



Ghulam Muhammad¹

¹Founder & Business Manager at GM Enterprises, Faisalabad, Pakistan. Master of Business Administration (MBA) from Virtual University of Pakistan, Email: orexomartllc@gmail.com

KEYWORDS	ABSTRACT
Digital Banking Fraud; Consumer Protection; Financial Regulation; Institutional Response; Pakistan	This growing trend of digital banking in Pakistan has improved the ease, accessibility, and efficiency of financial services, but has also introduced new challenges for consumers. Accurate and credible information about digital banking fraud, such as phishing, social engineering, impersonation, unauthorized transactions, and credential theft, has become a significant threat for financial institutions and regulators. This study aims to explore the issue of digital banking fraud and consumer protection in the context of regulatory challenges and institutional responses in Pakistan. This study uses qualitative descriptive research design and secondary documents as data sources. Data were gathered from circulars of the State Bank of Pakistan, regulatory policies, reports of the institutions, policy papers, academic journals and other relevant international reports. Qualitative document analysis and thematic analysis were used to analyse the collected material. The four main themes are highlighted: the growing complexity of digital banking fraud; the challenges faced by regulators in implementing their measures; the enhancement of consumer protection and redress measures; and a need for coordinated institutional action. Findings from the analysis reflect that Pakistan has been gradually improving its regulatory framework by introducing digital-fraud reporting, strengthening security measures, introducing consumer protection measures, introducing complaint-handling systems, and introducing provisions to provide compensation for consumers under specific circumstances. The effectiveness of these measures, however, relies on institutional capacity, level of regulatory enforcement, consumer awareness, timely reporting of fraud, easy access to redress mechanisms, and the coordination of relevant stakeholders. The study makes it clear that digital banking fraud is not a technology or a consumer problem, but a multi-faceted consumer-protection and regulatory-governance issue. To build trust and ensure safer digital banking in Pakistan, an ecosystem-based approach is critical that will include the role of regulators, financial institutions, payment providers, telecom actors and consumers.
ARTICLE HISTORY Date of Submission: 19-02-2026 Date of Acceptance: 26-03-2026 Date of Publication: 30-03-2026	 2026 Journal of Social Research Development
Correspondence	Ghulam Muhammad
Email:	orexomartllc@gmail.com
DOI	https://doi.org/10.59075/jsrd.v7i1.571
Volume/Issue	7(1), 2026, 199-218

Introduction

Digital banking has changed the financial services landscape around the globe by quickly expanding the way financial services are delivered and consumed. The speed, access and convenience of financial transactions has been enhanced with mobile banking applications, internet banking, digital wallet, online fund transfer and electronic payment systems. Digital financial services have the potential to bring benefits to financial inclusion, with a focus on lowering transaction fees and increasing access to formal financial services, especially in developing economies (World Bank, 2020). At the same time, the growing digitization of financial transactions has opened up new risks for consumers against which to protect themselves, such as phishing, identity theft, social engineering, unauthorized transactions, mobile application fraud, and other types of cyber-enabled financial crime (CGAP, 2017; World Bank, 2017). Thus, digital banking fraud has become a matter of cyber security, but also of financial consumers' safeguarding, institutional responsibility and regulatory governance.

Digitalisation of financial services has gained tremendous momentum in Pakistan and over the years, financial institutions have increasingly embraced mobile and web banking platforms. This has broadened access to financial services, but has also grown consumers' vulnerability to digitally enabled fraud. The State Bank of Pakistan (SBP) has identified social engineering, fake calls and other digital banking frauds as serious issues and banks and microfinance banks are mandated to report information for attempted and successful frauds systematically (State Bank of Pakistan [SBP], 2021). In 2022, SBP enhanced these reporting obligations by stipulating that banks and microfinance banks should report a fraud or scam that was detected via call centre, email or letters sent to them, or identified internally (SBP, 2022). Such measures signal enhanced regulatory focus on detecting patterns of fraud and boosting institutional capability to address digital financial risks.

The dimension of consumer protection from digital banking fraud is especially significant as consumers' financial losses can lead to a loss of trust in formal financial institutions and a reduction in their willingness to use digital banking and financial services. The World Bank (2017) points out that it can be especially damaging when fraud and unauthorized transactions are directed at consumers with limited prior experience in financial services or digital technologies. Likewise, World Bank's digital finance framework recognizes that fraud, data misuse, technology vulnerabilities, and poor complaint-resolution systems are all significant consumer risks of digital financial services (World Bank, n.d.). Such risks illustrate that consumer protection can't be achieved through technological security alone, but also needs clear institutional accountability, robust complaint procedures, prompt responses, equitable remedies and regulation.

These challenges have been addressed by the regulatory framework in Pakistan, which has gradually adapted to meet them. SBP's efforts to improve the security of digital banking products and services call on banks and microfinance banks to enforce certain security controls and put in place measures to combat fraudulent activities (SBP, 2023a). Importantly, the framework also stipulates that affected customers shall receive compensation in certain cases in which the required

controls are not implemented (SBP, 2023a). In addition, SBP created a Consumer Protection Department to provide enhanced supervision over the consumer protection, redress of complaints and the assessment of conduct risks within the financial sector (SBP, 2023b). In addition, the launch of the Sunwai customer complaint management service is another sign of the institutionalisation of support for consumers to submit and track complaints (SBP, 2023c).

However, digital banking fraud challenges are ongoing in the regulatory and institutional space. Fraud techniques are constantly evolving, making it challenging for regulators and financial institutions to keep up with their work to prevent or remediate fraud. Consumer awareness, authentication mechanisms, data security, inter-institutional coordination, fraud reporting and timely dispute resolution are still significant characteristics of digital financial consumer protection (CGAP, 2017; World Bank, 2020). Accessible and timely recourse mechanisms are especially important, as they enable consumers to exercise their rights and enable regulators to learn about systemic issues that need to be addressed (World Bank, n.d.).

