International Journal of Business, Management and Visuals (IJBMV), ISSN: 3006-2705
Volume 8, Issue 1, January-June, 2025, Available online at: https://ijbmv.com

Digital Fraud in India: Issues and Remedies

Anand Kumar[1], Sushila[2]

[1]Associate Professor of Commerce, MNS Govt. College, Bhiwani (Haryana)
[2]Associate Professor of Commerce, G.C.W. Rohtak (Haryana)

ABSTRACT

The rapid growth of digital banking has changed the way people in India manage their financial activities. Mobile banking, internet banking, UPI, cards, and other digital payment services have made banking faster, easier, and more convenient. However, the growing use of these services has also increased the risk of digital fraud. Fraudsters are using different methods such as phishing, OTP fraud, UPI fraud, fake customer-care calls, identity theft, fraudulent links, QR-code scams, and social engineering to target bank customers. Such activities can cause financial loss and may also reduce customers' confidence in digital banking.This paper examines the major forms of digital fraud in the Indian banking sector and discusses the factors that make customers vulnerable to such frauds. It also highlights the importance of digital awareness, safe banking practices, effective fraud detection systems, and timely reporting of suspicious transactions. The study is based mainly on secondary information collected from research studies, banking-related reports, and other relevant sources. The review indicates that digital fraud is not only a technological issue but also a problem related to customer awareness and behaviour. Strong security systems alone cannot provide complete protection if customers are unaware of common fraud techniques. Therefore, banks and other concerned institutions need to regularly educate customers and strengthen their fraud prevention and monitoring systems. The study concludes that cooperation among customers, banks, regulators, technology providers, and law-enforcement agencies is necessary to create a safer digital banking environment in India.

Keywords: Cyber Fraud, Digital Banking, UPI Fraud, Online Banking, Customer Awareness, Cyber Security, Digital Payments, Fraud Prevention.

INTRODUCTION

The Indian banking system has undergone a major change with the widespread use of digital technology. Banking is no longer limited to branch visits, paper-based transactions, or cash payments. Customers can now transfer money, check account balances, pay bills, make purchases, and access other banking services through mobile phones and internet-based platforms. Services such as mobile banking, internet banking, ATMs, cards, and UPI have made banking more convenient and have reduced the time required for many financial transactions.Along with these advantages, the rapid movement towards digital banking has created new opportunities for financial fraud. Digital fraud has become a serious concern because financial transactions can now take place instantly and across digital platforms. Fraudsters have also adapted to these changes and are using different methods to target bank customers. Instead of relying only on traditional forms of cheating, they increasingly use technology and human behaviour to obtain money or confidential information.One important feature of digital fraud is that the fraudster often tries to gain the victim's confidence rather than directly attacking a bank's system. A person may receive a phone call claiming to be from a bank, an SMS containing a fraudulent link, or a message offering a reward, refund, loan, or other financial benefit. In other cases, fraudsters may pretend to be bank officials, customer-service representatives, or other trusted persons. Victims may then be persuaded to disclose an OTP, PIN, password, card details, or other confidential information. Some frauds also involve fake applications, remote-access tools, or misleading payment requests.The increasing use of UPI and mobile payments has added another dimension to the problem. Digital payments allow money to be transferred within seconds, which is useful for genuine transactions but can also make fraudulent transfers difficult for victims to stop once they have been completed.

The ease with which customers can make digital payments therefore needs to be supported by adequate security awareness and effective safeguards.The risk of digital fraud is not the same for all bank customers. Differences in age, education, digital knowledge, experience with online banking, and awareness of security practices may affect a person's ability to identify a fraudulent communication. Customers who are unfamiliar with digital banking may be more likely to trust a false message or follow instructions given by an unknown person. At the same time, even experienced users can become victims when fraudsters use convincing stories, false identities, or carefully designed messages.Digital fraud also creates difficulties for banks. A fraudulent transaction can result in direct financial loss for a customer and may also reduce confidence in digital banking. Repeated incidents can affect the public perception of banking institutions and their digital services. Banks therefore have to balance two important objectives: making digital transactions simple and convenient while maintaining strong systems for authentication, transaction monitoring, fraud

