Wells Fargo scandal, where fake accounts were opened without customers' knowledge to fulfill sales quotas, created public outrage across the country and substantial loss of customer trust (Wikipedia, 2023). Likewise, in Australia, one family lost AUD 1.1 million through a single scam, and it created a national controversy regarding banks' fraud protection systems (News.com.au, 2024). These instances demonstrate the extent to which systemic factors and poor internal controls can reach to impact consumer confidence, public image, and regulatory oversight.

Regulatory action has also contributed to customer trust. Laws such as the General Data Protection Regulation (GDPR) in the EU and the Gramm-Leach-Bliley Act (GLBA) in the United States require financial institutions to implement robust data protection measures(Afzal 2024, Afzal 2024). Gupta and Shukla (2024) contend that these regulations boost consumer confidence by keeping banks on their toes and making them disclose any violations and act in anticipation. Additionally, the new Payment Services Directive (PSD2) in the EU strengthens protection against fraud by implementing Strong Customer Authentication (SCA), which has registered favorable correlations with trust indices in recent surveys (European Commission, 2023). Public awareness campaigns and customer educational programs have become primary methods of preventing financial fraud and regaining trust. As Featurespace (2024) identifies, customers who are informed regarding prevalent fraud strategies are less susceptible to becoming victims and are more likely to become loyal members of institutions with transparency and protection at their core.

Banks that spend money on fraud prevention training, both internally for employees and externally for customers, show a sense of ethical banking that has a positive effect on trust. New education programs such as the "Stop. Think. Connect." program have shown to be effective at raising scam awareness among at-risk populations (Cybersecurity Alliance, 2023). Financial scams also have macroeconomic effects. A report by the Financial Conduct Authority (FCA, 2024) quantified persistent fraud as likely reducing consumer spending, lowering savings rates, and reducing engagement in digital finance. This wider economic cost causes a feedback loop where lowered trust leads to lower banking activity, which in turn increases the sector's exposure to cybercrime. A number of nations, such as Canada and Singapore, have suggested public-private task forces to deal with these systemic issues at the policy level (OECD, 2023). Digital technologies like biometric authentication, blockchain technology, and tokenization have emerged as potential means of improving security and, indirectly, customer trust. A study by Chubb (2024) reveals that biometric technologies such as fingerprint and facial recognition provide better protection from identity theft. But the success of these technologies relies upon their availability and acceptance by users. Research by Shankar et al. (2021) finds that although biometric security is widely trusted, clients still require openness about data usage and storage policies. Blockchain technologies' application in Know Your Customer (KYC) processes and between-bank settlements has also helped reduce fraud, as per research by Finextra (2024). Through decentralized verification and real-time updates, blockchain minimizes the scope for information asymmetry, a key driver of fraud schemes. Consumer expectations have changed in recent years, such that trust is not only driven by security but also by ethical conduct, inclusivity, and social responsibility.

Accenture's Global Banking Consumer Study (2025) has discovered that 72% of consumers would change banks if they found out about unethical practices or poor data protection. This figure highlights the importance for banks to uphold high ethical standards and reflect their practice in customer value. Green banking practices and transparency policies in data have been discovered to be related to higher levels of trust among consumers, especially Gen Z consumers (Kantar, 2024). The incorporation of AI-powered chatbots and customer service interfaces is another influence on trust. While these tools offer efficiency and 24/7 support, a lack of personalization or inadequate responses can frustrate users and erode trust. According to PYMNTS (2024), 61% of consumers prefer human assistance when resolving fraud-related issues, indicating that technology must be used judiciously to complement, not replace, human interaction. Furthermore, the use of multilingual chatbot services has demonstrated to close gaps in trust between non-native speakers and underprivileged communities (Gomez & Lin, 2023). Restoring trust after a financial scam demands an all-embracing and multi-faceted effort. Compensation policy

is important. Feedzai (2023) states that 77% of customers anticipate complete compensation when they have been scammed, and not delivering this has a severe impact on long-term loyalty. Open dispute resolution mechanisms and prompt refunds are critical elements of a successful trust recovery plan. Customer satisfaction levels are much higher in regions where compensation is statutorily required (IMF, 2022).