In this context, the current study explores the issue of fraud and protection in digital banking in Pakistan using a qualitative study on regulatory and institutional issues. The research employs secondary documentary methods where regulatory documents, institutional reports, policy documents and relevant academic literature are used to investigate the significant forms and patterns of the digital banking fraud, the challenges faced by the regulators and institutions and the consumer protection mechanisms adopted by relevant institutions. This study aims to contribute to the understanding of the tension between the growth of digital financial services and shielding consumers from the new versions of financial fraud in Pakistan's digital banking regulatory environment.

Problem Statement

While digital banking has provided significant opportunities for financial inclusion, convenience, and efficient financial transactions in Pakistan, it has also introduced new and evolving forms of digital banking fraud that are posing significant challenges to both consumers and financial institutions. Phishing, social engineering, identity theft, unauthorized transactions, fraudulent calls, text messages and other frauds using electronic devices impose financial and non-financial risks on consumers and new burdens on banks and regulators. The State Bank of Pakistan has taken steps towards regulating digital banking security, reporting of frauds, customer protection, and address complaints, but there are concerns about the effectiveness and application of these processes. Several issues arise regarding the effectiveness of current consumer protection measures, which are complicated by the changing nature of digital fraud, differences in consumer awareness and sensitivity, the role of institutional coordination, the availability of consumer protection reporting and the availability and timeliness of redress. Furthermore, the prevailing discourse on cybersecurity and the prevention of fraud or the discourse on financial inclusion are currently prevailing and comparatively less efforts are dedicated towards analyzing financial banking fraud as a combined regulatory, institutional and consumer protection issue in Pakistan. Thus, a systematic qualitative study of the patterns and modalities of digital banking fraud, regulatory and

institutional issues of tackling digital banking fraud and consumer response and protection mechanisms to digital banking fraud is required.

Scope of the Study

This study focuses on Pakistan to limit the scope of the study regarding digital banking fraud and consumer protection, especially regulatory challenges and institutional responses. This study is dedicated to frauds in the context of digital banking channels – internet banking, mobile banking, electronic transactions and digital banking services. It explores the regulatory and institutional environment set up by the relevant authorities including the State Bank of Pakistan and the role and action of banks and other relevant financial institutions. The results of this study are based on secondary data, such as legislation, SBP circulars and regulations, institutional reports, policy documents, official publications, academic research and credible reports on digital banking fraud and consumer protection. Analysis focuses on fraud prevention, detection, reporting, complaint handling, consumer redress, institutional accountability and regulatory implementation. It is not based on primary interviews or surveys of banking customers, employees, regulators or fraud victims and does not seek to quantify the extent or financial impact of digital banking fraud. The study is therefore designed to provide a qualitative and documentary evaluation of the current regulatory framework and institutional reaction, not an empirical analysis of actual experiences of consumers.

Significance of the Study

The study holds special importance as effective consumer protection is crucial to build trust and confidence in the growing digital banking landscape of Pakistan. Through this study, the regulation and institutional aspects of digital banking fraud can be studied, which can help in developing a comprehensive understanding of the challenges of consumer protection in the digital financial landscape. The results could be relevant to regulators, especially as respects the need for further strengthening of the various mechanisms of fraud prevention, reporting, complaints handling and redress. The study can raise awareness in banks and financial institutions about the responsibilities of institutions regarding fraud detection, customer authentication, communication, and dispute resolution and also recurring issues of these areas. The study can also be useful in contributing to academia by linking the literature on digital banking fraud with financial consumer protection and regulatory governance in the Pakistani context. Consumers and consumer protection stakeholders may find it useful to know about institutional arrangements and legal provisions as they become aware of fraud and may wish to go for redress. On a broader scale, the study could provide useful guidance to the creation of a more secure and responsible digital banking ecosystem, emphasizing the need for coordinated regulatory oversight, institutional accountability, consumer awareness, and effective tools to address digital banking fraud.

Research Objectives

The research objectives are as follow:

- To examine the emerging forms and patterns of digital banking fraud in Pakistan and their implications for consumer protection.
- To critically analyze the regulatory and institutional challenges faced by Pakistani authorities and financial institutions in preventing, detecting, and responding to digital banking fraud.
- To evaluate the institutional responses and consumer protection mechanisms adopted by banks, regulators, and other relevant stakeholders in addressing digital banking fraud in Pakistan.

Research Questions

Following are the research questions:

- What are the major forms and patterns of digital banking fraud in Pakistan, and how do they affect consumers?
- What regulatory and institutional challenges hinder the effective prevention, detection, and response to digital banking fraud in Pakistan?
- How do banks, regulatory authorities, and other relevant institutions respond to digital banking fraud, and what consumer protection mechanisms are available to affected customers?

Research Design and Research Methodology

Research Design

The qualitative descriptive research design is used to explore the issues of digital banking fraud and consumer protection in Pakistan, specifically regulatory issues and institutional response. A qualitative design is suitable for the study because it aims to describe and interpret the nature of the existing regulatory provisions, institutional practices, consumer protection mechanisms and documented challenges, rather than measure relationships statistically. In regard to social and institutional phenomena, qualitative research helps the researcher to explore and describe systematically the interpretations that are found in textual and documentary evidence (Creswell & Poth, 2018). The design in the present study allows for a detailed analysis of the digital banking fraud depicted in regulatory documents and relevant institutions' reactions to the new fraud risks.

The study has no primary data as such. This is an appropriate approach as the digital-banking regulatory ecosystem in Pakistan is documented in the form of laws, regulatory circulars, policy documents, institutional reports, banking guidelines, complaint management systems and other public documents. For instance, the State Bank of Pakistan (SBP) has taken certain initiatives regarding the security of digital banking, reporting of fraud, protection of customers, and institutional controls. The digital banking fraud/attempted fraud information was requested from

banks and microfinance banks as part of SBP's instructions of 2021; and the security controls and provisions regarding compensation in cases where security controls were not implemented were contained in SBP's measures of 2023 (State Bank of Pakistan [SBP], 2021, 2023).

