

ANALYSING THE REGULATORY FRAMEWORK: ENSURING SECURITY AND TRUST IN THE DIGITAL ECOSYSTEM

Jyoti Sharma*

ABSTRACT

Digital India initiative led the foundation for digital economy, which has shown impact on every sector of economy. The financial payment system in India focused on digital payments to be a part of Digital India programme. For the transparency of financial system demonetisation played sustainable role in providing boost to digital payment which has affected the ecosystem of security in payment system by cyber security problem with increased frauds. A safe and congenial environment is required for cashless economy that provide prevention of frauds. Therefore, the study of regulatory framework is important to control the financial payment system by its legislation including rules and regulations.

KEYWORDS: Regulatory, Framework, Security, Ecosystem, Frauds.

Introduction

India has experienced a remarkable increase in digital payments since the COVID-19 pandemic began. This growth is driven by several factors, including advancements in payment technology, favourable government regulations, the extensive use of smartphones with more affordable mobile internet access. Payment service providers, both established and new, have been instrumental in this transformation by delivering seamless, secure, and cost-effective payment solutions, further boosting the adoption of digital transactions across the nation.

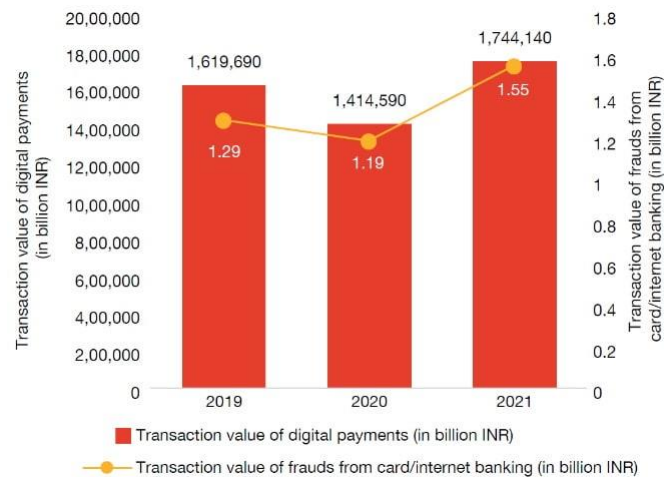
Digital payments have surged in India through various methods, such as cards, wallets, the Unified Payments Interface (UPI), mobile banking, and QR codes. Among these, UPI has emerged as a game-changer, revolutionizing payment processes. In the fiscal year 2021-22, UPI transactions soared to an astonishing 46 billion, making up a substantial portion of the total 72 billion digital payment transactions processed during that time. This phenomenal growth marks a 109% increase from the previous year's volume of 22 billion, highlighting UPI's crucial role in enhancing India's digital payments landscape.

However, the extensive implementation of digital payment systems has also led to a rise in fraudulent activities, as criminals increasingly exploit system vulnerabilities and human error. A recent report from the Reserve Bank of India (RBI) has identified a troubling trend of escalating financial fraud in the country. The report, covering the period from 2019-20 to 2021-22, found that the number of frauds reported by financial institutions involving cards and internet banking rose by 34%, from 2,677 in 2019-20 to 3,596 in 2021-22. Additionally, the value of fraudulent transactions increased by 20%, from INR 1.29 billion in 2019-20 to INR 1.55 billion in 2021-22. Card and internet-related frauds constituted 0.2% of the total value of fraudulent transactions in 2021-22, up from 0.1% in 2019-20. Overall, the incidence of payment frauds as a percentage of total digital payments in India rose from 0.008 basis points in 2019-20 to 0.0089 basis points in 2021-22.

* Research Scholar, Department of Commerce, Indira Gandhi University, Meerpur, Haryana, India.

The surge in technological advancements has also given rise to more organized and sophisticated fraud schemes, including targeted hacking of networks and databases, as well as phishing attacks. This increase in fraud is a significant concern for consumers, especially given the vast amounts of sensitive card information being stored and transferred digitally. Fraudsters are increasingly taking advantage of vulnerabilities in digital systems to access this data for malicious purposes.

Value of Frauds vis-a-vis the Digital Payments Transactions (Cards and Internet Banking)



Source: www.pwc.in

Digital Payments Frauds in India

Payment fraud is a multifaceted issue shaped by various factors, including local payment habits, customer awareness, the security of payment systems, regulatory frameworks, the maturity of the payments industry, technological advancements, and prevailing economic conditions. The payments ecosystem is a complex network involving multiple stakeholders, such as banks, networks, payment gateways, sellers, merchants, customers, and buyers. Each participant carries inherent risks that can contribute to instances of fraud.

