UPI FINANCIAL FRAUDS IN INDIA: - "AN EMPIRICAL AND LEGAL STUDY OF PUBLIC AWARENESS, CONSUMER PROTECTION AND PREVENTIVE MEASURES.

ABSTRACT

In India, with the growing use of UPI, concerns related to financial fraud, public awareness, consumer protection, and complaint redressal have increased. This study focuses on users' awareness, methods of fraud prevention, consumer protection, and the existing legal and regulatory framework. Its aim is to study users' awareness of different types of fraud, safe payment behavior, and preventive measures. In this study, an empirical research approach is used along with secondary sources. Primary data were collected from active UPI users through a questionnaire prepared using Google Forms. The collected data were analyzedusing descriptive statistics.

The findings of the study highlight a lack of awareness about certain reporting mechanisms, delays in bank responses, and difficulties in coordination among the concerned institutions. Although the Information Technology Act, 2000, and the BharatiyaNyayaSanhita, 2023, provide a necessary legal framework, legal provisions alone are not enough to ensure effective consumer protection. Timely assistance, a simple complaint process, and appropriate support for victims are also necessary. Therefore, this study suggests strengthening reporting mechanisms, improving institutional coordination, increasing cyber security awareness, and developing victim-centric solutions. In conclusion, a coordinated approach involving prevention, consumer protection, and prompt complaint redressal is essential to address UPI financial fraud effectively.

Keywords: Unified Payments Interface (UPI), Financial Fraud, Consumer Protection, User Awareness, Information Technology Act 2000, BharatiyaNyayaSanhita(BNS) 2023, 1930 Helpline.

1. INTRODUCTION

In India, digitalization has significantly changed the way financial transactions are conducted. Digital payment systems have provided users with the facility to make payments electronically

UNDER PEER REVIEW IN IJAR

instead of relying only on traditional cash-based transactions. The digital payment ecosystem in India has continued to grow and develop over time.

The Unified Payments Interface (UPI) is animportant part of the digital payment system in India. It was developed by the National Payments Corporation of India (NPCI). UPI enables users to make direct digital payments from their bank accounts to another person or merchant. For this purpose, users can use a mobile phone and a UPI-enabled application. UPI has played apivotal role in facilitating instant digital payments between different bank accounts.

In recent years, the use of UPI has rapidly increased in India. UPI enables both person-to-person and person-to-merchant digital payments. Due to its simplicity, quick payment facility and widespread acceptance, it has become an essential channel for daily financial transactions. The increasing transaction volume and transaction value of UPI also reflect its growing use.

With the increasing use of UPI, the risk of related financial fraud has also become asignificant matter of concern. Fraudsters may mislead or deceive UPI users through different methods. These may include techniques such as fake customer-care calls, phishing links or messages, fake QR codes, screen-sharing or remote-access applications, and attempts to make users enter their UPI PIN under the pretext of receiving money. Therefore, not only technical security measures but also users' awareness and behavior may play acrucial role in preventing such fraud.

To understand UPI fraud, studying only technical preventive measures is not sufficient. Users' awareness and behaviorplays a critical role for fraud prevention. It is necessary for users to understand when and in which situations their UPI PIN, OTP and other authentication information should be used. If a person trusts or follows a fraudster's misleading instructions, the person may unknowingly take an action that could result in financial loss. Therefore, the study of public awareness, safe payment practices and user behavior is necessary in the context of UPI fraud.

After a fraud occurs, protecting the transaction alone is not sufficient; appropriate consumer protection and grievance redressal are also vital for the affected person. In the situation of a fraudulent transaction, victims need timely reporting, complaint registration and access to

UNDER PEER REVIEW IN IJAR

available dispute-resolution mechanisms. Therefore, it is imperative to understand how the present system provides protection and assistance to fraud victims and how effective the complaint and redressal process is. In this study, consumer protection is examined as afundamental aspect of UPI fraud.

UPI financial fraud is not only a technological or behavioral problem but also has asignificant legal and regulatory dimension. In India, various laws and regulatory mechanisms apply to electronic transactions, cyber offences, banking transactions and consumer protection. In cases of UPI fraud, these legal and regulatory provisions play an important role. Therefore, this study will examine the existing legal and regulatory framework and will also seek to understand how this framework relates to the prevention, protection and redressal of UPI fraud.

2. <u>LITERATURE REVIEW: -</u>A systematic summary of existing studies in this area and their main findingsare presented in the table below.

