
A COMPREHENSIVE STUDY OF BANK ACCOUNTABILITY IN MOBILE BANKING

Vivek Yadav, LLM (CB&IL), Amity University, Noida

Dr. AP Bhanu, Amity Law School, Amity University, Noida

ABSTRACT

The swift growth of mobile banking has changed the financial services industry by increasing the ease of access and convenience offered to clients around the world. Nevertheless, this new development has generated issues related to accountability of banks, especially in terms of security, transparency, protection of consumers' interests, and regulation. The following paper represents an investigation into the problem of bank accountability in mobile banking, specifically the processes and factors involved in achieving accountability in mobile banking systems.

Mobile banking applications allow customers to engage in different financial activities such as fund transfer, bill payment, and account management via smartphone and other electronic gadgets. Although there are many advantages offered by the application of mobile banking, it comes along with certain challenges related to the risk of data breach, unauthorized transactions, fraud, and technical failures. In view of these challenges, the accountability of the banks is very important.

The study will look into the regulations and guidelines that exist regarding accountability in mobile banking from the perspective of legal and regulatory frameworks in terms of data protection, grievance handling, liability apportionment, and cybersecurity issues among others. In this case, special attention will be paid to the role of the regulating authority.

In addition, the research examines the roles played by the banks in protecting their customer information and providing for secure online transactions through the use of advanced authentication techniques, encryption, fraud prevention measures, and real-time surveillance to detect any suspicious activity. Moreover, it assesses the effectiveness of banks' risk management processes in securing their networks and responding to security threats.

Another issue that the study considers is that of customer awareness about the risks involved with mobile banking services and secure practices while using them. In many cases, customers have low levels of digital literacy,

which increases their vulnerability to cyber frauds. The study stresses the responsibility of both parties and the need for banks to ensure proper communication, notifications, and training of users. Finally, one of the aspects studied in detail is the complexity and ambiguities surrounding the assignment of liability in cases where online transactions involve various other participants besides the bank and the customer. For instance, such transactions may include payments made via payment gateway sites, or transactions involving telecom operators and third-party websites.

Furthermore, this research considers new developments in relation to technology such as artificial intelligence, blockchain, and biometrics being used in mobile banking transactions, and its effect on accountability. These technologies provide an avenue for improved efficiency and security but can pose new challenges that require careful consideration.

1.Introduction

In this era, mobile banking has become one of the greatest innovations in the field of modern banking because of the revolution it has brought to the sector. The use of mobile phones, together with other advanced technologies in computing and internet access, has made it possible for customers to carry out various banking activities via their phones without the need to visit the banks physically. Mobile banking is therefore an important innovation that has increased convenience and efficiency in the delivery of financial services.

Mobile banking involves the delivery of various financial services through mobile phones using either applications or websites. Mobile banking comes under the category of electronic banking or e-banking. Mobile banking depends on internet connectivity and reliable software systems. Over the last few years, the growth of mobile banking has been tremendous due to increased penetration rates of the internet as well as availability and affordability of phones. Initiatives such as Digital India as well as the introduction of UPI payment systems have led to increased use of mobile banking.

Also, the growing intricacy of digital finance demands an accountability framework comprising various elements like legal, ethical, and operational issues. The legal aspect means banks need to conform to the laws laid down by central agencies, such as the RBI, for security in relation to cybersecurity, data protection, and digital transactions. In terms of ethics, the bank should be transparent in its business dealings and keep the clients informed about various terms and conditions and associated risks. Regarding operation, it implies effective internal

controls, monitoring, and risk management measures.

A further important issue related to accountability in mobile banking is customer education or awareness. Some users may be less literate or aware in respect to matters pertaining to digital technology. As a result, there could be chances of being exploited by fraudsters. Hence, banks need to take up an educational role apart from ensuring that digital platforms are secured against any form of external attacks.

Mobile banking trends have also put into focus the importance of having an effective mechanism for grievance redressal. Clients may find themselves facing problems such as transaction failures, breach of security, and other technical faults in the system. It is therefore imperative for banks to have systems in place where clients can air out any grievances they have with the service.

2. Concept of Bank Accountability in Digital Context.

In the light of digitization in the current business environment, bank accountability in the digital context has become a crucial topic because of the increasing use of mobile banking and other forms of digital banking services. The responsibilities of banks have broadened due to the growing reliance on digitization, shifting from managing financial issues to technology-related problems.