The process of payment transfer from customers to merchants involves a network of interconnected entities, each vital for ensuring secure and efficient transactions. When a customer initiates a payment, their information passes through various entities, including the merchant's payment gateway, processor, the customer's bank that issued the card, and the card network. Throughout this process, numerous checks and validations occur to confirm the transaction's legitimacy and prevent fraudulent activities.

Despite a robust infrastructure, fraudsters continue to develop clever methods to exploit vulnerabilities within the payments ecosystem. The following section explores some common techniques employed by these malicious actors.

The RBI's Annual Report for 2020-21 indicates a significant increase in both the volume and value of payment frauds incidents in India. In response, the RBI has outlined measures to combat these issues in a recent press release. This report examines prevalent fraud schemes in the Indian context, highlighting common methodologies used by fraudsters and the most commonly used payment instruments and channels that are most susceptible to these crimes.

Common Fraud Techniques

- **Identity Theft/Impersonation:** Criminals increasingly target personal information for financial fraud, stealing sensitive data such as PAN/Aadhaar details, social media credentials, and bank account information. This stolen data is often used to gain unauthorized access to individuals' accounts and initiate fraudulent transactions. In some instances, fraudsters open new payment accounts in victims' names, aided by the availability of personal data on the dark web. Numerous incidents in India have reported victims discovering unauthorized transactions made with their personal information, including the misuse of credit card facilities.

- **Phishing/Vishing:** The rise of digital transactions in India has been accompanied by an uptick in phishing and vishing scams. Vishing fraudsters impersonate bank customer service representatives, tricking customers into updating or completing their e-KYC online to maintain account activity. During this process, fraudsters capture sensitive information and use shared OTPs for unauthorized transactions, often keeping the customer on the phone to avoid detection. Phishing scams involve sending emails or text messages with malicious links redirecting customers to fake websites that mimic genuine bank sites, leading them to unknowingly disclose confidential information.
- **Web Skimming:** Cybercriminals use a technique known as web skimming to steal sensitive payment information by injecting malicious software into payment pages on websites or applications. This malware captures confidential data like credit card numbers, expiration dates and CVV codes. E-commerce websites are prime targets due to their popularity and the vast amounts of sensitive data they process. Numerous cases of web skimming in India have highlighted the urgent need for businesses to implement strong cybersecurity measures to protect customer information.
- **Social Engineering:** Attackers often employ deceptive tactics to manipulate individuals into revealing sensitive information or taking actions that compromise their security. These tactics frequently involve impersonating trusted organizations or individuals, such as bank representatives or tech support specialists. By exploiting human vulnerabilities like fear, urgency, or curiosity, attackers can trick victims into disclosing personal details or clicking on malicious links.
- **Account Takeover:** Account takeover fraud occurs when fraudsters gain unauthorized access to a user's account, typically by stealing their login credentials. Once inside, they can make unauthorized payments, alter personal information, or lock the user out of their account. Often, fraudsters quickly change account details like passwords or email addresses, making difficult to realize their accounts have been compromised.
- **QR Code Scams:** Scammers are increasingly using QR codes to deceive individuals into granting access to their bank accounts. Posing as customer service representatives or even friends, they may ask victims to scan a seemingly legitimate QR code with their phones. However, this code often links to a malicious website or app that prompts users to enter personal information or approve transactions, allowing scammers to steal money.
- **SIM Swap/SIM Cloning:** Cybercriminals target bank account holders by gaining control of their mobile phone numbers, either by acquiring the customer's SIM card or creating a duplicate SIM, including electronic SIMs. Once they control the SIM, they can intercept one-time passwords (OTPs) sent for two-factor authentication, using these to authorize fraudulent transactions. Often, cybercriminals impersonate telephone or mobile network employees to gather personal information under the guise of offering free upgrades or additional benefits.
- **Juice Jacking:** Public charging stations can be convenient but pose significant security risks. Fraudsters can exploit these stations to install malware on unsuspecting users' phones, gaining access to personal data such as emails, text messages, and saved passwords. This tactic, known as juice jacking, involves tampering with charging ports to transfer malicious software or extract data from connected devices.

Literature Review

A thorough review of studies on the regulatory and legislative landscape for financial fraud prevention emphasizes the vital role banker association's play in addressing credit card fraud. Setting clear principles and policies is critical to protecting the interests of both banks and merchants (**Dave Arthur Williams, 2007**).

To strengthen security awareness among current and prospective internet banking users, collaborative education programs should be created and implemented through partnerships among banks, universities, and government agencies. These programs should provide essential information on potential risks and threats (P Subsorn, S Limwiriyakul, 2010).