The research design thus offers a coherent approach in which three dimensions are analyzed: (a) forms and patterns of digital banking fraud, (b) regulatory and institutional challenges, and (c) institutional responses and consumer-protection mechanisms. Rather than treating fraud merely as a technological or cybersecurity problem, the study approaches it as a broader governance and consumer-protection issue involving banks, regulatory authorities, financial institutions, complaint-resolution mechanisms, and consumers.

Research Approach

The study takes qualitative interpretative approach. Where there are meanings, priorities, assumptions, responsibilities, and understandings of consumer protection within the regulatory documents and institutional responses, an interpretive orientation is appropriate. The research is not designed to determine the statistical prevalence or cause and effect relationships between evidence in the dossiers; it attempts to reveal patterns and themes in the documentary evidence.

The qualitative approach also enables comparison with the actual institutional responses to regulation. For example, SBP has introduced measures that demand banks and microfinance banks to have better security measures in place for digital banking and has put mechanisms in place to report digital fraud. SBP's consumer-protection framework also offers avenues for complainant to seek remedy. The documents are significant sources of data on the formal concept and implementation of consumer protection in the banking system in Pakistan.

Sources of Data

The study uses secondary documentary data collected from credible and authoritative sources. The principal sources include:

- State Bank of Pakistan (SBP) circulars, notifications, regulatory frameworks, policy documents, and consumer-protection materials;
- Government of Pakistan legislation and relevant legal/regulatory documents;
- Reports and publications of relevant financial and regulatory institutions;
- Banking and financial-sector reports;
- Reports concerning digital banking fraud, cybersecurity, and consumer protection;
- Peer-reviewed academic journal articles and books;
- Reports published by international organizations concerning digital financial services and consumer protection;

- Credible newspaper and professional reports where they provide documented information concerning digital banking fraud and institutional responses.

In this regard, special focus will be placed on official documents of the SBP as it contains first-hand information on the action taken by the SBP in the regulatory sphere. For instance, SBP's instructions for the security of digital payments in 2018 focused on vulnerability assessment, alerts for transactions, customer awareness and security of digital banking channels. Likewise, the 2022 reporting rules now broadened the reporting of digital frauds and scams beyond their call-center reports to fraud reported via other channels or identified by banks themselves.

Data Collection Procedure

Documentary research will be used systematically to collect data. Documentary research refers to a method of identifying, selecting, reading and interpreting documents that are relevant to the phenomenon under investigation. Documents can be used as important sources of qualitative data when they are explored and analysed systematically, as Bowen (2009) says.

The researcher will initially determine the relevant documents, which directly meet the three overall research goals. Then documents will be reviewed based on their relevance, credibility, institutional authority, date and connection with Pakistan's digital banking fraud and consumer protection. These documents will then be themed.

The documentary corpus will broadly be divided into four groups:

1. **Regulatory documents:** SBP circulars, regulations, guidelines, and policy frameworks;
2. **Institutional documents:** banking-sector reports, complaint-management information, and institutional responses;
3. **Legal and policy documents:** relevant legislation, rules, and government policy materials;
4. **Academic and contextual literature:** peer-reviewed studies and credible reports addressing digital fraud, cybersecurity, financial consumer protection, and digital banking.

Sampling Technique

Documentary sources will be selected by using purposive sampling technique. In qualitative research, when researchers want to select information-rich sources that are directly relevant to the research questions, then purposive sampling is appropriate (Creswell & Poth, 2018). Documents will therefore be selected based on relevance, not statistical representativeness, and evidentiary value.

Documents will be included when they:

- ⑩ directly address digital banking, digital fraud, cybersecurity, or consumer protection;
- ⑩ concern Pakistan or provide relevant comparative/international context;
- ⑩ originate from credible governmental, regulatory, institutional, academic, or internationally recognized sources;
- ⑩ provide information relevant to at least one research question; and
- ⑩ contain substantive information concerning fraud prevention, detection, reporting, institutional responsibility, or consumer redress.

Documents that are outdated, unverifiable, repetitive, promotional without substantive evidence, or unrelated to the Pakistani regulatory context will be excluded.

Data Analysis

The study will use qualitative thematic analysis to analyze the collected documentary data. Thematic analysis is suitable because it is a method that allows researchers to detect, code, interpret and report meaningful patterns in qualitative data (Braun & Clarke, 2006). It also offers some flexibility in analysing the various types of documentary evidence.

The analysis will proceed through the following stages:

1. **Familiarization with the data:** The researcher will read the selected documents repeatedly to develop an overall understanding of their content.
2. **Initial coding:** Relevant statements, provisions, institutional practices, challenges, and responses will be assigned descriptive codes.
3. **Identification of themes:** Related codes will be grouped into broader themes.
4. **Review of themes:** Emerging themes will be examined against the original documentary material to ensure consistency.
5. **Definition and naming of themes:** Each major theme will be clearly defined according to its relationship with the research questions.
6. **Interpretation:** The final themes will be interpreted in relation to the study objectives and existing literature.

Potential analytical themes may include forms of digital banking fraud, social engineering and phishing, cybersecurity vulnerabilities, regulatory gaps, institutional accountability, fraud reporting, customer awareness, complaint resolution, compensation mechanisms, and inter-institutional coordination. These themes will not be predetermined as fixed findings; rather, they will provide an initial analytical framework that can be refined as documentary evidence is examined.

Document Analysis

The secondary data will be analysed using the following main methodological approach: Document analysis. According to Bowen (2009) document analysis is a systematic process used to interpret and review documents and it is recommended for use in qualitative research.