Bank accountability in the digital context means that the banks are responsible for securing their digital services, making sure they operate in a transparent manner, are efficient, and provide quality services to their clients. Banks are accountable for their digital actions, protecting the customer's information, and maintaining the reputation they enjoy despite the absence of human contact. Because the customers completely depend on digital tools like apps and websites to conduct transactions, banks need to make sure that they function efficiently at all times.

The other important aspect of accountability revolves around the issue of data security and privacy. For instance, with digital banking services, clients provide their banking credentials such as account numbers and passwords as well as personal identification information. Therefore, there should be adequate measures of protecting such information from cyber

threats¹ and attacks. Banks have a responsibility of ensuring that such information is not compromised through such means like encryption and firewalls. Failure in this would create severe problems for banks due to issues like fraud and other liabilities.

Finally, transaction accuracy and consistency is another major dimension of accountability in digital banking. This implies that transactions that take place in a digital banking environment should always be accurate and reliable, as any error in transaction could result in inconvenience or financial losses for the customer. Such an occurrence could arise due to technical issues with servers and networks or software defects.

Transparency is another element that needs to be considered when looking at the elements of accountability in digital banking. This implies that banks should clearly outline terms and conditions, charges, privacy policy, and possible risks involved in the use of mobile banking facilities. The customer should be completely aware of the information that will be collected from him or her and the security measures involved. Inability to do so would create confusion and lower customer trust. Therefore, communication is necessary for accountability.

Besides transparency, the process of redressal of customer grievances should also be considered. Problems like failed transactions, fraud, or delay in transaction could arise due to various reasons in a digital world. Banks need to establish convenient ways for redressal, which could be in the form of toll-free numbers, live chat facility, and online portals.

Legal and regulatory compliance is another aspect of banking. Banks must adhere to the guidelines laid out by the regulatory authorities. This includes compliance with regulations on cybersecurity, data protection, limitations on digital transactions, and consumer rights, among others. The need for compliance stems from the existence of an established framework through which banks are supposed to conduct their activities safely, and failure to do so will attract repercussions.

3. Regulatory Framework and Guidelines.

The regulatory environment and policy guidelines concerning mobile banking are essential in ensuring accountability and stability in the digital banking world. Mobile banking entails

¹ Basel Committee on Banking Supervision, *Principles for Operational Resilience* (Bank for International Settlements, 2021).

financial transactions made via the Internet; hence, it is critical to develop clear guidelines and rules that banks will adhere to while offering such services². The formulation of regulations and guidelines for mobile banking falls under the jurisdiction of central banks and relevant financial regulatory authorities in addition to data and cybersecurity bodies.

For India, the Reserve Bank of India acts as the regulatory body responsible for mobile banking in the country. The Reserve Bank of India develops stringent guidelines regarding the implementation of digital transactions to ensure that banks are reliable and efficient in offering digital services. Guidelines issued include customer authentication procedures, transaction ceilings, encryption, and risk management. One of the notable guidelines issued is the requirement of two-factor authentication for making digital transactions. It implies that customers have to authenticate their identities using two different factors like passwords and OTPs.

Cybersecurity regulation is another significant component of the regulatory framework. In view of the growing incidence of cyber-related crimes such as hacking, phishing, and malware attacks, banks are expected to have adequate cybersecurity systems in place. There are regulations that demand the installation of technology security systems, frequent system audits, and constant monitoring in order to thwart any kind of fraudulent activity. It is also incumbent upon banks to report instances of cybersecurity breaches to the regulatory authority within a stipulated period³.

Customer data protection and privacy are essential aspects of mobile banking regulations. Banks are expected to ensure that the information provided by customers does not fall into the wrong hands. Some of the key regulations relating to mobile banking in India stress on data protection and privacy, which include securing data against any form of misuse, limiting the use of data only to authorized personnel, and customer consent prior to its usage.

Consumer protection is yet another aspect considered by the regulatory regime. Consumers engaging in mobile banking might encounter problems such as fraudulent transactions, failed payments, and technical errors among others. In light of this, regulatory agencies compel banks to create efficient mechanisms for addressing such complaints. Banks must ensure that

² Basel Committee on Banking Supervision, *Risk Management Principles for Electronic Banking* (Bank for International Settlements, 2003).

