Impact Factor – (SJIF) –8.632 ISSN – 2278-9308

B.Aadhar

Single Blind Peer-Reviewed & Refereed Indexed

Multidisciplinary International Research Journal

March -2024

ISSUE No - (CDLXIII) 463

75th Years of Indian Economy: Achievements and Challenges

Prof. Virag.S.Gawande
Chief Editor
Director
Aadhar Social Research &, Development Training Institute, Amravati.

Dr. R. K. Shanediwan
Executive-Editors
Principal,
Shri Shahaji Chhatrapati Mahavidyalaya, Kolhapur

Prof. Dr. Mrs. S. S. Rathod
Editor
Shri Shahaji Chhatrapati Mahavidyalaya, Kolhapur

Dr. D. P. Gawade
Co-Editor
Shri Shahaji Chhatrapati Mahavidyalaya, Kolhapur

Aadhar International Publication
For Details Visit To : www.aadharsocial.com

B.Aadhar International Peer-Reviewed Indexed Research Journal
Impact Factor -(SJIF) –8.632, Issue NO, (CDLXIII) 463
ISSN : 2278-9308
March, 2024

Unmasking the Shadows: Understanding and Preventing Digital Fraud in UPI Banking Transactions.

Shivani j Patil [1], Dr. Smt.M.B.Desai[2]
1.Research Fellow, Department of Economics, Shivaji University Kolhapur
2.Professor, Dept. of Economics, R. C. Shahu College, Kolhapur

Abstract:
The introduction of the Unified Payments Interface (UPI) in India has led to an increase in digital fraud, including traditional methods like phishing, social engineering, and SIM swapping. The article underlines the need to maintain user alertness, protect UPI PINs and OTPs, and implement security processes. It emphasizes the duties of banks and governments in maintaining a safe digital payment environment. Banks should strengthen their security measures, educate their consumers, and provide effective dispute-resolution systems. The Reserve Bank of India plays an important role in establishing rules and safeguarding consumers.

Introduction

In recent years, the rise of digital banking and payment methods has revolutionized the way we handle our financial transactions. One such method that has gained immense popularity in India is the Unified Payment Interface (UPI) system. It is a real-time payment system that allows users to transfer funds between bank accounts using a mobile application. With its ease of use and convenience, UPI has become the go-to choice for millions of people in India. However, this rapid growth has also attracted the attention of fraudsters, who are constantly finding new ways to exploit vulnerabilities in the system. In this paper, we will explore the world of digital fraud in UPI banking transactions, understand its causes, and discuss preventive measures to safeguard against it.

UPI (Unified Payments Interface) is a popular digital payment method in India, but it is becoming increasingly susceptible to fraudulent activities. To prevent UPI scams, avoid sharing your PIN or OTP with anyone, verify recipient details before sending money, use a strong PIN, avoid public Wi-Fi, keep your phone and UPI app updated, and report suspicious activity to your bank. Be cautious of unsolicited calls, download apps from untrusted sources, monitor transaction history, and set daily transaction limits. To protect UPI transactions, use a strong PIN, enable multi-factor authentication, use a screen lock, avoid public Wi-Fi, and regularly update your operating system. Stay alert for suspicious activity and verify information before sending money. If scammed, contact your bank, create a new strong PIN, or report the fraudulent activity to the National Payments Corporation of India (NPCI).

Review of literature:

This document provides an overview of recent cybercrime incidents and arrests in India, including the Chandigarh Police busting a Jamtara gang, information about a chartered accountant's loss to fraudsters, Google's AI cybersecurity tools, and the arrest of a Chennai woman who gave away bank accounts to online fraudsters. It promotes government programs including a National Cybercrime Reporting Portal and a National Helpline number, as well as citizen vigilance and prompt reporting.(cyber digest).Tthe report covers the expansion of digital payments in India, as well as the rising fraud concerns that accompany them. It exposes the weaknesses that fraudsters exploit in emerging payment systems, such as hacking and phishing attempts. Identity theft, phishing, online skimming, and social engineering are all common types of fraud. The document underlines the need of establishing fraud risk management procedures in order to save operating costs, protect reputation, and retain consumers. It suggests strategies such as fraud orchestration, consumer awareness, fraud governance framework, simulation testing, analytics, and real-time monitoring. (PwC).The document investigates COVID-19's impact on digital payments in India, focusing on the shift in consumer behavior toward online transactions. According to an NPCI and PRICE poll, digital payment adoption is growing across all socioeconomic categories, with a significant number of households using these methods. There is a mismatch between smartphone owners and digital payment users that must be addressed via education, particularly in online banking. The study underlines the banking sector's strong digital connection with clients, particularly those in low-income households, as well as the success of the Direct Benefit Transfer (DBT) distribution system. Overall, the statement emphasizes the trend toward digital payments in India and the need of empowering customers while also enhancing the safety and efficiency of online

199

transactions.(Bijapurkar, shukla and Rai).The article investigates the adoption of digital payment

	Domestic Payment Frauds			
	Volume (Lakh)	Value (Crore)	One in every X payment transaction fraudulent	FTS (Fraud / Payment Value * 10000)
September 2022	1.71	249	58177.41	0.127 bps
October 2022	1.79	220	59533.35	0.127 bps
November 2022	2.06	257	50620.69	0.143 bps
December 2022	1.54	204	72426.75	0.103 bps
January 2023	1.57	195	71681.44	0.106 bps
February 2023	2.29	317	47018.00	0.177 bps
March 2023	2.25	333	53907.48	0.142 bps
April 2023	1.75	273	68927.36	0.152 bps
May 2023	2.03	285	63051.71	0.147 bps
June 2023	1.74	265	72554.96	0.128 bps
July 2023	2.24	286	59898.87	0.146 bps
August 2023	2.40	320	58391.71	0.157 bps
September 2023	2.52	366	55057.76	0.174 bps
October 2023	2.23	335	66950.05	0.164 bps
November 2023	2.57	428	57618.81	0.209 bps
December 2023	2.92	432	53327.09	0.187 bps
January 2024	2.69	435	58505.69	0.199 bps
Total	36.3	5200	1027643	0

systems and related variables, examining research from 2015 to 2020. It highlights motivations and barriers, such as customer expectations for transaction performance and simplicity of use, perceived risk, and a lack of trust. The authors believe that overcoming these constraints is critical for reaping the full benefits of digital payments. (Sahi, Khalid and abbas).The document highlights the growing importance of digital payments in the Indian banking sector and the risk of cyber crimes, particularly digital payment frauds. It advocates for proactive fraud mitigation measures to build customer trust. The scheme for fraud data collection and use includes five process levels: monitoring, prediction, detection, analysis, and reporting. The Reserve Bank of India's regulatory guidelines are also discussed. The paper emphasizes the importance of reinforcing internal fraud control mechanisms to secure digital payments and uphold customer trust. (Priya, Ahmed and Alam)

Research gap:

A lot of research has been conducted on the digital payment system and its benefits, yet there have been few studies on digital fraud in UPI financial transactions in India. This is a national approach. There is no one study on assessing the risk of digital fraud, hence there is a strong need to research digital payments.

Research Methodology:

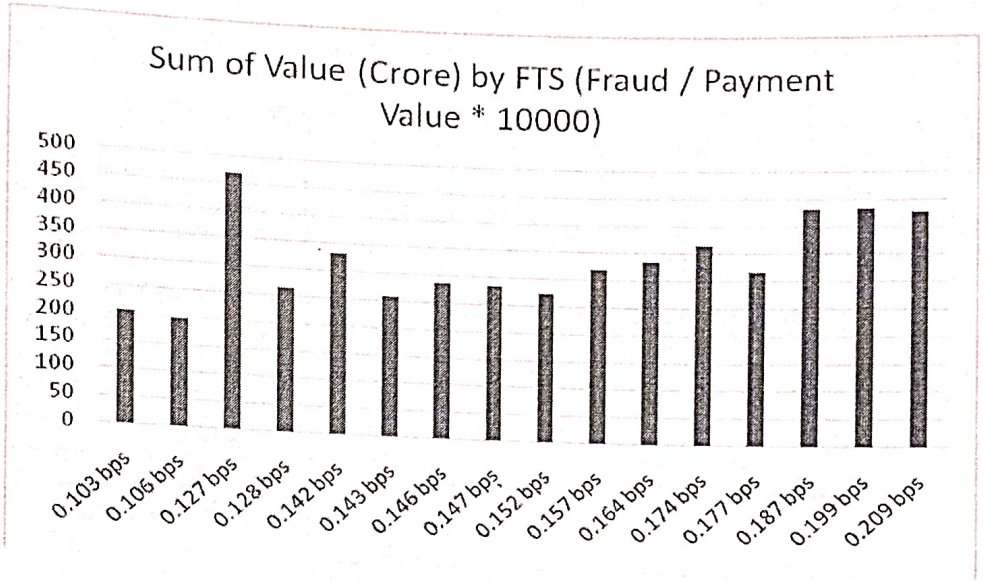
The current research papers evaluate digital fraud in UPI financial transactions. This research paper is based on secondary data gathered from many sorts of websites, government surveys, and publications.

Combating Fraud in the Age of Digital Payments, Cyber Security Awareness for Citizens, and Digital Payment Adoption: A Review (2015-2020). To support the result and identify the research gap.

Objective of the paper:

1) To Understand the type and scope of digital fraud in UPI financial transactions in India.
2) To explain digital fraud and preventative measures in the context of UPI banking transactions.

(rbiwebsite.gaush1)



Above table and graph data on domestic payment fraud in India from September 2022 to January 2024. It displays the volume (Lakh) and total value (Crore) of fraudulent transactions, with a frequency of one in every X. The Fraud-to-Sale ratio (FTS) assesses fraudulence risk by dividing the value of fraudulent transactions by the overall transaction value. The volume of fraudulent transactions varies, with February 2023 having the greatest (2.29 lakh) and September 2022 having the lowest (1.71 lakh). The frequency of fraudulent transactions appears to be decreasing, with the "One in every X" number gradually increasing from September 2022 to January 2024. The FTS (fraudulence risk) typically remains around 0.2 basis points, indicating a comparatively low degree of fraud compared to the total transaction value.

Key point of UPI and digital fraud concept :

1. UPI's rising popularity: UPI has become a popular digital payment system in India, but it has also attracted scammers.
2. Understanding digital fraud: The article outlines and describes the many types of digital fraud in UPI transactions, including phishing, social engineering, and SIM swapping.
3. Balancing convenience and security: UPI is convenient, but it demands care and adherence to safe standards to maintain secure transactions.
4. Individuals should exercise caution when providing personal information, utilize trusted app stores, use strong passwords, and monitor transactions for unusual behavior.
5. Banks and governments have different roles. Banks are in charge of educating clients and putting security measures in place. The government contributes to raising awareness and upgrading UPI's security framework.

Understanding Digital Fraud in UPI Banking Transactions:

Digital fraud in UPI financial transactions is defined as any fraudulent or illegal behavior that occurs during the transmission of funds via the UPI network. It may take numerous forms, including as phishing assaults, SIM swapping, counterfeit software, and social engineering scams. The ultimate goal of these fraudsters is to gain the user's UPI PIN or bank data and then use these to transfer funds from the victim's account to their own. One of the primary causes of the current rise in digital fraud in UPI transactions is the rising usage of smartphones and the internet. As more people utilize digital banking,

fraudsters might target a large number of potential victims. Furthermore, a lack of understanding and information about the risks associated with digital transactions exposes consumers to falling victim to these frauds.