detection, and customer protection.The nature of digital fraud is also changing with technological developments. Fraudsters regularly modify their methods in response to changes in banking technology and customer behaviour. This makes fraud prevention a continuing process rather than a one-time security exercise. Banks need to improve their technological controls, while customers need to remain alert about the information they share and the instructions they follow during digital transactions.Against this background, the present study examines the issue of digital frauds in the Indian banking sector. It focuses on the major forms and methods of digital fraud, factors that may increase customer vulnerability, and the effects of fraudulent activities on customers and banking institutions. The study also considers the role of customer awareness and banking security measures in reducing the risk of digital fraud.The issue is important because the success of digital banking depends not only on the availability of technology but also on the confidence of people who use it. A secure digital banking environment requires cooperation among banks, customers, regulators, technology providers, and law-enforcement agencies. Better customer education, stronger authentication and monitoring systems, prompt reporting of suspicious transactions, and continuous improvement in security practices can contribute to a safer digital banking environment in India.

REVIEW OF LITERATURE

1. Sharma and Sharma (2018)- Sharma and Sharma studied the increasing problem of fraud in the Indian banking sector. Their study showed that banking fraud can create serious financial and economic problems. They emphasized the need for better control systems and preventive measures to reduce fraud in banks.

2. Sood and Bhushan (2020)- Sood and Bhushan reviewed earlier research on banking fraud. They found that research gradually moved from traditional accounting fraud towards newer problems such as cyber fraud and identity theft. They also highlighted the importance of customer awareness and understanding customer experiences with fraud.

3. Roy and Prabhakaran (2022)- Roy and Prabhakaran examined cyber fraud carried out through internal weaknesses in Indian banks. They identified different forms and causes of such fraud and suggested the use of machine-learning methods to help banks identify and prevent fraudulent activities.

4. Sood and Bhushan (2022)- Sood and Bhushan developed a conceptual framework to understand factors that can contribute to banking fraud in India. Their work suggests that fraud is influenced by several connected factors, making it necessary for banks to consider organisational, technological and human aspects while developing fraud-control measures.

5. Lonkar et al. (2024)- Lonkar and other researchers studied how prepared Indian consumers are to deal with digital payment fraud. Their study of 372 consumers found that awareness of fraud risks was relatively low, while protection was moderate and responsiveness was comparatively better. They recommended stronger security measures and regular customer-awareness programmes.

6. Chandra (2025)- Chandra examined the role of India's National Cybercrime Reporting Portal in dealing with digital financial fraud. The study explained that quick reporting and coordination between police, banks, payment institutions and other agencies can help stop fraudulent money from moving further. However, the study also pointed out the need for better accountability and improvements in the system.

7. Puri et al. (2025)- Puri and colleagues reviewed research on digital financial fraud and discussed major areas for future research. Their work shows that digital fraud is becoming an important financial and technological issue and that better understanding of fraud methods, detection systems and prevention strategies is needed. The review also identifies banking fraud research as an important area for further study.

Objectives of the Study

1. To study the concept of digital frauds in India.
2. To study the major types of digital frauds in India.
3. To suggest the suitable preventive measures to reduce digital frauds.

Research Methodology- The present study is descriptive in nature and is based entirely on secondary data.The required information was collected from:

Research journals, Books, published research articles, Business magazines, Companies reports, Websites.

Research Design- A descriptive research design was adopted because it helps explain the concept, major types and preventive measures related to digital frauds in India.

Common Types of Digital Frauds in India

The rapid growth of digital banking and online payments in India has made financial transactions easier and faster. At the same time, it has created new opportunities for fraudsters to misuse digital platforms. Digital fraud can occur in many forms, and fraudsters often use both technology and psychological tricks to deceive people. The following are some of the common types of digital frauds found in India.