³ Reserve Bank of India, Circular on *Reporting of Cyber Security Incidents* (2016).

consumers can report any grievances to a specified channel and take necessary actions within an agreed period. Besides, banks must pay compensation in case of faults caused by them⁴.

Mobile banking transaction limits and guidelines form another key component of the regulatory regime. The regulator sets the maximum amount that can be transacted via mobile banking. This helps reduce the likelihood of fraud and misuse of the platform. Further, regulators also dictate that banks provide a convenient and easy-to-use platform to cater for different categories of customers including the less technologically literate ones.

Compliance and monitoring play a critical role in ensuring banks comply with regulations. Financial institutions must comply with stipulated guidelines and standards and failure to do so might attract sanctions. Regulators conduct routine inspections and audits to check the compliance status of banking systems.

Apart from national requirements, there are also international standards and practices that may affect the development of mobile banking guidelines. Cybersecurity, data protection, and financial stability frameworks are likely to be in compliance with international standards⁵.

4. Key Components of Accountability in Mobile Banking.

Accountability within the realm of mobile banking becomes an essential aspect which helps to evaluate how trustworthy, effective, and sustainable the system is. As the majority of banking processes are completed via mobile applications, banks need to make sure that these processes are transparent, reliable, and focused on customer needs. There are several main factors which contribute to creating the concept of accountability.

The first and foremost one is information security and customer data protection. Mobile banking is a process which presupposes the use of personal data of clients and banking details related to transactions. Hence, the protection of all data from any possible external threats is a primary responsibility of the bank. Hacking and phishing become a common problem faced by mobile banking providers. Advanced tools and techniques can be used to ensure information safety.

⁴ Reserve Bank of India, *Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions*, 2017.

⁵ Bank for International Settlements and Financial Stability Board, *International Standards on Cybersecurity and Financial Stability*.

Accuracy and reliability of transactions are also an important aspect of accountability. Consumers depend on mobile banking services for real-time, and accurate financial transactions. This means that banks have to guarantee that all transactions, such as transfer of money, paying of bills, and updating of accounts are carried out with perfection. Technical challenges may cause the transactions to be faulty, duplicated, or unsuccessful. It is therefore necessary to have reliable technological resources, as well as performing regular system checkups.

In the same manner, transparency and disclosure are key factors to guaranteeing accountability. Banks need to provide all required information to consumers about charges and terms applicable to their transactions⁶. Transparency will allow customers to make proper judgments regarding their financial affairs. Notifications are also important in order to help them follow up on what happens in their accounts.

Accountability entails the existence of an effective system of customer grievances' redressal. When using their online service, the consumers can experience any problems ranging from unsuccessful transactions to hacking issues. In this regard, the bank should be ready and capable of solving arising problems quickly and effectively. It must offer its customers channels such as phone lines, email contacts, chatbots, and complaint portals. Timely handling of complaints will reflect positively on customer satisfaction and the accountability of mobile banks.

Another vital tool used to ensure accountability entails a mechanism of detecting and preventing fraudulent activity. Today, the world experiences increased cases of cyber fraud, which calls for action by banks to combat the menace. The process requires the use of artificial intelligence and machine learning algorithms in detecting unusual behaviour of customers in transactions. Moreover, the banks need to be accountable for complying with the requirements of regulatory bodies. The rules cover issues ranging from cybersecurity to digital transactions⁷.

The next element worth considering is customer education. Financial institutions need to make sure that they educate their clients regarding online security and safe practices while using digital banking channels. For instance, banks should explain how customers can protect

⁶ Reserve Bank of India (RBI), *Guidelines on Customer Protection and Transparency in Digital Banking*, 2021.

⁷ RBI, *Master Directions on Digital Payment Security Controls*, 2021.

themselves by changing passwords and not clicking on any suspicious links.

Lastly, the efficiency of bank operations and its internal control system is essential in terms of accountability. Banks have to create an effective system of internal controls and monitor the operations of their employees who deal with the digital channel.

5. Risks and Challenges.

With mobile banking, people enjoy convenient and flexible financial services, but there is also an array of dangers associated with the process of banking. Indeed, as the banking industry becomes increasingly digitized, banks need to focus on overcoming challenges and threats in order to maintain their high level of accountability⁸.