S. No.	Details of Literature	Area of Research / Key Findings
1	Title: Unified Payment Interface-An Advancement in Payment Systems Author: Rahul Gochhwal Year:2017 Journal: American Journal of Industrial and Business Management, Vol. 7, No. 10 Methodology: Empirical and theoretical literature review	➢ Study on UPI technology, architecture, and security systems. ➢ Examines the key features of UPI, including cost, ease of use, settlement time, and security. ➢ Discusses the modular API-based architecture of UPI.
2	Title: Unified Payment Interface (UPI) A Way Towards Cashless Economy Authors: RadhikaBasavarajKakade& Prof. Nupur A. Veshne Year:2017 Journal: International Research Journal of Engineering and Technology (IRJET), Vol. 4, Issue 11, 2017	➢ Study on the key features of UPI. ➢ The study focuses on the role of UPI in promoting digital payments and a cashless economy. ➢ The study highlights smartphones as the main medium for UPI-based payments.

UNDER PEER REVIEW IN IJAR

	Methodology: Survey Study	
3	Title: UPI Based Mobile Banking Applications – Security Analysis and Enhancements Authors: K. Krithiga Lakshmi, Himanshu Gupta andJayanthiRanjan Year: 2019 Publication: 2019 Amity International Conference on Artificial Intelligence (AICAI) Methodology: Study and analysis of the security of UPI based mobile banking applications.	➢ The study examines the presence of known and unknown security risks in UPI-based mobile banking applications. ➢ It analyzes the architecture, transactions, and main features of these applications. ➢ It discusses authentication and authorization to make UPI applications more secure. ➢ The main focus is on technical security, whereas the focus on user behavior is limited.
4	Title: Security Issues of Unified Payment Interface and Challenges: Case Study Authors: YashMadwanna, MayurKhadseandB. R. Chandavarkar Year: 2021 Publication: 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC), 2021 Methodology: In this study, the problems and challenges related to UPI security are examined through a case study.	➢ The study examines the problems and challenges related to UPI security. ➢ It discusses the system of two-factor authentication. ➢ The first authentication factor is the mobile phone, while the second factor is MPIN and/or biometric authentication. ➢ The study compares UPI and IMPS and also discusses UPI-related security issues.
5	Title: UPI Frauds: A Study on UPI Usage, Awareness and Impact in India	➢ The study examines the relationship between UPI usage

UNDER PEER REVIEW IN IJAR

	Authors: NibeditaMukhopadhyay&MahadebMukhopadhyay Year: 2024 Journal: International Journal of Research in Commerce and Management Studies (IJRCMS) Methodology: The study uses data collected from UPI users and secondary data from the RBI.	and UPI fraud. ➢ It studies UPI users' awareness of fraud. ➢ It focuses on security issues such as two-factor authentication, phishing, and unauthorized access. ➢ It also studies users who were victims of fraud and those who successfully avoided fraud.
6	Title:Tackling Digital Payment Frauds: A Study of Consumer Preparedness in India Authors:AmeyaLonkar, SonaliDharmadhikari, NehaDharurkar, KanchanPatil& Ravi Ashok Phadke Year: 2024 Journals: Journal of financial crime Methodology: Data were collected from 372 consumers through a structured questionnaire, the study review literature on digital payment fraud and analyzed the collected data statistically.	➢ The study focuses on consumer preparedness towards digital payment fraud. ➢ Consumer preparedness was assessed on the basis of awareness, protection, and responsiveness. ➢ The study found a low level of awareness, moderate level of protection, and a high level of responsiveness. ➢ Overall, consumer preparedness was found to be moderate.
7	Title:Role of UPI Application Usage and Mitigation of Payment Transaction Frauds: An Empirical Study Authors: B. Franklin Edburg, K. Umadevi, M. Vidya& P. M. Ramesh Kumar Year:2024 Publication:MDIM Journal of Management	➢ The study examines the relationship between UPI application usage and payment transaction fraud. ➢ It examines users' perceptions regarding safety, security, and

UNDER PEER REVIEW IN IJAR

	Review and Practice Methodology:-In this empirical study, primary data were collected from UPI payment-app users through a structured questionnaire. The study analyzed perceived safety, security, risk, and fraud-prevention behavior using descriptive statistics	fraud risk. ➢ The study focuses on reducing UPI fraud and promoting fraud-prevention behavior. ➢ It also focuses on users' behavior and fraud mitigation, providing empirical evidence on UPI fraud prevention and user behavior.