Reputational risk also needs to be factored into banks' anti-fraud plans. The reputational loss from financial fraud is usually far greater than the monetary loss. 85% of bank leaders regard reputational damage as the worst impact of fraud, says KPMG's Global Banking Scam Survey (2025). Institutions, therefore, have to focus on proactive risk communication and crisis management planning. Scandinavian banks' case studies reveal that prompt public admission of violations and proactive engagement lead to faster trust rebound (Nordic Bank Report, 2023). Lastly, cross-segment coordination is critical for successful fraud prevention and trust maintenance. Financial institutions, regulators, law enforcement, and technology providers need to coordinate to exchange intelligence, create standardized procedures, and provide victim support programs. The Financial Stability Board (2024) asserts that concerted international effort is imperative to addressing the transnational dimension of cyber fraud. Regional partnerships like ASEAN Cyber Shield and the EU Digital Finance Package are instances of cooperative action against financial crime(Afzal 2024, Afzal 2024). Overall, the influence of financial scams on customer belief in banks is deep and far-reaching. Trust once lost is hard to rewin, and the effects reach farther than personal relationships to the larger financial system. Banks need to embrace a unified philosophy of technological innovation, compliance with regulations, customer literacy, emotional connection, and ethical behavior to reestablish and maintain trust in the new digital age. As fraud methods change at a fast pace and customers increasingly have high expectations, as well as ongoing adaptation, human-focused techniques, and watchfulness, are vital to protect both economic values and consumer trust. In addition to reinforcing customer confidence in the post-scam recovery period, banks should also pay attention to the efficacy of their communication strategy. Crisis communication literature suggests that timely, truthful, and coherent messaging during and after a crisis is essential. Banks that take a victim-oriented stance, accepting blame, showing empathy, and providing concrete remediation measures are more likely to maintain public trust, according to Coombs' Situational Crisis Communication Theory (SCCT) (Coombs, 2020). Conversely, institutions that react with ambiguous, protective comments stand to aggravate public outcry and customer defection. Public apology coupled with action, like refunds or service improvement, has been found to generate much higher levels of restoration of trust (Lee & Chung, 2022). Internal culture and employee training also have a foundational role in scam prevention and recovery. A report by Ernst & Young (2023) determined that banks with a robust culture of compliance, openness, and ethical leadership have fewer instances of internal fraud and are better at addressing external threats. Frontline staff empowered with fraud awareness training support quicker detection of suspicious behavior and consistent support to customers when there is a scam. Additionally, institutions with whistleblower programs and moral reporting mechanisms are more likely to anticipate systemic weaknesses prior to affecting customers. Besides institutional actions, financial literacy of customers is a vital preventive factor. World Bank (2024) studies provide evidence that nations with better financial literacy have considerably lower rates of online fraud and higher resilience in trust indicators following an incident.

Initiatives to enhance customer awareness of phishing cons, insecure online behavior, and password management have played an essential part in lowering vulnerability to fraud. Mobile banking applications that use gamified educational materials e.g., interactive risk situations or scam identification tests—have proven especially useful in reaching younger consumers (Patel & Huang, 2023). Another emerging topic of study is the influence of social media on attitudes toward trust following financial fraud. Social media sites are also public amplifiers, frequently relaying consumer complaints, scam warnings, and corporate reaction in real time. While this makes consumer advocacy more democratic, it also increases reputational risk. A viral tweet claiming negligence or abuse can trigger simultaneous account closings and regulatory investigations. A study by Thompson and Silva (2023) indicates that banks, through actively engaging and monitoring customers on social media, giving real-time assistance, correcting misinformation, and being publicly responsive can neutralize reputation loss and sustain trust even during crises. Cross-industry benchmarking is also emerging as a means for banks to learn from other industries with similar challenges in digital trust. For example, the online shopping sector, which also processes large volumes of digital payments and customer information, has led in frictionless authentication methods and real-time fraud dashboards, which banks are now embracing. Cross- industry workshops, shared security measures, and information exchanges among banking, insurance, and retail industries are increasingly promoted by cybersecurity councils (CSIS, 2023). These cross-industry approaches drive better standardization, enhance situational awareness, and offer shared

defense mechanisms against spoofing innovations. In addition, the application of user-centric design principles within digital banking interfaces is increasingly becoming a part of building proactive trust.

Easy-to-use UI elements, transparent alerts to detect suspicious behavior, and easy fraud-reporting options can enable customers to take action quickly and feel empowered. A Nielsen Norman Group usability study in 2024 found that consumers are more apt to report fraud or interact with security elements when the interface of the platform reduces cognitive load and employs plain language. Elderly and differently abled accessibility are also becoming a growing priority in inclusive trust design. Case law and consumer protection judgments are meanwhile establishing key precedents on holding scammers accountable. Recent court wins for victims of fraud in the UK and Canada have tipped the balance of blame more strongly in the direction of banks. Courts are now increasingly acknowledging the imbalance in power and information between banks and ordinary customers, forcing institutions to provide greater protection and take responsibility for systemic flaws (Financial Ombudsman Service, 2024).

These advances are not only redesigning institutional conduct but also reviving customer confidence by reaffirming the principle of justice and safeguard within the banking environment. Finally, scholarly developments in trust research are shifting to encompass emerging models that support digital complexities. Classic trust models such as Mayer, Davis, and Schoorman's model (1995) are being augmented to encompass algorithmic trust, platform integrity, and digital transparency as central constructs. Recent research by Han et al. (2025) has developed a Digital Financial Trust Model that incorporates affective, behavioral, and contextual dimensions specific to internet banking. Such theory-building is needed in order to inform future empirical studies, policy-making, and institutional design. Lastly, financial scams are a sophisticated and dynamic threat to customer trust in banks. Their effects are not only economic but emotional, reputational, and systemic. As digital innovation offers new technology for the detection and prevention of fraud, it also brings new expectations for transparency, responsiveness, and accountability. Banks that serve these expectations by technological, educational, and ethical means are more likely to be successful in restoring and maintaining trust. As the online world keeps changing, sustained research, collective action, and policy creativity will continue to be necessary to address the challenges presented by financial fraud and promote a secure and reliable banking system for everyone.

3. Methodology

3.1 Research Design

This study adopts a qualitative, exploratory research design to investigate the experiences of Pakistani consumers affected by bank-related scams. Given the complex and subjective nature of scam experiences including emotional, psychological, and behavioral dimensions qualitative methods are well-suited to capturing rich, contextualized insights (Creswell, 2013). Specifically, semi-structured interviews were employed to elicit detailed narratives from scam victims, allowing for in-depth exploration of their lived experiences.