In the field of e-payment settlements, safety standards must be continually adapted and enhanced to cover authorization, authenticity, confidentiality, minimum benefits, integrity control, and

auditing. Utilizing Information and Communication Technology (ICT) solutions—such as Secure Socket Layer (SSL), Secure Hypertext Transfer Protocol (HTTPS), e-signatures, and personal identity cards—can greatly strengthen the security of electronic financial transactions (Dale Dzemydiene, Ramute Naujikiene, Marius Kalinauskas, Eugenijus Jasiunas, 2010).

Effective credit card fraud prevention requires a comprehensive approach that includes addressing root causes, implementing thorough fraud prevention policies, promoting fraud awareness, leveraging technology-driven protections, establishing strong identity management systems, and encouraging legal deterrence measures. This collective effort should engage various user institutions, networks, governments, and industries (Hendi Yogi Probowo, 2011).

Research has shown that security strategies such as firewalls, password authentication, encryption, Secure Socket Layer (SSL), and virtual keyboards have been effective when implemented in Zimbabwe (Tafadzwa Zimucha, Ngonidzashe Zanamwe, and Kerina Chimwayi, 2012).

Consumers and merchants need to be aware of the risks tied to e-payment systems. Organizations should establish strong safeguards against internal tampering and adopt effective strategies to detect, prevent, and eliminate fraud (Lina Fernandes, 2013).

As payment innovations evolve, the security provisions of the Payment Services Directive must be regularly assessed and updated. It is critical to thoroughly compare existing regulations with new recommendations to prevent fraud under the revised Payment Services Directive (Kovacs Levente and David Sandor, 2016).

The Payment Card Industry Data Security Standard (PCI DSS) outlines guidelines and controls for securely storing and processing sensitive card information. Standardizing and centralizing these practices can reduce the risk of data fraud attacks (Mohammed Aamir Ali, Budi Arief, Martin Emms, and Aad Van Moorsel, 2017).

Governments and regulatory bodies should adopt various strategies to encourage digital payments, such as licensing payment banks, promoting mobile wallet usage, and removing service charges on digital and card transactions. Additionally, awareness campaigns should be conducted to train the public on the benefits of digital payments (Preeti Garg, 2018).

Institutional factors, such as insufficient monitoring and limited client education, can greatly increase banks' and clients' vulnerability to electronic banking fraud. Strengthening security protocols and raising awareness about PIN protection are among the most impactful measures to help prevent fraud (Amoh John, Kenneth Ofori-Boateng, and Awunyo-Vitor Dadson, 2020).

Research Methodology

- The present study is descriptive in nature.
- The present paper aims to study the regulatory framework in India that monitors digital payments.
- The secondary data is taken for the study.

Regulatory Framework in India

In India, the regulatory framework for digital payments is managed by several organizations collaborating to ensure consumer protection, mitigate fraud, and encourage responsible financial innovation. These entities play a vital role in maintaining the integrity of the digital payments ecosystem and fostering user trust.

- **Reserve Bank of India (RBI):** As the central bank of India, the RBI is primarily responsible for overseeing the financial system, including digital payments. It issues guidelines and regulations to enhance security, risk management, and customer protection within the digital payments sector. Key initiatives include:
- **Master Circular on Fraud Risk Management in Digital Payments:** This detailed circular sets forth the RBI's expectations for banks and payment service providers regarding the management of fraud risks in digital transactions.
- **'BE(A)WARE' Campaign:** The RBI's 'BE(A)WARE' initiative aims to educate consumers about digital payment security practices and raise awareness of prevalent fraud tactics.

- **National Payments Corporation of India (NPCI):** Established by the RBI, NPCI is a non-profit organization that manages retail payment infrastructure and systems in India. It operates various payment platforms, including the Unified Payments Interface (UPI), which has transformed digital payments in the country. NPCI's role in fraud prevention includes:
- **Fraud Monitoring and Alert System:** NPCI operates a real-time system to monitor and alert on fraudulent transactions across its platforms.
- **Tokenization of Sensitive Card Data:** NPCI advocates for tokenization, which replaces sensitive card data with unique tokens to minimize data breach risks.
- **Indian Computer Emergency Response Team (CERT-In):** CERT-In is the national cybersecurity agency responsible for coordinating cybersecurity initiatives in India. It plays a crucial role in addressing cyberattacks and security vulnerabilities that may affect digital payments. CERT-In's activities include:
 - Issuing advisories and alerts about cybersecurity threats and vulnerabilities.
 - Coordinating response efforts in the event of cyberattacks.
 - Promoting cybersecurity awareness and training among stakeholders in digital payments.
- **Ministry of Electronics and Information Technology (MeitY):** MeitY oversees the broader policy framework for digital payments in India. It collaborates closely with the RBI and other regulatory bodies to ensure a secure environment for digital transactions. MeitY's initiatives include:
- **Digital Payments Security Guidelines:** MeitY has issued guidelines outlining standards and best practices for digital payment security across various stakeholders.
- **Promotion of Digital Payments Infrastructure:** MeitY supports the development and incorporation of digital payment infrastructure throughout India, encouraging the acceptance of digital payments in various sectors.
- **Cybersecurity and Infrastructure Protection Agency (CIPA):** Recently established within MeitY, CIPA aims to enhance India's cybersecurity measures and protect critical information infrastructure. Its responsibilities in digital payments security include:
 - Identifying and mitigating cyber threats to digital payment systems.
 - Alongside regulatory bodies to formulate and implement cybersecurity measures.
 - Promoting cybersecurity awareness and training among stakeholders involved in digital payments.