1. Phishing Fraud- Phishing is one of the most common forms of online fraud. In this method, fraudsters send fake emails, SMS messages, or links that appear to come from a bank, financial institution, or other trusted organisation. The victim may be asked to update account information or verify a transaction. When the victim enters confidential information through the fake link, the fraudster can misuse it.

2. OTP Fraud- In OTP fraud, criminals try to obtain the one-time password sent to a customer's mobile phone. They may pretend to be bank employees or customer-care representatives and create a false emergency to convince the victim to share the OTP. Once the OTP is obtained, it may be used to complete an unauthorized transaction.

3. UPI Fraud- UPI has made money transfers very convenient, but it is also misused by fraudsters. A person may receive a false payment request or be asked to scan a QR code for receiving money. In some cases, victims are wrongly told that entering a UPI PIN is necessary to receive a payment. Such tricks can result in money being transferred from the victim's account.

4. Debit and Credit Card Fraud- Card fraud occurs when criminals obtain or misuse debit or credit card information. Card details may be stolen through fake websites, fraudulent calls, compromised payment terminals, or other methods. The stolen information can then be used for unauthorized purchases or transactions.

5. Internet Banking Fraud- Internet banking fraud involves unauthorized access to a person's online banking account. Fraudsters may obtain login details through fake websites, phishing messages, malware, or social engineering. After gaining access, they may transfer money or make other unauthorized changes to the account.

6. Fake Customer-Care Fraud- Fraudsters sometimes create fake customer-care numbers or profiles and present themselves as representatives of banks, payment companies, shopping websites, or other service providers. They may ask customers to share confidential information or install software on their phones. This information can then be used to carry out fraudulent transactions.

7. SIM Swap Fraud- SIM swap fraud occurs when a criminal manages to obtain a replacement SIM card connected to another person's mobile number. Once the fraudulent SIM becomes active, the victim may stop receiving banking alerts and OTPs. The criminal can then attempt to misuse services linked to the mobile number.

8. Identity Theft- Identity theft involves the unauthorized use of another person's personal information. Fraudsters may misuse information such as identity documents, mobile numbers, account details, or other personal data to carry out financial transactions or obtain services in the victim's name.

9. Fake Loan and Investment Fraud- Fraudsters may offer quick loans, high-return investment opportunities, or attractive financial schemes through social media, websites, phone calls, and messaging applications. Victims may first be asked to pay processing charges, registration fees, or other amounts. After receiving the money, the fraudster may disappear without providing the promised service or investment.

10. QR Code Fraud- In QR code fraud, criminals send or display a QR code and convince the victim to scan it for receiving money, a refund, or another benefit. However, scanning the code may actually initiate a payment from the victim's account. This type of fraud is often successful because many users are not fully aware of how QR-based payments work.

11. Malware and Remote- Access Fraud- Some fraudsters persuade victims to download an unknown application or allow remote access to their mobile phones or computers. The software may allow criminals to view sensitive information or control parts of the device. Banking credentials and other confidential information may then be misused.

12. Social Media and Online Shopping Fraud- Fraudsters also use social media platforms and online marketplaces to deceive customers. They may advertise fake products, create false profiles, or offer products at unusually attractive prices. After receiving payment, they may fail to deliver the product or may use the transaction to obtain additional personal information.

Digital fraud in India is taking different forms as the use of online banking and digital payments continues to expand. Phishing, OTP fraud, UPI fraud, card fraud, fake customer-care calls, identity theft, QR code fraud, and investment scams are among the major methods used to target customers. Many such frauds depend not only on technical

weaknesses but also on deception, trust, urgency, and lack of awareness. Therefore, reducing digital fraud requires a combination of strong banking security, regular monitoring, effective complaint and reporting systems, and continuous customer awareness about safe digital practices.

Remedies and Preventive Measures Against Digital Frauds in India

The increasing use of digital banking has made financial services convenient, but it has also increased the risk of online fraud. Preventing digital fraud requires efforts from customers, banks, government agencies, and technology providers. The following measures can help reduce the risk of digital fraud in India.