3.2 Philosophical Perspective

The research was grounded in an interpretivist paradigm, emphasizing the co-construction of meaning between the researcher and participants (Lincoln & Guba, 1985). Interpretivism, sometimes called anti-positivism, is a research philosophy that asserts that social reality is not singular or objective but is rather shaped by human experiences and social contexts (Kivunja & Kuyini, 2017). It posits that knowledge in the social sciences cannot conform to the models of natural science because human experience involves features like emotions, values, and subjective understandings that cannot be objectively measured (Smith, 1993).

This paradigm rests on several key assumptions that make it uniquely suited for this study:

Ontology (Nature of Reality): Interpretivism holds a relativist ontology, believing that realities are multiple and socially constructed (Greener, 2008). The "reality" of a financial scam is not just the objective fact of a financial transaction, but the subjective experience of violation, shame, and fear as constructed by the victim within their specific social and cultural context.

Epistemology (Nature of Knowledge): Knowledge is seen as subjective and co-created through the interaction between the researcher and the participants (Kivunja & Kuyini, 2017). The goal is not to discover universal, generalizable laws, but to generate deep, contextualized understanding, what Max Weber termed *Verstehen*, or empathetic understanding of human action (Eliaeson, 2002).

Methodology: The interpretivist paradigm naturally leads to the use of qualitative methods like in-depth interviews. These methods allow the researcher to become embedded in the phenomena under investigation and to explore the rich, and often "messy," narratives of participants (Creswell, 2013). The focus is on understanding *how* and *why* individuals make sense of their experiences.

This paradigm is therefore perfectly suited for this study, as the impact of a financial scam is not an objective event but a deeply personal, emotional, and socially mediated experience. Understanding the 'lived experience' of shame, violation, and trust erosion requires a methodology that prioritizes subjective meaning over objective measurement. This approach acknowledges the inherently subjective and socially situated nature of scam experiences and seeks to understand them from the victims' perspectives. The research was grounded in an interpretivist paradigm, emphasizing the co-construction of meaning between the researcher and participants (Lincoln & Guba, 1985). This approach acknowledges the inherently subjective and socially situated nature of scam experiences and seeks to understand them from the victims' perspectives.

3.3 Sampling and Participants

A purposive sampling strategy was used to recruit participants who had directly experienced bank- related scams in Pakistan. The inclusion criteria required that participants had been targeted by, or fallen victim to, a financial scam involving impersonation of banks, phishing, fake online shopping platforms, or similar tactics. This approach ensured that the sample was information-rich and aligned with the study's objectives (Patton, 2002). The following Table 1 shows demographic information of respondents.

Table 1: Demographic Profile of Respondents and Nature of Scam Encountered

Respondent ID	Gender	Age	Profession	Type of Scam Encountered	Approximate Financial Loss
R1	Male	30	Medical Officer	OTP Phishing / Bank Impersonation	150,000
R2	Female	36	School Teacher	Fake Investment Application	50,000
R3	Female	28	Not Specified	OTP Phishing / Bank Impersonation	30,000
R4	Male	29	Not Specified	OTP Phishing / Bank Impersonation	Not Specified
R5	Female	50	Not Specified	Fake Utility Bill / Phishing Link	Full month's salary
R6	Female	Not Specified	Not Specified	Fake Online Shopping	15,000
R7	Male	Not Specified	Not Specified	OTP Phishing / Bank Impersonation	Large amount
R8	Male	Not Specified	Not Specified	Cryptocurrency Investment Scam	45,000
R9	Male	Not Specified	Not Specified	Prize Notification / Lottery Scam	30,000
R10	Male	Not Specified	Not Specified	Fake Loan Offer	25,000
R11	Male	Not Specified	Not Specified	Fake Government Support Program	10,000
R12	Male	Not Specified	Not Specified	Fake Job Offer	40,000
R13	Male	Not Specified	Not Specified	Fake Inheritance Scam	35,000
R14	Male	Not Specified	Not Specified	Fake Online Shopping	20,000
R15	Female	Not Specified	Not Specified	Fake Investment Application	50,000

Fifteen participants were recruited through personal networks, online forums, and referrals from consumer protection groups. Efforts were made to achieve diversity in age, gender, and geographic location to capture a broad range of experiences.

3.4 Data Collection

Data were collected through semi-structured interviews conducted in 2024. The interview guide was developed based on a review of relevant literature and the study's research questions. It covered six thematic sections: scam experience, emotional and psychological impact, institutional response, consumer vulnerability, post-scam behavior, and awareness and recommendations. The guide was intentionally designed to elicit rich narratives across the entire scam lifecycle from the initial

contact and victimization event to the emotional aftermath, the interaction with the financial institution, and subsequent changes in behavior. This holistic approach is central to the interpretivist goal of capturing a complete, contextualized experience rather than isolated data points. Interviews were conducted in Urdu or English, depending on participant preference, and lasted between 30 and 60 minutes. Interviews were conducted face-to-face or via secure online platforms, following COVID-19 safety protocols where applicable. All interviews were audio-recorded with participants' consent and subsequently transcribed verbatim.

3.5 Data Analysis

Thematic analysis was employed to analyze the interview data, following Braun and Clarke's (2006) six-phase framework: familiarization, coding, theme development, review, definition, and reporting. This method was chosen for its flexibility and suitability for identifying patterns within qualitative data. The analysis process began with multiple readings of the transcripts to ensure immersion in the data. An initial coding scheme was developed based on the interview guide and emergent insights. Coding was conducted manually and supported by spreadsheet tools (coding 6-18.csv), ensuring transparency and traceability. Codes were then grouped into higher-order themes and categories, reflecting patterns across the dataset. The coding process was iterative and reflexive, with constant comparison across interviews to refine themes. The resulting thematic structure was validated through peer debriefing and consultation with academic supervisors. The final themes included: scam experience (types and mechanisms), emotional and psychological impact, institutional response and trust, consumer vulnerability, and post-scam behavior and protection.