Alongside the main regulatory bodies, several other organizations play vital roles in regulating and managing digital payments in India, consisting of:

- **Financial Intelligence Unit (FIU-India):** This unit monitors and analyzes financial transactions to prevent financial crimes, particularly those associated with digital payments.
- **Cyber Police:** Responsible for investigating cybercrimes, the Cyber Police focus on threats targeting digital payment systems.
- **Adjudication Committees:** Established under the Payment and Settlement Systems Act (PSS Act), 2007, these committees handle disputes and complaints related to digital payments.

Together, these organizations create a comprehensive regulatory framework designed to ensure the safety, security, and integrity of digital payments in India, thereby fostering trust and encouraging financial inclusion throughout the country.

Conclusion

Digital payments have turned into a transformative force in India's economy, fueled by the government's commitment to a cashless society and rapid technological advancements. To adapt to this evolving digital payment landscape, India's legislative framework has been continuously refined, with the Payment and Settlement Systems Act (PSS Act) as a key pillar for ensuring security and protecting privacy. Merchants play an essential role in maintaining the integrity of the digital payments sector by adhering to established standards.

As India moves toward a more digitized economy, the future of digital payments appears promising, with the sector set for significant growth. The adoption of innovative technologies like UPI and e-RUPI, alongside the increasing use of smartphones and the internet connectivity, will further drive the increase in digital transactions. The shift towards cashless economy is expected to accelerate in the coming years, enhancing convenience and promoting financial inclusion for millions of Indians.

References

1. <https://rbidocs.rbi.org.in/rdocs/content/pdfs/BEAWARE07032022.pdf>
2. <https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/PR163037E920A47573411FBC7D79B058FED34A.PDF>
3. https://www.rbi.org.in/scripts/FS_Speeches.aspx?Id=1022&fn=2
4. <https://www.getastra.com/blog/knowledge-base/cert-in-certification/>
5. Arthur Williams, D. (2007). Credit card fraud in Trinidad and Tobago. *Journal of Financial Crime*, 14(3), 340–359.
6. Subsorn, P., & Limwiriyakul, S. (2010). A Comparative analysis of internet banking security in Thailand: A customer perspective. *Procedia Engineering*, 32, 260–272.
7. Dzemydienė, D., Naujikiėnė, R., Kalinauskas, M., & Jasiūnas, E. (n.d.-a). VE RI TIA TAS IVS TI EVALUATION OF SECURITY DISTURBANCE RISKS IN ELECTRONIC FINANCIAL PAYMENT SYSTEMS. *Online) INTELEKTINĖ EKONOMIKA INTELLECTUAL ECONOMICS*, 2010(2), 21–29.
8. Yogi Prabowo, H. (2011). Building our defence against credit card fraud; a strategic view. *Journal of Money Laundering Control*, 14(4), 371–386.
9. Zimucha, T., & Zanamwe, N. (2012). Journal of Internet Banking and Commerce An Evaluation of the Effectiveness of E-banking Security Strategies in Zimbabwe: A Case Study of Zimbabwean Commercial Banks. In *Journal of Internet Banking and Commerce* (Vol. 17, Issue 3).
10. Fernandes, L. (2013a). FRAUD IN ELECTRONIC PAYMENT TRANSACTIONS: THREATS AND COUNTERMEASURES. In *Asia Pacific Journal of Marketing & Management Review* (Vol. 2, Issue 3).
11. Kovács, L., & David, S. (2016a). Fraud risk in electronic payment transactions. *Journal of Money Laundering Control*, 19(2), 148–157.
12. *Moving towards a digital economy Critical security and fraud control measures to embrace.* (2017).
13. Garg, P., & Panchal, M. (2017). Study on Introduction of Cashless Economy in India 2016: Benefits & Challenge's. *IOSR Journal of Business and Management*, 19(04), 116–120.
14. Amoh, J. K., Awunyo-Vitor, D., & Ofori-Boateng, K. (2020). Customers' awareness and knowledge level of fraudulent acts in electronic banking in Ghana: Evidence from a universal bank. *Journal of Financial Crime*, 28(3), 870–882.