2.1RESEARCH GAP

Existing studies have examined UPI technology and security, UPI fraud and awareness, consumer preparedness fraud prevention behavior. However, comparatively less attention has been given to examining UPI fraud by integrating public awareness, preventive measures, consumer protection, and legal aspects. Therefore, the present study attempts to examine these aspects together based on empirical data from UPI users.

2.2 RESEARCH OBJECTIVES

1. To study the level of awareness of UPI frauds among UPI users in India.
2. To examine the preventive measures followed by UPI users to avoid UPI frauds.
3. To examine the consumer protection and grievance redressalmechanisms available to consumers in cases of UPI fraud.
4. To study the existing legal and regulatory framework related to UPI frauds.
5. To analyze the key findings related to awareness, preventive measures, and consumer protection based on the empirical responses of UPI users.

2.3RESEARCH QUESTIONS

1. How much awareness do UPI users have regarding various types of financial fraud and safe payment method?

UNDER PEER REVIEW IN IJAR

2. What security measures and safe payment practices do UPI users adopt to protect themselves from financial fraud?
3. What legal and regulatory mechanisms exist for consumer protection and redressal in cases of UPI fraud, and what role do they play?

3.LEGAL AND REGULATORY FRAMEWORK

3.1 Regulatory framework of UPI:- In India, (UPI) Unified Payments Interface is a real time digital payment system that was developed and launched by the National Payments Corporation of India (NPCI). Through UPI, users can instantly transfer electronic funds between their bank accounts. The Reserve Bank of India (RBI) is primarily responsible for the regulation and supervision of payment systems in India, while NPCI provides the necessary procedures and guidelines framework for UPI operations, standards, and participating members. Thus, the regulatory framework of UPI is based on the combination of the regulatory oversight of the RBI and the operational framework of NPCI.

3.2 Customerprotection against Unauthorized transactions:- The RBI has prepared a customer protection framework to limit customers' liability in cases of unauthorized electronic banking transactions. According to this framework, if an unauthorized transaction involves the bank's negligence, deficiency, or fraud, the customer's liability is applicable under the prescribed circumstances. Similarly, if the transaction occurs due to a third-party breach and the customer informs the bank within the prescribed time, the customer may be entitled to zero or limited liability. The RBI has also emphasized that customers should report such transactions to the bank as soon as possible after becoming aware of them, as a delay in reporting may affect the customer's liability and loss recovery.

3.3 Relevant legal provision for UPI fraud:- The provisions of the Information Technology Act, 2000 and the BharatiyaNyayaSanhita, 2023 (BNS) strictly apply in cases related to UPI fraud. Section 66C of the IT Act is related to the fraudulent or dishonest use of another person's electronic signature, password, or unique identification feature, whereas Section 66D is related to cheating by personation through a computer resource or communication device. In addition, Section 318 of the BNS is related to cheating, which includes dishonestly or fraudulently inducing a person to deliver property or to do or omit to do any act.

UNDER PEER REVIEW IN IJAR

3.4 Complaint/Grievance redressal mechanism:- In case of UPI fraud, customers should immediately report the fraud to their bank or the relevant UPI service provider. If the complaint is not appropriately resolved, the customer can complain under the RBI Integrated Ombudsman Scheme, subject to the prescribed conditions. This system provides customers with an additional grievance redressal mechanism for complaints related to banking and digital payment services.

3.5 The '1930'helpline and cybercrime reporting:- Whenever UPI or other online financial fraud occurs, the victim can immediately report it to the National Cyber Crime Helpline 1930 and can also register an online complaint through the National Cyber Crime Reporting Portal. This mechanism is designed for the immediate reporting of financial fraud and for preventing fraudulently transferred funds from being transferred further. Therefore, early reporting after fraud is an important part of consumer protection.

3.6 Existing framework and practicalgap:-In India, legal, regulatory, and grievance redressal mechanisms are available to deal with UPI fraud. However, the effectiveness of these mechanisms does not depend only on the availability of laws and regulations. Public awareness, safe payment practices, timely reporting, and proper grievance handling also play an important role in protection from financial fraud. Therefore, along with legal protection, the study of users' awareness and preventive practices is also necessary to reduce UPI fraud.