A review of the regulatory documentation for provisions on institutional responsibility, security measures, reporting on fraud, informing customers, complaint resolution and consumer redress will be undertaken. In the case of banks and microfinance banks, SBP's security measures, for instance, demand specific security measures and stipulate compensation for the customer when they do not implement the required security measures and the conditions are satisfied. The study will review these provisions and other institutional and academic evidence to evaluate the institutional structure of consumer protection.

Trustworthiness of the Study

Qualitative rigor will be achieved in the study in terms of credibility, dependability, confirmability and transferability. Authoritative primary institutional documents, especially regulatory documents, will be used in conjunction with academic literature that has been peer-reviewed, to enhance credibility. The systematic documentation of the selection of the documents, coding procedures, and thematic developments will increase dependability. Confirmability will be supported by using documentary evidence to back up interpretations, rather than unsupported assumptions. Enhancing transferability will be achieved by providing detailed description of the Pakistani context of digital banking and regulation.

Different types of documents will also be used for triangulation. For instance, if there is any convergence between regulations and institutions, any challenges in implementing the regulations, or any differences in interpretation, they will be identified by comparing the two. Triangulation is one of the methodological advantages that can be assured by systematic document analysis according to Bowen (2009).

Ethical Considerations

The study doesn't require interviews, surveys or face-to-face interaction with human subjects, but ethical standards are still relevant. The research will rely on information sources publicly available and suitably attributed and information will be presented accurately and in context. Regulatory documents and institutional statements will not be selectively quoted in a way which distorts them. Academic sources will be properly acknowledged using APA 7th edition referencing. Special care will also be exercised not to reproduce personally identifiable information, confidential banking information, account details and other information which may be found in publicly available reports in the course of the research as this information falls within the category of fraud and consumer protection.

Review of Literature

Digital banking has revolutionized the financial institution–consumer interaction. Mobile banking, internet banking, digital wallets, instant payment systems and fintech platforms have made banking much more convenient and easier to access financial services, especially in developing economies. Digitalisation of financial services, however, has also increased the types of consumer risks related to fraud, data misuse, identity theft, unauthorised transactions and technology issues. The increasing body of literature now regards digital banking fraud not just as a cyber security issue but as an issue related to financial consumer protection, institutional accountability, regulatory governance and consumer trust. New international data shows that fraud and scams are one of the largest threats that face financial consumers, especially as digitalisation increases in size and complexity. (OECD, 2024, 2026).

Digital Banking and Emerging Fraud Risks

There are numerous fraud risks associated with digital financial services as identified in the literature. In addition to traditional methods of unauthorized access, phishing, smishing (SMS phishing), vishing (voice phishing), identity fraud, SIM-swap attacks, malicious applications, biometric fraud, and authorized push-payment scams are becoming more common. World Bank (2023) digital finance literature highlights that fraudsters can target vulnerabilities in mobile apps, identity systems, consumer information, and electronic payment systems. In an analogous fashion, World Bank's digital finance framework outlines mobile-app fraud, biometric identity fraud, synthetic identity fraud, and authorized push-payment scams as key consumer risks related to digital financial services (World Bank, 2024).

CGAP's research shows that the digital financial consumer risks have become significantly different. In recent years, data misuse, network vulnerabilities, poor response capabilities and third-party activities are increasingly linked to fraud (Chalwe-Mulenga et al., 2022). Recent CGAP studies have suggested that fraud is becoming harder to detect, as fraudsters utilize social media, speedy payment methods, consumer information, organized crime groups, and artificial intelligence (AI) (Duflos et al., 2026). This can be especially relevant in developing economies where the rate of financial literacy and awareness among consumers and their institutions can be slower than the rate of digital financial technology adoption.

The rapid expansion of digital financial services has also resulted in a rise in financial scams and fraud across many jurisdictions, according to the OECD (2024). Some of the most significant risks to financial consumers are identified in its analysis as phishing, impersonation, payment fraud, and other frauds enabled by digital technology. The OECD's 2026 analysis also highlights that phishing, vishing, smishing, impersonation of financial-service providers, payment schemes, and mobile banking or the use of digital wallets fraud now have emerged as key types of consumer fraud (OECD, 2026). The results indicate that technological innovation has not only changed the way fraud is committed, but also the nature of fraudsters and victims' relationships.

Consumer Vulnerability and Financial Literacy

Another prevalent strand in the literature is consumer vulnerability. The digital banking journey demands consumers to go through authentication, passwords, one time passwords, mobile app, link, digital identity, and transaction validation. Consumers might be more vulnerable to misleading communication and social engineering tactics due to a lack of financial and/or digital literacy. World Bank (2024) states that consumer awareness can be a driver for exposure to fraud and misconduct in digital financial services. In the same fashion, OECD (2024) has highlighted financial literacy and consumer awareness as key aspects of the policy response to emerging financial risks.

Consumer vulnerability does not mean that the individual is negligent. Fraud schemes are becoming more sophisticated and are now seeking to mimic genuine financial institutions and exploit their psychological and behavioral traits. Consumers can be fooled into revealing credentials or authorization for transactions that they think are legitimate. Therefore, an individual responsibility approach to combating fraud might not be sufficient. CGAP (2026) says that the need to protect consumers effectively must be addressed at every stage of the fraud chain—from prevention to detection, disruption, response, and recovery.

It has implications for Pakistan which are of great importance. Consumer protection relies on more than consumers' ability to identify these bogus communications in the growing adoption of digital banking. Financial institutions and regulators are also responsible for transaction monitoring, authentication, customer alert, fraud reporting, complaint handling and recovery strategies. Increasingly, the literature indicates that there is a shared-responsibility approach to fraud prevention, where consumers, financial institutions, regulators, telecom providers, technology vendors, and law-enforcement agencies are responsible for preventing fraud.