3.5 Trustworthiness and Rigor

To enhance the trustworthiness of the study, several strategies were employed. Credibility was supported through prolonged engagement with the data, peer debriefing, and member checking with selected participants. Transferability was facilitated by providing rich, contextualized descriptions of participants' experiences. Dependability was ensured through an audit trail documenting the coding and analysis process. Confirmability was supported by maintaining reflexive notes and acknowledging researcher subjectivities.

3.6 Limitations of Methodology

While the qualitative design enabled rich exploration of scam experiences, it also entails certain limitations. The use of purposive sampling limits the generalizability of findings to the broader population. Self-selection bias may have influenced the sample, as individuals more willing to discuss their experiences may differ from those who declined participation. Additionally, recall bias may have affected participants' accounts of past scam experiences. Despite these limitations, the study provides valuable insights into an under-researched phenomenon in Pakistan. The methodological rigor employed supports the credibility and relevance of the findings, contributing to both academic understanding and practical interventions for consumer protection.

4. Data Analysis

This section presents a detailed analysis of the study's findings in relation to the five Research Questions (RQs) and the existing body of literature. The analysis moves beyond descriptive results to interpret underlying patterns, connections between themes, and the socio-psychological mechanisms driving consumer experiences of bank-related scams in Pakistan. The thematic structure developed through Braun and Clarke's (2006) framework provides the basis for this analytic narrative.

4.1 RQ1 — Types of Bank-Related Scams Experienced by Consumers

The data reveal that Pakistani consumers are exposed to a wide variety of scam types, including OTP phishing, fake online shopping platforms, fake investment schemes, and impersonation of bank staff. OTP fraud and online shopping scams were the most frequently reported experiences across the sample. A notable analytic insight is that scam typology appears closely linked to emerging digital behaviors and trust gaps in new platforms. Younger participants who used online shopping platforms extensively were more exposed to fake store scams, while middle-aged users relying on mobile banking were more vulnerable to OTP scams. This reflects the findings of Hasan and Ali (2020), who argue that digital transformation in Pakistan is occurring faster than public understanding of its risks. Additionally, scam success was consistently linked to the use of trust cues scammers exploiting the logos, language, and scripts of trusted banks and platforms. Participants often cited

being deceived because "it looked exactly like my bank" or "the SMS had the bank's name." This underscores the sophistication of scams and highlights a systemic need for enhanced consumer education about digital impersonation (Cross et al., 2016).

4.2 RQ2 — Emotional and Psychological Impacts on Victims

Emotional impact emerged as one of the strongest and most consistent themes. Participants reported feelings of embarrassment, anger, helplessness, anxiety, and erosion of self-trust**.** Several experienced symptoms akin to post-traumatic stress, including sleeplessness and ongoing fear about using digital services. A particularly salient pattern is that emotional distress was compounded by the social stigma attached to being scammed. In the Pakistani cultural context, where financial competence is linked to personal and family honor (Hasan & Ali, 2020), admitting to victimization was seen as shameful. Participants often described not telling family members about the incident or feeling "too embarrassed to even complain." This dynamic aligns with findings by Button et al. (2014) and Whitty (2018), who note that the shame associated with financial scams leads to underreporting and delays in seeking help. In Pakistan, this effect may be amplified by cultural expectations**,** indicating a need for public discourse that destigmatizes victimization.

4.3 RQ3 — Institutional Response and Consumer Trust

Institutional response was highly inconsistent and emerged as a critical factor influencing long-term trust. Positive experiences (prompt action, empathetic handling) were rare but built trust. Negative experiences (dismissiveness, blaming the victim, lack of follow-up) were far more common and led to profound distrust. Many participants felt that banks prioritized limiting their liability over supporting the victim. This finding mirrors global patterns (Lichtenstein & Williamson, 2006), where institutional responses often fail to meet victims' emotional needs. In Pakistan, this perception of institutional indifference appears to be driving a broader crisis of trust in digital financial services. An important analytic insight is that pre-existing institutional trust acted as both a vulnerability and a recovery factor. High pre-existing trust made impersonation scams more effective. Conversely, when banks handled scam reports well, it helped repair trust post-scam. This suggests that trust operates as a double-edged dynamic in the scam experience lifecycle, a finding of significant conceptual value.

4.4 RQ4 — Consumer Vulnerabilities and Risk Factors

Vulnerability was shaped by a complex interplay of individual, contextual, and systemic factors:

Individual factors included low financial literacy, limited digital literacy, and personality traits (trustfulness, risk-seeking behavior).

Contextual factors included reliance on family advice, social isolation (for elderly victims), and urgency created by the scammer.

Systemic factors included lack of consumer education, inadequate institutional warnings, and limited enforcement against scammers.

The psychological tactics used by scammers, creating urgency, invoking authority, exploiting fear were found to be consistently effective across victim profiles. This supports Cross et al.'s (2016) argument that emotional manipulation is central to scam success. A key analytic finding is that vulnerability is dynamic and situational**,** not simply a fixed trait of certain groups. Participants who considered themselves digitally savvy still fell victim when caught in a moment of distraction or stress. This suggests that consumer protection efforts must move beyond targeting "high-risk groups" and instead focus on building situational resilience across all consumers.