4. RESEARCH METHODOLOGY

4.1 Research design and approach:-This study is based on an empirical research approach, in which users' awareness, consumer protection and preventive practices in relation to UPI financial fraud were studied. Primary data were collected from 100 respondents through a structured questionnaire using Google Forms. In addition, secondary data were used on the basis of existing literature, legal provisions and regulatory documents. Thus, both primary and secondary data were included in the study.

4.2 Data collection:-In this study, primary data were collected through a structured questionnaire. The questionnaire was prepared to understand UPI users' awareness of different types of fraud, knowledge of safe payment practices, reporting after fraud, bank cooperation, and their experiences and perceptions related to consumer protection. The

UNDER PEER REVIEW IN IJAR

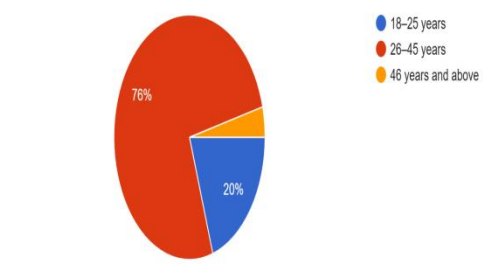
questionnaire was sent to respondents online, and a total of 100 responses were received. These responses were used for data analysis.

4.3 Respondent and sample:-The study included respondents who use UPI. Respondents were selected by making the questionnaire available online so that responses could be obtained from different UPI users. A total of 100 respondents participated in the study. Personal identity information was not collected from the respondents, and the responses received were used only for research purposes.

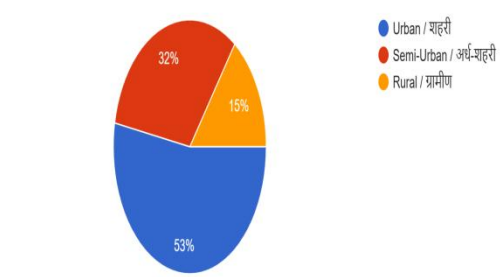
4.4 Data analysis: -The collected questionnaire responses were analyzed using descriptive statistical methods. The responses were systematically presented on the basis of frequency and percentage. The data were presented through tables and charts so that the responses related to respondents'UPI awareness, fraud-related experiences, safe payment practices and consumer protection could be clearly understood.

4.5 Sampling technique:-The respondents were selected through an online questionnaire. The questionnaire was made available online to UPI users, and responses were collected from them.

5. DATA INTERPRETATION

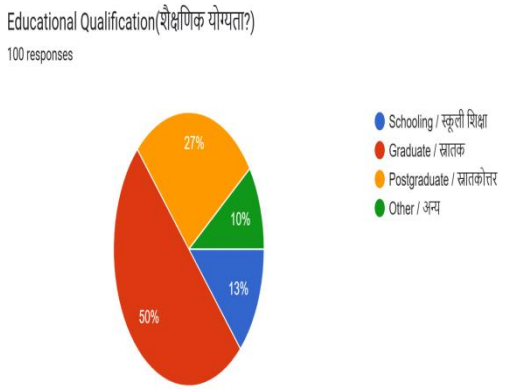
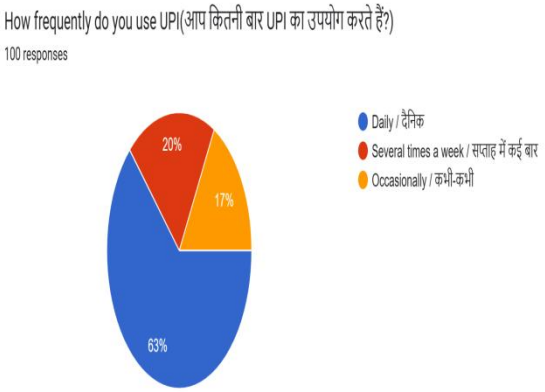
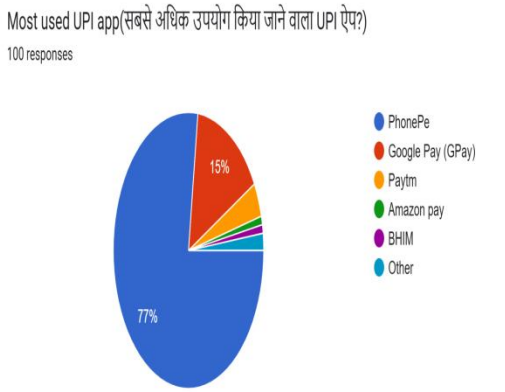
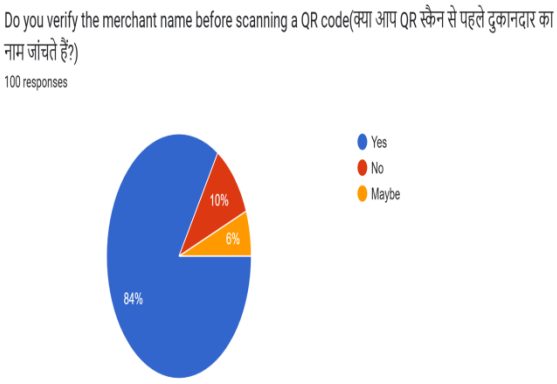