Regulatory Challenges in Digital Finance

One of the problems that arose in the recent literature is the inability to control the rapidly changing digital financial ecosystems. Banks, fintech, electronic-money institutions, payment service providers, telecommunications operators, technology providers, and third-party service providers are central to the increasing digital financial services. As a result, regulatory authority may be dispersed among various institutions and regulations. The World Bank (2024) recognizes the regulatory perimeter as an issue of consumer protection because the regulators are not well equipped to address consumer protection issues that arise in the absence of a provider or digital product within the traditional institution-based regulatory categories.

The literature thus highlights the importance of technology-neutral, risk-based and flexible regulatory approaches, capable of dealing with new types of fraud. According to the World Bank (2023), financial innovation can bring opportunities and challenges for the regulator due to the rapid pace of technological advancements in financial services. OECD (2024) also highlights the

need for regulatory and supervisory measures that evolve to address new risks presented by consumers, and not solely those in the financial sector.

Another regulatory issue is who is responsible in the event of fraud? Conventional models of consumer protection can be very demanding of consumers in terms of protecting their passwords, authentication information, and devices. But modern frauds are more often than not complex in nature, use third-party systems that have been compromised, or weaknesses in institutional control. In recent international literature, mechanisms of shared liability and reimbursement are increasingly being studied. Shared-liability arrangements are a new regulatory tool that could see banks, telecommunications service providers and other stakeholders assume responsibility for losses under specified conditions, CGAP (2026) reports.

Consumer Protection and Institutional Accountability

The protection of financial consumers is gaining traction as a critical component of trust in digital financial systems. World Bank (2024) states that robust consumer-protection systems provide consumers with the ability to make informed choices, exercise consumer rights, and have a fair process for addressing consumer complaints. Complaint-handling and dispute-resolution processes are thus key elements of digital banking governance.

Similarly, the OECD (2024) states that financial consumer protection must not only cover fraud prevention, but also the conduct of institutions, transparency, complaint resolution and the supervision of the institutions. In recent literature, the suggestion has been made to apply consumer protection measures across the whole chain of a fraudulent transaction, from prevention to security measures, transaction monitoring, notification, investigation, reimbursement and dispute resolution.

This is reinforced by CGAP's ecosystem approach. Financial institutions alone are not able to effectively counter fraud, as the use of telecommunications services, technology suppliers, payment systems, and other middlemen are often crucial to the digital financial transactions. This coordinated action between financial authorities, data-protection regulators, telecommunications authorities, law enforcement, financial-service providers and consumer organizations is therefore emphasized by Duflos et al. (2026). This ecosystem view is particularly relevant in Pakistan as it may necessitate cooperation among the State Bank of Pakistan, banks, payment system operators, telecommunications firms, law enforcement and consumer protection institutions in order to effectively address digital banking frauds.

Regulatory and Institutional Response in Pakistan

In the past few years, the digital banking scene in Pakistan has seen significant regulatory evolution. The State Bank of Pakistan (SBP) has taken a series of steps to enhance the security of digital banking and bolster institutional measures against digital banking fraud. SBP asked banks and microfinance banks to gather data on digital banking frauds/attempted frauds in 2021. This reporting framework has been extended to incorporate fraud reported via various channels

including call centers, emails, letters and financial institutions' internal detection (State Bank of Pakistan [SBP], 2021, 2022).

One of the most significant developments was the SBP's security plan in 2023. The framework mandates that banks and microfinance banks take certain measures regarding digital banking products and services. It also states that institutions not putting in place the controls prescribed within the specified time may be asked to settle affected customers within three working days of reporting the fraud (SBP 2023a). This is a significant step toward institutions being held accountable for consumer protection, as they are linked to preventive controls rather than simply to individual consumers' responsibilities.

SBP's consumer-protection framework also includes formal complaint-resolution mechanisms. All banks, microfinance banks, and development finance institutions are mandated to establish a mechanism for handling consumers' grievances while consumers can escalate any grievance they might have through the Banking Mohtasib Pakistan or, in appropriate cases, to SBP (SBP, 2026). The mechanisms are important because consumer harm can only be prevented if there is an effective recourse in case of fraudulent transaction.

Later, SBP streamlined and bolstered its consumer protection mechanism with the Business Conduct and Fair Treatment of Consumers Regulatory Framework (BC&FRF) published in October 2025. The aim of the framework was to rationalize the existing instructions and to harmonise the requirements for the treatment of consumers with the international market practice (SBP, 2025). This is a sign of a shift towards a more holistic and conduct-based approach to consumer protection, rather than considering individual instances of fraud as a technological problem.

Digital Fraud, Trust, and Financial Inclusion

Another theme in the literature is the relationship between fraud and financial inclusion. By reducing transaction costs and bringing financial services to those who have not had them in the past, digital banking can enhance financial inclusion. But exposure to fraud by consumers can lead to mistrust, and loss of trust can lead to decreased uptake of digital services. CGAP (2026) states that financial-inclusion benefits can be undone by fraud, as consumers' lost finances could lead them to cut back on or stop using digital financial services. Finally, the World Bank (2024) highlights the need to build trust in the formal financial sector with robust consumer protection to ensure sustainable development of digital finance.

This is particularly important in developing countries like Pakistan, where digital banking is emerging as a tool to grow financial inclusion. However, if consumers see digital transactions as unsafe or think that institutions will not make up for the losses when the transactions are lost to fraud, this may not lead to long-term financial inclusion. Consumer protection is a key prerequisite for the sustainable growth of digital banking.

Research Gap

While there is considerable literature that covers the issue of financial fraud, financial security, financial inclusion and consumer protection, there are gaps. Increasingly, international studies are taking an ecosystem approach, while studies on country-specific aspects such as the role of fraud patterns, regulatory issues, institutional accountability, and consumer redress are still primarily limited. The current regulatory frameworks in Pakistan also indicate that significant institutional measures have been taken such as reporting requirements on fraud, digital security measures, compensation measures, and complaint resolution frameworks (SBP, 2021, 2022, 2023a, 2025). But a need was still identified to qualitatively synthesize all those measures to understand the extent to which the array of measures collectively address the evolving nature of digital banking fraud.