4.5 RQ5 — Post-Scam Behavior and Protective Actions

Post-scam behaviors revealed a split pattern:

Positive adaptations included heightened vigilance, adoption of stronger passwords, multi-factor authentication, and greater skepticism toward unsolicited messages.

Negative adaptations included withdrawal from digital banking, avoidance of online purchases, and reduced engagement with financial services.

The data show that emotional recovery and institutional response strongly influenced which path victims took. Those who received supportive responses from banks were more likely to re-engage safely with digital services. Those who felt blamed or unsupported were more likely to disengage entirely. This aligns with Button and Cross (2017), who found that institutional support is a key moderator of post-scam consumer behavior. The Pakistani data suggest that without institutional trust repair, scam experiences can reverse gains in financial inclusion — an insight of considerable policy relevance.

4.6 Cross-Theme Connections

The analysis reveals important interactions between themes:

Institutional trust erosion magnifies emotional impact and drives maladaptive post- scam behaviors.

Consumer vulnerability interacts with scam typology — for example, highly trusting consumers were more vulnerable to impersonation scams, while digitally adventurous consumers were more exposed to fake online shopping scams.

Post-scam behaviors feed back into vulnerability — withdrawal from digital services may increase reliance on cash and informal channels, which have their own risks.

These cross-theme dynamics underscore the importance of integrated consumer protection strategies that address both technical fraud prevention and the emotional, relational, and behavioral dimensions of the scam experience.

4.7 Summary of Analysis

This analysis demonstrates that bank scams in Pakistan are not simply financial crimes but deeply social and emotional events with lasting impacts on consumer trust and behavior. Vulnerability is situational and dynamic, shaped by both individual and systemic factors. Institutional responses play a pivotal role in moderating the trajectory of post-scam adaptation. The study extends prior literature by foregrounding the cultural and relational dynamics of scam victimization in Pakistan and by illustrating how institutional trust operates as a double-edged factor in both scam susceptibility and recovery. These insights call for holistic, consumer-centered interventions that go beyond technical fixes to engage with the human dimensions of digital financial protection.

5. Results

This section presents the key findings of the study, based on thematic analysis of 15 in-depth interviews with Pakistani consumers who experienced bank-related scams. Thematic analysis followed Braun and Clarke's (2006) six-phase framework. The analysis identified six key themes:

- Scam Experience
- Emotional and Psychological Impact
- Institutional Response and Trust
- Consumer Vulnerability and Risk Perception
- Post-Scam Behavior and Protection
- Awareness and Recommendations

The results are organized thematically below, supported by representative participant quotes (R1, R2, etc.).

5.1 Scam Experience

Participants reported encountering a wide variety of scams. The most commonly experienced scams were OTP phishing**,** fake online shopping, and impersonation of bank staff**.** OTP fraud was particularly damaging, often resulting in direct financial losses after scammers impersonated bank officials to obtain verification codes. Participants emphasized how scammers created a false sense of urgency and used trust cues such as bank logos and professional-sounding language. As one participant explained: *"They called me pretending to be from my bank's fraud department… it sounded so real" (R5).* Fake online shopping scams were also prevalent, particularly among younger participants. Several respondents were drawn in by advertisements on social media platforms, paying for products that never arrived.

"I ordered from a Facebook page that looked like a real store… but it was fake" (R7).

5.2 Emotional and Psychological Impact

Victims experienced strong emotional responses, including embarrassment, anger, helplessness, and anxiety**.** Several participants reported losing confidence in their financial decision-making and feeling isolated. The sense of shame associated with victimization was particularly acute, discouraging some from disclosing the incident even to close family members. One participant shared: *"I didn't tell anyone because I felt so stupid" (R3).*

Others reported ongoing fear and anxiety when using digital financial services after the incident.

"I still get nervous when making online transactions now" (R12).

5.3 Institutional Response and Trust

Participants' experiences with banks' responses to scam reports were mixed**.** A minority of respondents reported professional and supportive handling of their complaints, but most felt that banks were dismissive or blamed them for the loss**.**

"The bank just told me it was my fault for giving out the OTP, even though they never warned me clearly" (R8).

Such interactions led to a profound erosion of trust in banks' ability or willingness to protect customers. Participants expressed disappointment that banks prioritized their own liability concerns over supporting victims.

"They were polite but basically said: you lost the money, nothing we can do" (R10).

5.4 Consumer Vulnerability and Risk Perception

Vulnerability to scams was shaped by low financial literacy**,** limited digital literacy**,** and psychological factors such as trustfulness and emotional susceptibility. Many participants admitted they were unaware that banks never ask for OTPs or personal details via phone.

"I honestly thought the call was from my bank… I didn't know this could be a scam" (R5).

In some cases, social isolation or lack of peer consultation increased risk, particularly for older participants. Scammers also skillfully used emotional manipulation — invoking authority or urgency — to bypass rational scrutiny.

"They made it sound like I would lose my account if I didn't act immediately" (R9).

5.5 Post-Scam Behavior and Protection

After experiencing a scam, many participants adopted heightened caution and improved security practices, such as stronger passwords and greater skepticism toward unsolicited communications.

"Now I never give out any information on the phone, no matter who it is" (R6).

However, some participants responded by withdrawing from digital services**,** avoiding online banking or mobile payments altogether.

"I stopped using mobile banking completely… it's not worth the risk" (R14).

Such avoidance can undermine financial inclusion and suggests that supportive institutional responses are critical for helping victims rebuild trust.

5.6 Awareness and Recommendations

Participants strongly advocated for more proactive consumer education by banks and regulators. There was a clear consensus that most scams could be avoided if customers were better informed.