1. Increase Customer Awareness- Banks should regularly educate customers about common forms of digital fraud. Awareness programmes can explain the risks of phishing, OTP fraud, UPI fraud, fake customer-care calls, and other scams. Customers should be clearly informed that genuine bank officials do not normally ask for confidential passwords, PINs, or OTPs.

2. Never Share Confidential Banking Information- Customers should never share their OTP, ATM PIN, internet banking password, UPI PIN, card CVV, or other confidential information with anyone. Such information should be kept private even when the caller claims to represent a bank or financial institution.

3. Verify Calls, Messages, and Links- Customers should not immediately trust messages, emails, phone calls, or links related to banking transactions. Before responding, they should independently verify the information through the bank's official website, mobile application, or verified customer-care channel.

4. Use Strong Passwords- Customers should create strong and different passwords for banking and other important accounts. Passwords should not be based on easily available information such as names, dates of birth, or mobile numbers. Regularly changing passwords can also improve account security.

5. Enable Transaction Alerts- SMS and email alerts can help customers identify unusual transactions quickly. Customers should keep transaction notifications active and check their account statements regularly. Any transaction that they do not recognize should be reported to the bank without delay.

6. Be Careful with UPI Payments- Customers should remember that a UPI PIN is generally used to authorize a payment, not to receive money. They should check the name and amount shown on the payment screen before approving a transaction. Unknown payment requests and QR codes should be treated carefully.

7. Avoid Unknown Applications and Remote Access- Customers should avoid downloading mobile applications from unknown sources. They should also not give remote access to their mobile phones or computers to unknown persons. Banking should preferably be conducted through official applications and trusted websites.

8. Secure Mobile Phones and Computers- Devices used for banking should have updated operating systems and security software. Screen locks, biometric protection, and other available security features should be enabled. Customers should also avoid carrying out sensitive banking transactions through unsecured public Wi-Fi networks.

9. Banks Should Strengthen Fraud Detection- Banks should continuously improve systems that identify unusual transactions. Automated monitoring, transaction limits, multi-factor authentication, and timely alerts can help detect suspicious activity. Banks should also regularly review their security systems as fraud methods continue to change.

10. Quick Reporting of Fraud- Customers should report fraudulent transactions to their bank as soon as they become aware of them. Early reporting can improve the possibility of stopping or recovering funds. Delay in reporting can make investigation and recovery more difficult.

11. Improve Customer Verification- Banks and financial institutions should use appropriate verification procedures before allowing sensitive account changes or unusual transactions. Additional checks may be useful when a transaction appears significantly different from a customer's normal banking behaviour.

12. Strengthen Digital and Financial Literacy- Digital literacy should be promoted along with financial literacy. Customers should understand how digital payments, UPI, cards, online banking, and authentication systems work. Special awareness efforts may be useful for people who have limited experience with digital technology.

13. Stronger Coordination Among Agencies- Banks, payment service providers, regulators, cybercrime authorities, and law-enforcement agencies should work together to respond to digital fraud. Sharing information about new fraud methods and suspicious activities can help institutions respond more quickly.

14. Regular Security Updates- Banks and technology providers should regularly update their applications and security systems. Security weaknesses should be identified and corrected as early as possible. Customers should also install official updates rather than continuing to use outdated software.

15. Promote a Culture of Caution- Customers should avoid making financial decisions under pressure. Fraudsters often create fear or urgency by claiming that an account will be blocked, a payment is pending, or a reward will expire. Taking a few minutes to verify such claims can prevent significant financial loss.

Digital fraud cannot be eliminated through a single measure. It requires a combination of technology, customer awareness, responsible banking behaviour, quick reporting, and effective institutional action. Banks need to strengthen their security and monitoring systems, while customers must remain careful about the information they share and the transactions they approve. Regular awareness programmes and improved digital literacy can further reduce the vulnerability of customers. A cooperative approach involving banks, customers, regulators, and law-enforcement agencies is therefore essential for creating a safer digital banking environment in India.