The present study aims to fill this gap by using a qualitative study of secondary documentary evidence. It gathers regulatory documents, institutional materials, policy and policy frameworks, academic literature and relevant reports to study the three interconnected issues, namely major forms and patterns of digital banking fraud in Pakistan, the regulatory/institutional challenges in preventing and responding to digital banking fraud, and consumer protection mechanisms of relevant institutions. The study thus goes beyond the narrow cyber security perspective of fraud and makes it a problem of regulatory governance, institutional responsibility, consumer protection and trust.

Findings and Discussion

The qualitative analysis of regulatory documents, institutional publications, policy frameworks, and relevant academic and international literature generated four major themes: (1) the changing nature of digital banking fraud, (2) gaps and challenges in regulatory and institutional responses, (3) strengthening of consumer-protection and redress mechanisms, and (4) the importance of coordinated institutional responsibility. Since this study is based on secondary documentary evidence, the findings represent thematic interpretations of documented regulatory and institutional responses rather than statistical estimates of fraud prevalence.

Changing Nature and Complexity of Digital Banking Fraud

The first thing that has emerged as a key finding is that digital banking fraud in Pakistan is not just about unauthorized access, but now also involves advanced social engineering and digitally enabled deception. The first major finding is that digital banking fraud in Pakistan is not only about the unauthorized access but also the involvement of sophisticated social engineering and digitally enabled deception. The literature reviewed suggests phishing, fraudulent calls and messages, impersonation, identity-related fraud, credential theft, and manipulation of customers to authorize transactions are important aspects of the current digital-fraud landscape. According to international evidence, fraudsters are taking advantage of social media, consumer data, fast payment systems and AI, making fraud more challenging for consumers and institutions to detect

(CGAP, 2026). In recent research, CGAP refers to fraud as a constantly changing and cross-sector/cross-border challenge that has the potential to destroy consumer loyalty and erode progress in financial inclusion.

From a Pakistan perspective, this discovery is significant as digital banking is gaining traction through mobile applications, internet banking, electronic payments, and other digital means. SBP's regulatory action acknowledges the need for further measures to prevent fraudulent activities in the context of the growth of digital banking. In 2023, the SBP framework had specific reference to digital transformation, emphasizing the importance of robust security measures and corrective actions. So it seems that fraud is not just a technology issue. Rather, it is a combination of technology, consumer behavior, institutional regulation, communication tactics, and other criminal approaches.

Another discovery is that as fraud becomes more sophisticated, so do the responses that target the consumer as the primary target. Another thing I noted as fraud becomes more sophisticated, so does the response to that fraud which targets the consumer as the primary target. While consumer awareness is still valuable, sophisticated methods of impersonation and social engineering can ensure that fraudulent messaging can look like the real thing. Consumer protection, therefore, must be institutional arrangements that can detect and deter fraudulent transactions before the financial loss. This is in line with CGAP's 2026 thinking: Fraud prevention must address the full fraud chain – from prevention through detection, disruption, response and recovery.

Regulatory Development Accompanied by Implementation Challenges

The second key takeaway is that Pakistan has increasingly established a regulatory framework to tackle digital banking fraud, and the impact of the regulatory protection would be significantly influenced by institutional implementation. SBP had issued certain guidelines to report Cases of digital banking fraud and attempted fraud in 2021 and in 2022, it further extended the guidelines to cover more categories of such frauds and attempts. These measures reflect an institutional approach to identifying and monitoring digital fraud, not a single case by case approach.

Measures to Enhance Security of Digital Banking Products and Services in 2023 was another step towards this approach. SBP mandated the banks and microfinance banks to implement certain controls and put plans in place for implementation. Significantly, institutions who didn't put in place the prescribed controls within the deadline will be liable to customers who have been affected within three working days of reporting the fraud, as well as possible enforcement action.

The document evidence thus points to a shift from a 'preventive' cybersecurity orientation to one that includes measures for institutional accountability and consumers' redress. The presence of regulations, however, doesn't mean they are effective in the real world. Implementation can be complicated due to rapidly evolving fraud techniques, the different institutional capacities, the participation of a multitude of actors in digital transactions and the challenge of establishing responsibility. In a recent research report, CGAP also notes that fraud is becoming more complicated and harder to spot and that the regulatory and institutional response is lagging behind.

So, the central regulatory problem is not just “no rules.” Instead, it’s about ongoing adaptation, enforcement, monitoring and coordination of regulatory measures to ensure that regulatory goals are met and translated into effective consumer protection.

Strengthening Consumer Protection and Institutional Redress

The third observation is on the enhancement of consumer protection in the financial regulatory framework, which has been occurring over time in Pakistan. The presentations show how consumer protection has increasingly come to be associated with responsible business practices, complaint management, institutional accountability, and fair treatment and has not been restricted to financial education.

An important breakthrough was the issuance of the Business Conduct and Fair Treatment of Consumers Regulatory Framework (BC&FRF) by SBP in October 2025. The framework simplified and recaps earlier regulatory guidance on responsible business practices and consumer fair treatment. It extends to financial institutions, as defined under the scope of financial institutions in the relevant financial instruments act, which are relevant to this, such as banks, development finance institutions, electronic money institutions and payment-system operators/service providers. The framework took effect immediately for financial institutions relevant to it, and in the case of the governance provisions, application for electronic money institutions from 1 January 2026.

This is meaningful as it adds digital banking fraud to a fair-treatment and conduct framework. The regulatory approach has shifted from treating consumers as consumers as users to recognizing institutional responsibilities in the context of responsible conduct, accountability, transparency and fairness. SBP’s latest regulatory documents outline the BC&FRF as part of its consumer protection and responsible business conduct initiatives in the financial services.