"If they had just sent a message warning about these calls, I would never have fallen for it" (R4).

Suggested recommendations included awareness campaigns**,** regular SMS alerts**,** and clearer onboarding about fraud risks**.** Participants also called for stronger action against scammers and improved institutional transparency. *"Banks should do more to protect us — not just blame us after it happens" (R11).*

6. Conclusion

The results reveal that Pakistani consumers are exposed to sophisticated scams that exploit trust gaps and systemic vulnerabilities. Emotional and psychological impacts are severe and often compounded by institutional responses that fail to adequately support victims. Consumer vulnerability is dynamic, situational, and shaped by both individual and systemic factors. Post- scam behaviors range from adaptive caution to maladaptive withdrawal. Participants clearly desire more proactive consumer education and stronger institutional protections.

The study's findings underscore that addressing bank scams in Pakistan demands a holistic, multi- stakeholder approach. This approach must be grounded in a deep understanding of trust, recognizing that it is built on perceptions of ability, benevolence, and integrity. Banks must enhance consumer education and improve institutional responses; regulators must lead public awareness efforts and enforce stronger standards; consumers must be empowered to protect themselves; and all actors must collaborate to build a safer, more trusted digital financial environment. By implementing these recommendations, Pakistan can make significant strides toward reducing scam victimization, supporting affected consumers, and strengthening trust in its digital banking ecosystem. Ultimately, this study demonstrates that the erosion of consumer trust following financial scams is not a simple outcome of financial loss, but a complex process driven by a perceived failure of institutional benevolence and integrity, a crisis in communication, and culturally amplified psychological distress, ultimately threatening the very foundations of Pakistan's digital financial inclusion goals.

REFERENCES

Accenture. (2025). Global banking consumer study.

ADB. (2024). Cybercrime trends in Asia-Pacific digital finance. Asian Development Bank.

Afzal, J. (2024). An Overview of Digital Law. Implementation of Digital Law as a Legal Tool in the Current Digital Era. J. Afzal. Singapore, Springer Nature Singapore: 1-21.

Afzal, J. (2024). Best Practice of Digital Laws and Digital Justice. Implementation of Digital Law as a Legal Tool in the Current Digital Era. J. Afzal. Singapore, Springer Nature Singapore: 95-120.
Afzal, J. (2024). Development of Legal Framework of Digital Laws. Implementation of Digital Law as a Legal Tool in the Current Digital Era. J. Afzal. Singapore, Springer Nature Singapore: 139-154.
Afzal, J. (2024). Execution of Bilateral Digital Law. Implementation of Digital Law as a Legal Tool in the Current Digital Era. J. Afzal. Singapore, Springer Nature Singapore: 79-93.
Afzal, J. (2024). Future of Legal Tools and Justice. Implementation of Digital Law as a Legal Tool in the Current Digital Era. J. Afzal. Singapore, Springer Nature Singapore: 155-177.
Afzal, J. (2024). Implementation of digital law as a legal tool in the current digital Era, Springer.
Afzal, J. (2024). Legal Challenges Regarding Digital Operations. Implementation of Digital Law as a Legal Tool in the Current Digital Era. J. Afzal. Singapore, Springer Nature Singapore: 23-45.
Afzal, J. (2025). "Comparative Review on Acceptance of Digital Evidence within the Legal Frameworks of Pakistan and China." International Journal of Law and Legal Advancement 1(1).
Afzal, J., C. Yongmei, A. Fatima and A. Noor (2024). "Review of various Aspects of Digital Violence." Journal of Engineering, Science and Technological Trends 1(2).
Alashwali, E. S., Khan, S., & Yusof, S. (2024). Emotional consequences of financial fraud: A qualitative perspective. Journal of Behavioral Finance, 25(1), 33–47.
Ali, F., & Ahmed, S. (2022). Digital fraud in Pakistan: Trends and consumer protection challenges. Journal of Financial Crime, 29(2), 521–534.
American Bankers Association. (2025). Annual report on consumer fraud and trust.
Bouveret, A. (2018). Cyber risk for the financial sector: A framework for quantitative assessment. IMF Working Papers, WP/18/143.
Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101.
Business Insider. (2025). How AI is transforming fraud detection in banks. https://www.businessinsider.com
Button, M., & Cross, C. (2017). Cyber frauds, scams and their victims. Routledge.
Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. Security Journal, 27(1), 36–54.
Chawla, D., Bansal, A., & Kaushik, R. (2023). Consumer vulnerability and trust loss in digital finance. International Journal of Consumer Studies, 47(2), 123–139.
Chubb. (2024). Biometric security in financial services: Trust and adoption. Chubb Insurance Insights.
Coombs, W. T. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. Corporate Reputation Review, 10, 163–176.
Coombs, W. T. (2020). Ongoing crisis communication: Planning, managing, and responding (5th ed.). Sage Publications.
Creswell, J. W. (2013). Qualitative inquiry and research design: Choosing among five approaches (3rd ed.). Sage Publications.
Cross, C., Richards, K., & Smith, R. G. (2016). Improving the prevention and reporting of cyber fraud. Trends & Issues in Crime and Criminal Justice, 508, 1–14.
CSIS. (2023). Cross-sector cybersecurity collaboration: Financial, insurance, and retail perspectives. Center for Strategic and International Studies.
Cybersecurity Alliance. (2023). Stop. Think. Connect.: Awareness campaign report.
DeLiema, M. (2018). Elder fraud and financial exploitation: Application of routine activity theory. The Gerontologist, 58(4), 706–718.
Deloitte. (2024). Global financial services fraud outlook. Deloitte Insights.
Eliaeson, S. (2002). Max Weber's methodologies: Interpretation and critique. Polity.
Ennew, C., Sekhon, H., & Kharouf, H. (2021). Introducing a composite measure of trust in financial services. The Service Industries Journal, 41(13-14), 869-892.
Ernst & Young. (2023). Global banking risk culture and compliance study.
European Commission. (2023). PSD2 and the evolution of strong customer authentication in the EU. https://ec.europa.eu
FATF. (2023). Money laundering risks from digital fraud channels. Financial Action Task Force. https://www.fatf-gafi.org
FCA. (2024). Economic cost of persistent financial fraud. Financial Conduct Authority.
Featurespace. (2024). Fraud education and trust in banking institutions.
Federal Investigation Agency. (2022). Annual cybercrime report. Islamabad: FIA.
Federal Trade Commission. (2023). Consumer Sentinel Network data book 2022.
Feedzai. (2023). Trust recovery and compensation expectations in digital fraud.
Financial Conduct Authority. (2023). Financial Lives Survey 2022.
Financial Ombudsman Service. (2024). Recent case decisions on bank responsibility in scams.
Financial Stability Board. (2024). Cyber fraud and international cooperation frameworks.
Finextra. (2024). Blockchain and fraud reduction in KYC. https://www.finextra.com
Gallup Pakistan. (2022). Public trust in banking institutions survey. Islamabad, Pakistan: Gallup Pakistan.
Gomez, L., & Lin, Y. (2023). Language and equity in fintech trust: The chatbot gap. Journal of Digital Communication, 14(3), 78–93.
Greener, S. (2008). Business research for shocking students. Ventus Publishing.
Gupta, R., & Shukla, M. (2024). Customer perceptions of digital trust in Indian banks. Journal of Financial Services Research, 62(1), 45–60.