Cybersecurity remains one of the greatest risks associated with mobile banking, with hackers often exploiting weak spots of banking systems through the application of various sophisticated techniques including phishing, malware attack, identity fraud, hacking, etc. Cyberattacks might be aimed at deceiving users by using fraudulent links, malicious apps, and other methods. In spite of the fact that advanced security solutions are applied in banking, cyber threats constantly change and pose a serious challenge to banks.

Data privacy and security issues also represent another important concern. Since mobile banking involves sharing financial and personal data, it needs to be safely stored and analysed. However, data breaches and other similar problems may result in exposing such data, causing it to be used by malicious parties to commit various crimes, such as identity theft. Compliance with data protection regulations and handling massive amounts of data are critical for banks. Privacy is an essential component of accountability, and banks need to ensure that data is protected from any possible threats.

Finally, technical issues may represent another problem for banks. As the process of mobile banking takes place online, various problems associated with technical aspects may occur. For example, due to server overload, customers may face difficulties accessing mobile banking applications. Moreover, there may be other similar problems, such as transaction duplication or delay. These issues make banks accountable for providing reliable services to their

⁸ World Bank, *Digital Financial Services Report*, 2022.

customers.

In addition, it may be possible that the majority of clients have little knowledge on cybersecurity as well as insufficient digital literacy, which makes them more vulnerable to being victims of various frauds and scams. As users, especially those living in developing countries, may not know enough regarding secure use of mobile banking services, including protecting their credentials from potential hackers, it may become necessary to provide them with additional guidance in this matter.

Finally, fraud as well as any other types of unauthorized activities in regard to online banking is also an aspect associated with both cybersecurity challenges and client behaviour. Even with such security methods as OTP codes and fingerprints, cybercriminals manage to bypass the system, often by fooling the user himself or exploiting some of the system's vulnerabilities⁹. At this point, resolving cases of this kind is quite challenging because it involves assessing liability for a case, which may include a certain share on behalf of the bank.

Apart from these factors, there are also some regulatory and compliance issues associated with cybersecurity and mobile banking.

Another issue that poses serious difficulties is that of the digital divide. As mobile banking grows rapidly, all the customers do not enjoy equal access to the necessary technologies or even knowledge about how to use these technologies. As a result, it brings inequality into the area of accessibility of banking services.

Finally, reputational risk management is of paramount importance. All the possible errors in security management or other aspects of service provision will affect banks' reputation negatively. With the development of social media, the information on poor quality of services spreads very fast and can do great harm to the reputation of a bank.

6. Role of Technology in Enhancing Accountability.

The use of technology has been vital in increasing the responsibility of banks in terms of enhancing security, efficiency, transparency, and building customers' trust. The increased utilization of technologies will help banks stay responsible and accountable in performing the

⁹ Symantec, *Internet Security Threat Report*, latest edition.

banking operations and ensure the provision of quality services to their customers¹⁰.

One of the areas where technology has played a major role in increasing accountability within the field of mobile banking includes the improvement of the security of mobile banking. Some of the advanced technologies that ensure enhanced security in mobile banking include encryption, firewall, and secure sockets layer (SSL). In addition, multi-factor authentication, which involves the use of OTPs, biometric verification using fingerprints or facial recognition, and password/PINs, helps build additional layers of security¹¹.

Artificial Intelligence and Machine Learning have also been used in fraud prevention as these technologies can detect abnormal trends through transaction data analysis in real-time. For instance, in case a transaction is out of the ordinary relative to the typical behaviour of the account holder, the transaction may be blocked or flagged as an alert to the bank. This will increase accountability since banks can now take steps to prevent fraud before it takes place.

The use of Blockchain technology can significantly enhance accountability in banking services since blockchain technology provides a decentralized system that enables transactions to be recorded securely with timestamps. With this technology, it will be difficult to manipulate any information recorded since all entries are immutable.

Furthermore, technology helps enhance transparency and communications between banks and customers. Banks have introduced mobile applications where transactions are updated in real time so that the customers can monitor their activities immediately. The provision of complete transaction details, digital receipts, and clear presentation of costs associated with the service enables the customers to get sufficient information about the services and products of the financial institution. This will help prevent misunderstandings that often arise due to lack of proper information.