The results further reveal the importance of complaint/reedress mechanisms as an element of consumer protection. It is important to have effective mechanisms in place post-fraud, as it cannot prevent all transactions from being fraudulent. There should be easily accessible processes that allow consumers to report, investigate, and, if appropriate, be reimbursed for fraudulent transactions. Therefore, the protection’s efficacy, besides preventing frauds, should also be measured by the availability, timeliness, transparency, and fairness of institutional responses to frauds.

Need for an Ecosystem-Based Institutional Response

The fourth key finding is that digital banking fraud requires a multi-agency response, as individual entities – banks and regulators – cannot solve the problem on their own. Digital transactions often engage multiple related actors such as banks, payment service providers, telecommunications, technology providers, regulators and even law-enforcement agencies. In its recent work, CGAP underscores that fraud is a cross-sector and cross-border problem, and calls for action across the entire fraud chain.

This discovery is of great significance to Pakistan. A fraudulent digital transaction can involve a customer's mobile device, telecommunications service, payment platform, bank account, authentication and perhaps third party digital services. Therefore, vulnerabilities in one area of this ecosystem can cause vulnerabilities in other areas. Regulatory responsibility can also be divided, because each institution has a different piece of information and/or authority.

The results thus highlight the need to consider inter-institutional coordination as a key element of consumer protection. Fraud reporting systems must produce valuable information; financial institutions must be able to provide information in acceptable and safe channels; regulators must have the supervisory resources they need; and consumers should have easy ways to report fraud. In the absence of coordination, individual institutions will be able to respond to isolated incidents without recognising common fraud patterns.

Discussion

All in all, the results illustrate a substantial shift in the comprehension of digital banking fraud in Pakistan. The problem is not just a problem of the individual user not keeping their password/authentication information safe. Rather, it's a multi-dimensional governance issue related to technological vulnerabilities, consumer conduct, institutional controls, regulatory regulation, and redress mechanisms.

The Pakistani regulatory journey is a move towards institutional responsibility. In 2023, SBP's security requirements included a clause that would incentivize institutions to comply with security standards by offering compensation to consumer-to-innovator, and in 2025, the BC&FRF merged the treatment of consumers under the security requirements in 2023 into a larger regulatory framework. These advances align with the thinking of the rest of the world that intervention is needed in prevention, detection, disruption, response and recovery for consumer protection.

However, the analysis suggests the strengthening of regulations should be seen as a process of strengthening, not a finished product. Fraud methods are constantly changing and new technology, such as generative AI, can make scams more sophisticated and believable. Meanwhile, the growth of digital financial services has created new stakeholders and channels of transactions that make accountability more complex. The main difficulty for Pakistan, therefore, is that its regulatory frameworks should be flexible and able to adapt while the institutions should have technological, organizational and supervisory capacities in place to implement them effectively.

Overall, the results indicate that there is a convergence toward a shared responsibility approach to protecting consumers in digital banking. While consumers are still a key player in fraud prevention, it is vital that this responsibility is spread across the financial institutions, payment providers, telecommunication companies and other relevant actors and stakeholders in the payment industry. Good consumer protection therefore requires improved security measures, but also needs to include effective complaint procedures, efficient investigation, adequate redress, institutions taking responsibility, consumer education, citizens' information and ongoing regulatory review and

development. This holistic strategy can be instrumental in achieving a balance between digital banking growth and maintaining consumer confidence and trust in the evolving digital financial ecosystem in Pakistan.

Conclusion

With the growing adoption of mobile banking, internet banking, electronic payments, and other digital financial services, digital banking fraud has become a serious issue for consumer protection and regulation in Pakistan. This qualitative study confirms that fraud in the modern era is often phishing, social engineering, impersonation, unauthorised transactions, credential theft and various technologically assisted frauds that can take advantage of both consumer vulnerabilities and institutional weaknesses. The secondary documentary evidence reveals that the State Bank of Pakistan has increasingly tightened the regulatory regime by introducing the requirement of reporting cases of fraud, strengthening the digital security systems, introducing consumer protection, complaint handling and provisions of compensation to customers under certain situations. But implementation of the measures relies on institutional action, regulatory supervision, consumer awareness, speedy resolution and cooperation among banks, payment systems, telecommunication service providers, and other participants. The study therefore underscores the need to consider digital banking fraud not only from a technical/ cyber security perspective or as a responsibility of individual consumers but also as a question of financial consumer protection, regulatory governance and institutional accountability. It is thus essential that a sustainable digital banking environment in Pakistan is built on an adaptive and ecosystem-based approach that includes preventive security measures, effective fraud detection and reporting, prompt resolution, and a continuous development of regulations. It can help build consumer confidence and help sustain the growth of safe and inclusive digital financial services in Pakistan through strengthening these interconnected mechanisms.

References

- Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2), 27–40. <https://doi.org/10.3316/QRJ0902027>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp0630a>
- Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). SAGE Publications.
- State Bank of Pakistan. (2018, November 28). *Security of digital payments* (PSD Circular No. 09 of 2018).
- State Bank of Pakistan. (2021, February 18). *Collection of digital banking frauds/attempted frauds information through call centers* (BC&CPD Circular No. 02 of 2021).
- State Bank of Pakistan. (2022, May 26). *Collection of digital banking frauds/attempted frauds information through call centers* (BC&CPD Circular Letter No. 03 of 2022).
- State Bank of Pakistan. (2022, January 3). *Licensing and regulatory framework for digital banks*.