Han, S., Zhou, T., & Wang, L. (2025). A digital financial trust model for modern banking. Journal of Internet Banking and Commerce, 30(1), 1–22.
Hasan, M., & Ali, F. (2020). Consumer vulnerability to online fraud in Pakistan: Challenges and responses. Journal of Consumer Protection and Policy, 43(1), 57–74.
Hofstede Insights. (2022). Collectivist culture and trust recovery in financial services. https://www.hofstede-insights.com
IMF. (2022). Compensation regulations and fraud resolution systems. International Monetary Fund.
Kantar. (2024). Green banking and trust among Gen Z consumers. Kantar Group.
Karandaaz Pakistan. (2022). Digital financial services consumer experience survey. Islamabad, Pakistan: Karandaaz.
Kim, H., Park, J., & Lee, S. (2021). Phishing, identity theft, and consumer trust in online banking: A systematic review. Cybersecurity & Finance, 26(4), 89-105.
Kivunja, C., & Kuyini, A. B. (2017). Understanding and applying research paradigms in educational contexts. International Journal of Higher Education, 6(5), 26-41.
KPMG. (2025). Global banking scam survey.
Lee, J., & Chung, N. (2022). The role of apology and action in crisis communication and trust recovery. Journal of Public Relations Research, 34(2), 112-130.
Lee, M. K. O., & Turban, E. (2001). A trust model for consumer internet shopping. International Journal of Electronic Commerce, 6(1), 75–91.
Lichtenstein, S., & Williamson, K. (2006). Understanding consumer adoption of internet banking: an interpretive study in the Australian banking context. Journal of Electronic Commerce Research, 7(2), 50–66.
Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. Sage.
Mahmood, A., & Malik, S. (2023). Gender differences in trust perceptions after financial scams. Journal of Gender and Finance, 5(1), 45-60.
Marwick, A., & Lewis, R. (2022). Social impacts of digital fraud. Data & Society.
Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of Management Review, 20(3), 709–734.
McKnight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in information technology: A new set of constructs. The DATA BASE for Advances in Information Systems, 42(2), 35-57.
Müller, S. R., Meeßen, S. M., & Thielsch, M. T. (2020). Trust in management information systems. In HCI in Business, Government and Organizations. HCIBGO 2020. Lecture Notes in Computer Science (Vol. 12204). Springer.
News.com.au. (2024). Australian family loses $1.1 million in banking scam.
Nordic Bank Report. (2023). Crisis communication and trust rebound in Scandinavian banking.
OECD. (2023). Public-private partnerships for financial crime prevention.
Patel, V., & Huang, Y. (2023). Gamification in financial literacy education for young adults. Journal of Financial Education, 49(1), 88-105.
Patton, M. Q. (2002). Qualitative research and evaluation methods (3rd ed.). Sage.
PTA. (2023). Annual report 2022-23. Pakistan Telecommunication Authority.
PYMNTS. (2024). The role of human assistance in fraud resolution.
Rosenzweig, S., et al. (2023). Empathy in institutional responses to fraud. Journal of Consumer Psychology, 33(4), 550-565.
SBP. (2021). National financial literacy program report. State Bank of Pakistan.
SBP. (2022). Annual performance review of the banking sector. State Bank of Pakistan.
Schoorman, F. D., Mayer, R. C., & Davis, J. H. (2007). An integrative model of organizational trust: Past, present, and future. Academy of Management Review, 32(2), 344–354.
Shankar, A., et al. (2021). Biometric authentication and consumer trust. Journal of Retailing and Consumer Services, 61, 102581.
Smith, J. K. (1993). After the demise of empiricism: The problem of judging social and educational inquiry. Ablex.
State Bank of Pakistan. (2022). Guidelines on digital fraud prevention.
Thales. (2025). 2025 Digital Trust Index – Consumer Edition.
The Times. (2025). UK fraud losses reach record levels.
Thielsch, M. T., Meeßen, S. M., & Hertel, G. (2018). Trust and distrust in information systems at the workplace. PeerJ, 6, e5483.
Thompson, R., & Silva, M. (2023). Social media, crisis communication, and institutional trust. Public Relations Review, 49(5), 102345.
Vieras, T., et al. (2025). Real-time fraud detection using AI: A trust perspective. IEEE Transactions on Dependable and Secure Computing.
Waliullah, et al. (2025). Cyber threats in online banking: A review.
Whitty, M. T. (2018). The emotional and psychological impact of online fraud. In The Cambridge Handbook of Psychology and Economic Behaviour. Cambridge University Press.
Wikipedia. (2023). Wells Fargo account fraud scandal.
World Bank. (2021). Pakistan: COVID-19 and the digital finance ecosystem.
World Bank. (2024). Global financial literacy and fraud report.
Yongmei, C. and J. Afzal (2023). "Impact of enactment of ‘the prevention of electronic crimes act, 2016’as legal support in Pakistan." Academy of Education and Social Sciences Review 3(2): 203-212.
Zarsky, T. Z. (2020). The trouble with algorithmic decisions: An analytic review. Philosophy & Technology, 33, 405-423.