In addition, technology plays an important role in improving the complaint handling process of banks. AI bots and virtual assistants give instant responses to queries raised by customers¹². Ticket tracking mechanisms are put in place to record complaints and resolve them within the stipulated period of time. This shows the bank's willingness to be accountable towards its

¹⁰ Reserve Bank of India, *Report on Trend and Progress of Banking in India* (latest edition).

¹¹ Reserve Bank of India, *Guidelines on Digital Payment Security Controls* (2021).

¹² AI-powered customer service tools enhance responsiveness and customer satisfaction in banking (e.g., chatbots and virtual assistants).

customers.

Lastly, data analysis and big data technologies are helpful in building accountability through understanding of the customer behaviour. Using customer data to conduct analyses helps banks make necessary adjustments in their service and system operation to prevent risks and boost performance.

The introduction of technology improves internal controls and compliance practices in banks. The use of automated audit systems, real-time monitoring tools, and compliance systems enable banks to follow their regulatory requirements. In addition, the use of such systems will ensure that all the processes performed by the bank are monitored and evaluated at all times, lowering risks of mistakes by employees.

The use of cloud computing makes mobile banking more reliable. The use of cloud computing enables the storage and processing of vast amounts of data without compromising on security. It increases the dependability of services offered by the bank.

7. Customer Perspective on Bank Accountability.

In terms of mobile banking, it is necessary to consider the issue of bank accountability from a customer's point of view because this is one of the main criteria which determine trust, satisfaction, and further use of banking services online. Customers need the service to be not only secure but also reliable, effective, and fully accountable for the possible problems which may occur.

Of course, trust is among the major aspects which customers look for. In mobile banking, everything takes place in the digital space without a direct contact between the client and the bank. This means that clients trust the service itself. They are sure that the money and all personal data provided are protected and nothing happens with them. Any mistake or problem that occurs leads to the breakdown of this trust and makes customers dissatisfied with the service.

Another key factor is **security assurance**. Customers expect banks to implement strong security measures such as encryption, one-time passwords (OTPs), and biometric

authentication¹³. However, beyond just implementing these features, customers also expect banks to take responsibility if security is compromised. For instance, in cases of fraud or hacking, customers often believe that the bank should provide timely support and fair compensation, especially if the issue arises due to system vulnerabilities.

Transparency is also highly valued from the customer's point of view. Users expect clear and accurate information regarding transaction charges, terms and conditions, and privacy policies. Hidden fees or unclear communication can lead to dissatisfaction and a sense of mistrust. Real-time notifications and easy access to transaction history enhance transparency, allowing customers to monitor their financial activities and feel more in control.

Moreover, customer grievance redressal processes pose serious problems. Customers expect their complaints related to transactions not going through, late payments, unauthorized access to account information, and other such concerns to be sorted out swiftly. Waiting times, unresponsive customer care services, or difficult processes to submit grievances might disappoint and discourage customers from using banking services provided by such institutions. Customer accountability requires swift solutions provided by the bank to rectify these problems¹⁴.

Customer expectations concerning usability and responsiveness of services provided by banks are linked to their perception of accountability. An application for online banking services that is easy to use, is responsive and does not experience too many glitches demonstrates a bank's consideration for their customers. Complicated interfaces that are prone to errors show negligence on the side of banks towards their clients.

Lastly, customer awareness plays an essential role in determining customers' view of their relationship with banks. Although banks offer customers secure services, the customers realize that their actions also matter. At the same time, customers want the banks to inform them on how they can ensure safer transactions and avoid scams.

8. Bank's Perspective and Responsibilities.

For the bank, accountability in mobile banking is one of the most basic obligations that can

¹³ Reserve Bank of India, *Guidelines on Digital Payment Security Controls* (2021).

¹⁴ World Bank, *Good Practices for Financial Consumer Protection* (2017).

guarantee trust, security, and sustainability in the electronic financial environment. Being service providers, banks should develop and operate mobile banking in a way that provides reliability, safety, and transparency to customers.

First of all, banks have an obligation to develop an effective internal control system. An internal control system includes certain policies, procedures, and technical measures that allow banks to conduct all their activities in a correct and secure way. With the help of internal controls, mistakes can be prevented, frauds can be detected, and risks can be reduced.

The other significant responsibility is risk management. Risks associated with mobile banking include cyber attacks, operational risks¹⁵, and financial frauds among others. The bank should be capable of identifying, evaluating, and managing these risks appropriately through proper policies. These include using advanced security measures, transaction monitoring, and having contingencies when things go wrong or when a crisis emerges. Risk management helps the bank to respond to risks quickly and limit their possible adverse effects.