- State Bank of Pakistan. (2023, April 14). *Measures to enhance security of digital banking products and services* (BPRD Circular No. 04 of 2023).
- State Bank of Pakistan. (2023, December 29). *Launch of Sunwai—A customer complaint management service by State Bank of Pakistan* (CPD Circular No. 01 of 2023).
- Consultative Group to Assist the Poor. (2017). *Fraud in mobile financial services*. World Bank Group. <https://www.cgap.org/research/publication/fraud-mobile-financial-services>
- State Bank of Pakistan. (2021, February 18). *Collection of digital banking frauds/attempted frauds information through call centers* (BC&CPD Circular No. 02 of 2021). <https://www.sbp.org.pk/circulars/bc-cpd-circular-no-02-of-2021>
- State Bank of Pakistan. (2022, May 26). *Collection of digital banking frauds/attempted frauds information through call centers* (BC&CPD Circular Letter No. 03 of 2022). <https://www.sbp.org.pk/circulars/bc-cpd-circular-letter-no-03-of-2022>
- State Bank of Pakistan. (2023a, April 14). *Measures to enhance security of digital banking products and services* (BPRD Circular No. 04 of 2023). <https://www.sbp.org.pk/circulars/bprd-circular-no-04-of-2023>
- State Bank of Pakistan. (2023b, August 1). *Bifurcation of Banking Conduct & Consumer Protection Department*. <https://www.sbp.org.pk/circulars/bcpd-circular-letter-no1-of-2023>
- State Bank of Pakistan. (2023c, December 29). *Launch of Sunwai—A customer complaint management service by State Bank of Pakistan* (CPD Circular No. 01 of 2023). <https://www.sbp.org.pk/circulars/cpd-circular-no-01-of-2023>
- World Bank. (2017). *Good practices for financial consumer protection: 2017 edition*. World Bank. <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/492761513113437043/good-practices-for-financial-consumer-protection-2017-edition>
- World Bank. (2020). *How countries can expand access to digital financial services*. World Bank. <https://www.worldbank.org/en/topic/financialsector/publication/digital-financial-services>
- World Bank. (2025). *The Global Findex Database 2025: Connectivity and financial inclusion in the digital economy*. World Bank. <https://www.worldbank.org/en/publication/globalindex>
- World Bank. (n.d.). *Financial consumer protection*. Digital Finance Inclusion. <https://digitalfinance.worldbank.org/topics/financial-consumer-protection>
- World Bank. (n.d.). *Complaints handling and dispute resolution*. Digital Finance Inclusion. <https://digitalfinance.worldbank.org/topics/financial-consumer-protection/complaints-handling-and-dispute-resolution>
- Consultative Group to Assist the Poor. (2017). *Fraud in mobile financial services*. World Bank Group.
- Chalwe-Mulenga, M., Duflos, E., & Coetzee, G. (2022). *The evolution of the nature and scale of DFS consumer risks: A review of evidence*. CGAP.
- Duflos, E., Chalwe-Mulenga, M., & others. (2026). *Solutions to protect consumers from fraud in digital finance*. CGAP.

- Financial Action Task Force. (2025). *Cyber-enabled fraud and money laundering*. FATF.
- International Telecommunication Union. (2024). *Global cybersecurity outlook and digital security developments*. ITU.
- Organisation for Economic Co-operation and Development. (2023). *Financial literacy and financial well-being in the digital age*. OECD Publishing.
- Organisation for Economic Co-operation and Development. (2024). *Consumer finance risk monitor*. OECD Publishing. <https://doi.org/10.1787/047b2ea6-en>
- Organisation for Economic Co-operation and Development. (2024). *G20/OECD high-level principles on financial consumer protection*. OECD Publishing.
- Organisation for Economic Co-operation and Development. (2026). *Protecting consumers from financial scams and frauds*. OECD Publishing. <https://doi.org/10.1787/d41817bb-en>
- State Bank of Pakistan. (2021, February 18). *Collection of digital banking frauds/attempted frauds information through call centers* (BC&CPD Circular No. 02 of 2021).
- State Bank of Pakistan. (2022, May 26). *Collection of digital banking frauds/attempted frauds information through call centers* (BC&CPD Circular Letter No. 03 of 2022).
- State Bank of Pakistan. (2023a, April 14). *Measures to enhance security of digital banking products and services* (BPRD Circular No. 04 of 2023).
- State Bank of Pakistan. (2023b). *Consumer protection*. State Bank of Pakistan.
- State Bank of Pakistan. (2023c, December 29). *Launch of Sunwai—A customer complaint management service by State Bank of Pakistan* (CPD Circular No. 01 of 2023).
- State Bank of Pakistan. (2024). *Annual report 2023–24: The state of Pakistan's economy*. State Bank of Pakistan.
- State Bank of Pakistan. (2025). *Business Conduct and Fair Treatment of Consumers Regulatory Framework (BC&FRF)* (BPRD Circular No. 04 of 2025).
- State Bank of Pakistan. (2025). *Financial stability review 2025*. State Bank of Pakistan.
- State Bank of Pakistan. (2026). *Consumer protection and complaint resolution*. State Bank of Pakistan.
- World Bank. (2020). *Payment aspects of financial inclusion in the fintech era*. World Bank.
- World Bank. (2022). *The Global Findex Database 2021: Financial inclusion, digital payments, and resilience in the age of COVID-19*. World Bank.
- World Bank. (2023). *Fintech and the future of finance*. World Bank.
- World Bank. (2024). *Inclusive digital financial services: A reference guide for policymakers and regulators*. World Bank.
- World Bank. (2024). *Financial consumer protection in digital financial services*. World Bank.
- World Bank. (2024). *Digital security and fraud*. Digital Finance Inclusion.
- World Bank. (2025). *The Global Findex Database 2025: Connectivity and financial inclusion in the digital economy*. World Bank.
- World Bank. (2025). *Financial consumer protection: Digital financial services*. World Bank.
- World Bank. (2026). *Digital finance inclusion: Financial consumer protection and digital security*. World Bank.
- CGAP. (2026). *An ecosystem approach to consumer protection: What, why and how?* CGAP.
- CGAP. (2026). *Solutions to protect consumers from fraud in digital finance*. CGAP.