Declaration

Conflict of Study: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Author Contribution Statement: F.A, J.H, B.U and J.A conceived the idea and designed the research; Analyzed and interpreted the data, and wrote the paper.

Funding Statement: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Availability of Data and Material: Data will be made available by the corresponding author on reasonable request.

Consent to Publish: All authors have agreed to publish this manuscript in the International Journal of Discovery in Social Sciences.

Ethical Approval: Ethical approval for the study was obtained from the ethics committee/board of Lahore Garrison University, Pakistan.

Consent to Participate: Informed consent was obtained from all participants before data collection. Participants were assured of confidentiality and the voluntary nature of their involvement. All data were anonymized during transcription and stored securely. Sensitive topics were handled with care, and participants were provided with contact information for support services if needed.

Acknowledgment: The author is thankful to the editor and reviewers for their valuable suggestions to improve the quality and presentation of the paper.

Author(s) Bio / Authors' Note

Faisal Akbar:

F.A *is a PhD scholar at Lahore Garrison University, Pakistan. Email* faisalakbarphd@gmail.com

Junaid Hussain:

J.H *is a PhD scholar at Lahore Garrison University, Pakistan. Email:* junaidhussain7771@outlook.com

Babar Usman:

B.U *is a PhD scholar at Lahore Garrison University, Pakistan. Email:* babarusman141@gmail.com

Dr. Jamil Afzal:

J.A *has been involved in research and teaching for various National and International institutes for more than ten years. He is the author of three books and a contributor/associate editor in two others, as well as the author of various high-ranking journal articles; he has also participated in reputable international conferences. Dr. Jamil Afzal founded Contemporary Theory of Digitalization (CToD); CToD consists of three levels, including 3Ds at the first and 5Ds at the second level, and 7Ds at the third level. He is the Principal Ethical Editor at the International Research and Publishing Academy (iRAPA) for its associated journals, and the academic editor of the PLOS ONE Journal, as well as a peer reviewer for various international journals.. Email:* sirjamilafzal@gmail.com

Appendix

Interview Guide

The Impact of Financial Scams on Consumer Trust in the Banking Sector: A Qualitative Analysis

Section A: Scam Experience (3 Questions)

1. Can you briefly describe a financial scam incident you or someone close to you experienced?
2. How did you first realize it was a scam?
3. What immediate steps did you take after discovering the scam?

Section B: Emotional and Psychological Impact (3 Questions)

1. How did the experience affect your emotional or mental well-being?
2. Did it change your sense of personal security or trust in others?
3. Have you discussed your emotional response with anyone (family, therapist, etc.)?

Section C: Institutional Response and Trust (4 Questions)

1. How did your bank respond when you reported the scam?
2. Did the bank's response impact your trust in them? Why or why not?
3. What could they have done differently to support you?
4. Did you change banks or limit your use of financial services after the incident?

Section D: Consumer Vulnerability and Risk Perception (3 Questions)

1. What do you believe made you or others vulnerable to the scam?
2. Do you think age, education, or financial literacy played a role?
3. What warning signs do you now recognize that you missed before?

Section E: Post-Scam Behavior and Protection (3 Questions)

1. Have you changed your behavior in using online or mobile banking platforms?
2. What security measures have you adopted since the scam (e.g., MFA, strong passwords)?
3. Do you feel more cautious or confident when managing your finances now?

Section F: Awareness and Recommendations (4 Questions)

1. Have you attended any fraud awareness or financial literacy sessions?
2. Do you think such programs could help prevent scams? How?
3. What advice would you give others to avoid becoming victims?
4. What should financial institutions do to better protect consumers from scams?

Section G: Banking Perspective (5 Questions)

1. What steps did your bank take to investigate the scam incident?
2. Did your bank offer any compensation or support after the scam? If yes, was it satisfactory?
3. Were you educated by your bank about common financial scams before or after the incident?
4. How would you rate the bank's customer service and communication during the incident?
5. What do you think banks should do differently to identify and prevent scam transactions in real-time?