Data security and privacy protection should not be underestimated in terms of a bank's accountability. Banks deal with confidential data of many customers, and thus it should be a priority of banks to secure it against any forms of misuse. This can be accomplished through adopting technologies of encryption, having secure servers, using multiple authentications, and keeping systems up to date in addition to regulatory compliance and handling of data properly.

Lastly, service reliability and effectiveness should be assured by the bank. Customers do not need constant inconveniences and failures in using mobile banking services provided by the bank. The bank should invest in efficient information technology infrastructure and upgrade its systems on a regular basis.

The next major area of responsibility includes training and awareness of the bank's staff. The involvement of the staff members is very significant for the successful management of the digital banking system and solving customers' problems related to this matter. Therefore, it is essential to ensure that the bank employees possess a sufficient level of knowledge and skills regarding cybersecurity and other important aspects of the digital systems' operation and client interaction.

¹⁵ Committee of Sponsoring Organizations (COSO), *Internal Control – Integrated Framework*, 2013.

Client support and redressal of grievances also belong to the main responsibilities. It is critical to provide a convenient platform for clients where they could complain about failed deals, cyber fraud attempts, etc. Efficient processing of complaints and provision of adequate assistance to the customers¹⁶ indicate that the banks are taking the issue seriously. In addition, the banks should show some ownership regarding the problem and take measures to rectify the mistake.

The compliance with regulatory guidelines is another important area of responsibility. It means that banks have to follow the rules established by the regulators concerning cybersecurity and consumer protection.

In addition to being accountable, banks are also ethically required to remain transparent and fair. Banks should clearly inform customers about the terms, conditions, costs, and risk factors involved in their mobile banking products. It is important to avoid any hidden charges and false promises for the sake of transparency and accountability.

Lastly, banks should always remain innovative and improve upon themselves as much as possible. With technology continuously changing, it is important for banks to stay up to date with these changes and incorporate them into their practices as needed.

9. Impact of Poor Accountability.

The problem of poor accountability in mobile banking may have grave consequences not only for financial institutions but also their clients due to the issues associated with finance security, client confidence, and the effectiveness of the entire digital banking process. Due to such features as technological basis and the need to trust the institution, low accountability may result in negative impacts that are felt throughout the process¹⁷.

The first consequence of such a lack of accountability can be considered financial losses suffered by the client due to the fact that the bank does not provide sufficient security. In addition, there can be mistakes in the process of transferring funds, as well as some other types of fraud. Poorly developed security measures or delays with dealing with financial fraud may

¹⁶ RBI, *Information Technology Framework for the NBFC Sector* and banking cybersecurity guidelines, 2017.

¹⁷ Basel Committee on Banking Supervision, *Principles for Operational Resilience* (Bank for International Settlements, 2021)

make the problem worse.

Another important consequence of the problem discussed above is that of losing customer trust. In the modern world, when dealing with digital banks, it is essential to have high customer trust as customers do not see representatives of the company. If customers face different problems related to failures, data leaks, lack of customer service, they start to believe that a particular bank will not be able to protect them from any risks.

Poor accountability is another consequence of the discussed issue which negatively influences the reputation of the company. In the contemporary world, when everything can easily be spread via Internet and social networks, the name of the organization may suffer greatly due to different information about the company.

Consequences from the perspective of law and regulation are also critical. Financial institutions have to adhere to certain laws regarding data privacy, cybersecurity, and customers' rights. In case of violations, there might be sanctions or even lawsuits filed by the respective authorities. In extreme scenarios, banks would be restricted from operating or would need to pay compensation to the affected customers, which could lead to higher costs.

In addition, there is a reduction in customer satisfaction as a result of low accountability levels. Issues like late redressal of grievances, inadequate customer care, and lack of transparency make clients dissatisfied with financial service providers. Customers are always expecting timely resolution of issues and any form of delay will leave them frustrated, leading them to opt for different banks or refrain from using mobile banking services.

Low accountability may affect the efficiency of the digital banking system as well. There could be frequent technical glitches, downtime, and poor monitoring. This would negatively impact the performance of mobile banking applications, which might hinder its adoption.