FINDINGS

Based on the review of digital frauds in the Indian banking sector, the following major findings can be identified:

1. Digital fraud is a growing concern. The rapid increase in mobile banking, internet banking and digital payments has created more opportunities for fraudsters to target bank customers.
2. Customers are commonly targeted through deception. Many frauds do not require advanced technical knowledge. Fraudsters often use fake calls, messages, links, offers, and false identities to gain the confidence of customers.
3. UPI-related fraud is an important area of concern. The convenience and speed of UPI payments can also be misused when customers approve unknown payment requests or follow misleading instructions.
4. Lack of awareness increases the risk of fraud. Customers who are not familiar with basic digital security practices may be more likely to share confidential information or follow fraudulent instructions.
5. OTP and banking credentials are frequently targeted. Fraudsters attempt to obtain OTPs, PINs, passwords, card details, and other sensitive information by pretending to be trusted persons or service providers.
6. Social engineering plays a major role. Fraudsters often exploit emotions such as fear, urgency, greed, or trust rather than depending only on technical weaknesses in banking systems.
7. Digital fraud affects customer confidence. Financial loss can make customers less confident about using online banking and digital payment services.
8. Banks need continuous improvement in security. As fraud techniques change, banks cannot depend only on existing security arrangements. Regular improvements in transaction monitoring, authentication, alerts, and fraud detection are necessary.
9. Quick reporting is important. Customers who identify suspicious transactions should report them immediately. Early reporting can improve the chances of taking timely action against fraudulent transactions.
10. Technology alone cannot solve the problem. Effective prevention requires both strong technological safeguards and responsible customer behaviour.
11. Digital literacy is an important preventive factor. Better understanding of online banking, UPI payments, phishing, fake customer-care calls, and other fraud methods can help customers make safer decisions.
12. Cooperation among stakeholders is necessary. Banks, customers, payment service providers, regulators, and law-enforcement agencies need to work together to control digital fraud and respond quickly to new forms of financial crime.

CONCLUSION

The study indicates that digital fraud is not only a technological problem but also an awareness and behavioural problem. Strong banking security must therefore be supported by customer education, digital literacy, careful transaction practices, and quick reporting mechanisms. A combined effort from customers, banks, government agencies, and technology providers is essential for making digital banking safer in India.

REFERENCES

1. Sharma, N., & Sharma, D. (2018). *Rising toll of frauds in banking: A threat for the Indian economy*. Journal of Technology Management for Growing Economies, 9(1), 71–88. https://doi.org/10.15415/jtmge.2018.91003
2. Sood, P., & Bhushan, P. (2020). A structured review and theme analysis of financial frauds in the banking industry. *Asian Journal of Business Ethics, 9*(2), 305–321. https://doi.org/10.1007/s13520-020-00111-w
3. Roy, N. C., & Prabhakaran, S. (2022). Internal-led cyber frauds in Indian banks: An effective machine learning-based defense system to fraud detection, prioritization and prevention. *Aslib Journal of Information Management, 75*(2), 246–296. https://doi.org/10.1108/AJIM-11-2021-0339

4. Sood, P., & Bhushan, P. (2022). Factors impacting banking frauds in India: A conceptual framework. *International Journal of Business and Globalisation, 31*(4), 500–519. https://doi.org/10.1504/IJBG.2022.127129
5. Lonkar, A., Dharmadhikari, S., Dharurkar, N., Patil, K., & Phadke, R. A. (2024). Tackling digital payment frauds: A study of consumer preparedness in India. *Journal of Financial Crime, 32*(2), 257–278. https://doi.org/10.1108/JFC-01-2024-0029
6. Chandra, D. (2025). Examining the contours and challenges of National Cybercrime Reporting Portal in countering digital financial frauds. *Journal of Victimology and Victim Justice, 8*(1), 65–83. https://doi.org/10.1177/25166069241306546
7. Puri, et al. (2025). *Digital financial fraud: A review and research agenda*. Journal of Economic Surveys