The RBI has devised a framework to reduce customer responsibility in cases of unlawful transactions. This prevents consumers from losing a large sum of money via no fault of their own. To avoid digital fraud in UPI transactions, consumers should be aware of the numerous approaches employed by fraudsters, such as sending bogus emails, establishing phony websites, and employing social engineering techniques. To prevent these assaults, users should never divulge their UPI PIN or bank information with anybody, even bank authorities. They should contact the bank directly if they have any questions. When downloading programs or clicking on links from unknown sites, users should always utilize reputable sources such as the Google Play Store or Apple App Store. In addition, users should protect their mobile devices with strong, unique passwords and activate two-factor authentication for all online accounts. Regularly examining bank records for suspicious activity and reporting unlawful transactions to the bank are critical measures in preventing fraud.If any illicit transactions are discovered, consumers should notify the bank and block their UPI account.

The Role of Banks and Government in Preventing Digital Fraud in UPI Transactions:

Banks and the government play critical roles in combating digital fraud in UPI transactions. Banks must educate clients about different forms of fraud and protect their accounts. The government and RBI improved the security of digital payments, including UPI, by implementing 'tokenization' in 2018 and launched a national-level awareness campaign, the 'UPI Challenge,' to educate people about the benefits and hazards of UPI transactions. Both banks and the government must put in place strong security measures to detect and prevent fraudulent activity.

Banks:

1.Security Measures	Banks need to have powerful encryption, secure multi-factor authentication, and periodic transaction monitoring for unusual patterns in place on their UPI platforms.
2.Fraud Detection and Prevention Systems	Banks ought to invest in fraud detection and prevention technologies that can instantly detect and stop fraudulent transactions using artificial intelligence and machine learning.
3.Customer Education	It is the duty of banks to inform their clientele about the dangers of UPI fraud and recommended procedures. This may be accomplished by means of educational campaigns, instructional content on their applications and websites, and unambiguous lines of contact for reporting questionable conduct.
4.**Dispute Resolution and Reimbursement:**	Banks should have efficient mechanisms for customers to report fraud and initiate a dispute resolution process. Ideally, this should include procedures for reimbursement in cases of proven fraudulent transactions.

Government (RBI):

Regulations and Guidelines:	The RBI establishes regulations and standards for UPI transactions. These rules describe how banks should approach fraud prevention, detection, and reporting.
Central Payments Fraud Information Registry (CPFIR):	The RBI maintains a central register where UPI fraud may be reported. This enables banks to share information about fraudulent activity and detect trends.
Customer Liability Framework:	The RBI has devised a framework to reduce customer responsibility in cases of unlawful transactions. This prevents consumers from losing a large sum of money via no fault of their own.

Suggestions and recommendations :

1) Never disclose your UPI PIN or OTP with anybody.
2) Enable secure passwords and Multi-Factor Authentication (MFA) in your UPI application.
3) Be cautious while inputting UPI IDs and verify recipient data before beginning transactions.
4) If you see any suspicious activity or unlawful transactions, notify your bank immediately.

Conclusion:

UPI's popularity has made it susceptible to fraud; nevertheless, users may remain attentive by knowing the various strategies employed by fraudsters and adopting safe measures such as securing UPI PINs and OTPs. Furthermore, banks must constantly enhance security measures and educate customers, while the government should continue to develop legislation and safeguard consumers. Through coordinated efforts, all UPI users may benefit from a better and more secure digital payment environment

References

" cyber digest." 20 feb 2024.

Bijapurkar, Rama, et al. "Digital Payment Adoption in India,2020." 2020.

Priya, Neha, Jawed Ahmed and m.Afshar Alam. "Digital Payments: A scheme for Fraud Data Collection and use in Indian Banking Sector." (2020).

PwC, india. "Combating fraud in the era of digital payment." May 2022.

rbiwebsite.gaush1. *PAYMENT SYSTEM INDICATORS*. January 2024. <https://www.rbi.org.in/Scripts/PSIUserView.aspx>.

Sahi, Alaa Mahdi, Haliyana Khalid and Alhamzah Fadhil abbas. "Digital Payment Adoption : A Review (2015-2020)." *Journal of Management Information and Decision Sciences* January 2021.