Furthermore, there will be effects on financial inclusion and the adoption of technology. In nations such as India, mobile banking forms a crucial part of financial inclusion in rural and other marginalized areas. However, when accountability fails, individuals are less likely to trust technology because of their fear of losing money. This creates a digital divide, preventing the advantages associated with technological progress from being fully realized.

The last effect is that the cost of operations at banks will rise. Dealing with cases of fraud,

settling disputes, compensating losses, and enhancing systems in response to failure all require substantial expenditure.

10. Measures to Improve Accountability.

It is crucial to enhance accountability in mobile banking so that the services offered become secure, transparent, and reliable. Banks need to introduce several strategies to boost their accountability to clients¹⁸.

One such strategy includes increasing the security level of digital banking. This involves employing advanced cybersecurity tools like firewalls, encryption, intrusions detection systems, and others. Security checks on a regular basis can minimize the risk of cyber attacks. Moreover, banks can continuously monitor all transactions through the application of artificial intelligence so that all suspicious activity can be detected immediately¹⁹.

In addition, banks have to introduce more data protection and privacy techniques. First, customer data has to be stored properly, and access to it provided to the authorized persons only. Second, banks have to follow the data privacy regulations and develop specific data usage policies to increase accountability and transparency.

Increased customer awareness and improved digital skills are just as critical in improving accountability. It is not uncommon to find most security incidents happening due to the lack of user awareness. The banks need to carry out campaigns aimed at creating awareness about mobile banking, regularly inform their users about potential security dangers and share tips regarding mobile banking²⁰.

Having a functional grievance redress mechanism is key to enhancing accountability. Banks need to ensure there are various channels through which users can raise complaints, including helplines, chatting services, among others. Customer complaints must be sorted out promptly to show that the bank values its users and takes responsibility in providing quality banking services.

¹⁸ Accountability in mobile banking is essential for building trust and ensuring reliable financial services (Basel Committee on Banking Supervision, *Sound Practices: Implications of fintech developments for banks*, 2018).

¹⁹ Artificial intelligence enhances fraud detection by identifying unusual transaction patterns in real time (European Banking Authority, *Report on Big Data and Advanced Analytics*, 2020).

²⁰ Reserve Bank of India (RBI), Guidelines on Digital Payment Security Controls, 2021.

Lastly, transparency is key in improving accountability. There is a need for the bank to ensure users are aware of all the terms and conditions, transaction fees, and other policies concerning mobile banking.

Improvement in the strength of internal controls and employee training contributes to enhancing accountability. The banks need to engage in the process of continuous training of their employees regarding the use of cyber tools, proper customer service, and risk management techniques.

Secondly, compliance with regulations is essential. The banks need to comply with the rules and regulations set forth by regulators concerning digitization and cybersecurity.

Lastly, the banks can benefit from the implementation of innovative technologies. The use of advanced technologies such as blockchain and artificial intelligence can contribute significantly towards achieving accountability.

11. Findings and Discussion.

Several notable trends and challenges emerged from the results of the research into bank accountability in mobile banking. First, it becomes clear that with the advent of mobile banking and its widespread popularity in modern society, the issue of customers' safety and security takes the forefront position among all other aspects of bank accountability. Indeed, the vast majority of consumers view mobile banking primarily as an additional tool for increasing the level of financial security through convenient payment transactions.

It is essential to note that despite the introduction of various protective mechanisms by the banks, including OTP codes, fingerprint and voice recognition, and other innovations, the vast majority of consumers perceive digital transactions as insecure and vulnerable to various cyber risks, including fraud, hacking, and phishing attacks. Thus, it can be seen that despite the introduction of various innovations and technological advances, banks are yet to reach the point where customers can feel fully secure when performing online transactions.

The study findings indicate that problems regarding technical matters and reliability also arise from time to time. Issues such as apps crashing, failed transactions, and delayed processing impact the customer experience. This points to the requirement of investment by the banking institutions in robust information technology infrastructure and provision of reliable services.

Reliability of the system goes hand-in-hand with accountability.

In the context of the banking institution, issues concerning regulatory compliance and risk management emerge prominently. The financial institutions try their best to adhere to regulations on the aspects of cybersecurity and data protection. However, keeping pace with the changes in the digital landscape is difficult for the institutions and makes compliance a difficult affair.

It is also found that grievances raised by customers need prompt action. Many banks fail to address customer complaints on time. This gap creates dissatisfaction among customers.

Technology is shown to have a dual function. Firstly, it contributes towards improving accountability through automation, real-time control, and fraud detection. However, excessive use of technology exposes institutions to system failures and cyber attacks. Hence, a mixed strategy should be considered, which will combine the two approaches.

Transparency and communication also turn out to be critical factors for the maintenance of trust. Financial institutions providing their customers with transparent information regarding fees and transactions can expect to preserve their trust. Conversely, insufficient transparency results in negative outcomes.

12. Conclusion

In summary, mobile banking has proven itself to be an innovative phenomenon in today's finance system. It has not only revolutionized banking in terms of the provision and use of services but also has made them extremely convenient, accessible, and efficient. Yet, on the one hand, along with these positive effects of mobile banking, the issue of bank accountability has become increasingly vital in the contemporary environment.

According to this research, bank accountability in mobile banking can be described in terms of security, reliability, regulatory and legal requirements, transparency, and responsiveness to customers' needs. The introduction of digital technology into banking services not only adds new features to banking services but also adds more responsibilities to banks, which become not only financial service providers but also digital data and technological solutions managers.

It is essential to mention that one of the core conclusions is about the significance of security

and data protection. The growing number of cybercrimes such as phishing, hacking, and identity theft means that the security of banks has to be improved constantly and enhanced by new innovations aimed at providing the necessary safety to customers' data. Otherwise, there is no guarantee that banks will not suffer financial losses and reputation damage.

What is more, another important issue associated with the implementation of the mobile banking system is customer trust and satisfaction with the provided services. It plays an essential role in the development of mobile banking because customer confidence is directly linked to the way transactions are managed. It goes without saying that customers are looking for complete accountability of banks.

Accountability is further ensured by considering the regulatory framework and compliance. Guidelines from regulatory bodies allow banks to follow a proper way of functioning that not only protects their customers but also ensures stability. But as the technology keeps changing, regulation needs to be kept up-to-date.

Technology is both a tool for accountability as well as a problem. For instance, artificial intelligence, blockchain, real-time monitoring systems, and so on can help in enhancing accountability through improved security and transparency. Nonetheless, they can cause complications in addition to providing benefits. Hence, there needs to be a proper balance between the two.

Another important conclusion drawn from the study is the necessity to ensure that customers are aware of their safety practices and are digitally literate. However well-protected any system may be, it is still vulnerable if users do not know how to use the technology safely. Customers must be actively involved in learning about possible dangers and appropriate behaviour in relation to mobile banking technologies.

Moreover, according to the study, effective internal management and control of banks' activities are extremely important for providing proper services. These factors guarantee high-quality services and efficient performance of banks.

Bibliography

- Basel Committee on Banking Supervision. *Principles for Operational Resilience*. Bank for International Settlements, 2021.
- Basel Committee on Banking Supervision. *Risk Management Principles for Electronic Banking*. Bank for International Settlements, 2003.
- Basel Committee on Banking Supervision. *Sound Practices: Implications of FinTech Developments for Banks*. Bank for International Settlements, 2018.
- Bank for International Settlements & Financial Stability Board. *International Standards on Cybersecurity and Financial Stability*.
- Committee of Sponsoring Organizations (COSO). *Internal Control – Integrated Framework*. 2013.
- European Banking Authority. *Report on Big Data and Advanced Analytics*. 2020.
- Reserve Bank of India (RBI). *Circular on Reporting of Cyber Security Incidents*. 2016.
- Reserve Bank of India (RBI). *Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions*. 2017.
- Reserve Bank of India (RBI). *Information Technology Framework for the NBFC Sector and Banking Cybersecurity Guidelines*. 2017.
- Reserve Bank of India (RBI). *Guidelines on Digital Payment Security Controls*. 2021.
- Reserve Bank of India (RBI). *Guidelines on Customer Protection and Transparency in Digital Banking*. 2021.
- Reserve Bank of India (RBI). *Report on Trend and Progress of Banking in India* (latest edition).
- Symantec. *Internet Security Threat Report* (latest edition).
- World Bank. *Good Practices for Financial Consumer Protection*. 2017.

- World Bank. *Digital Financial Services Report*. 2022.
- AI-powered customer service tools (chatbots and virtual assistants) – industry reports and publications on AI in banking.