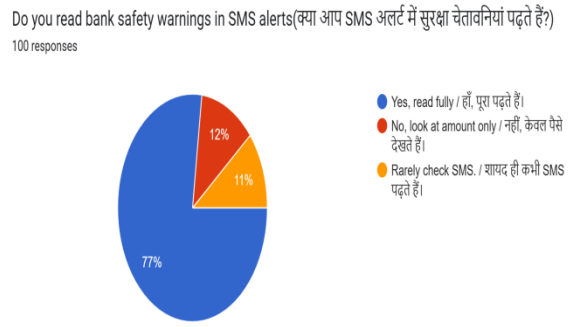
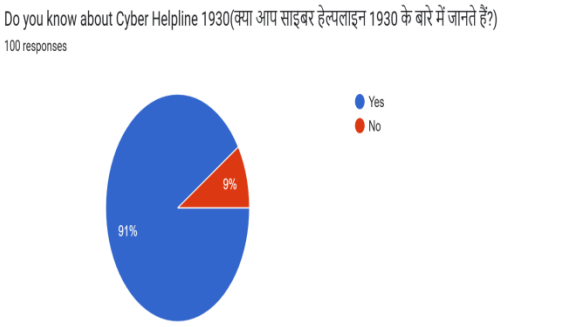
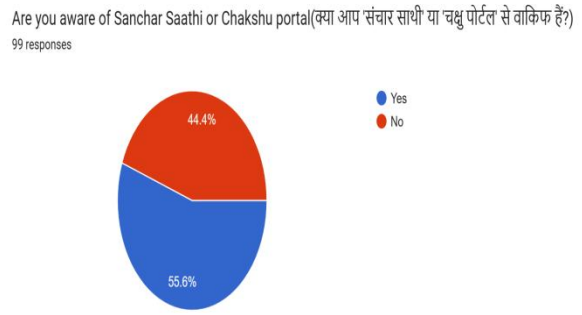
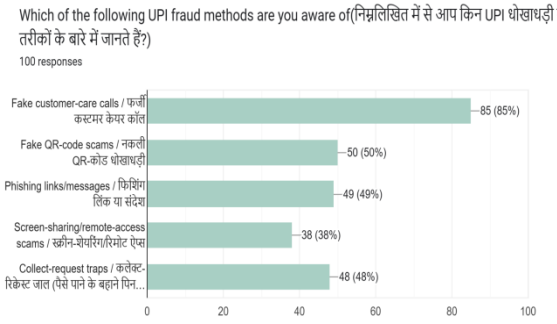
The largest proportion of respondents in the survey 76% belong to the working age group of 26–45 years, 20% who are young adults aged 18–25, while only 4% are aged 46 or older. This clearly indicates that UPI is primarily used by working professionals who engage in daily financial transactions.



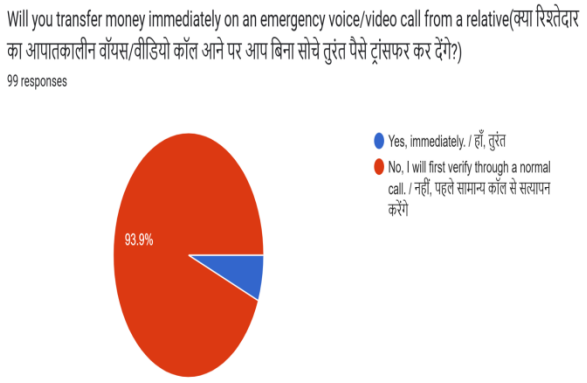
According to the area of residence data, 53% of respondents are residents of urban areas, while 32% are from semi-urban backgrounds, and the remaining 15% are from rural areas. This clearly indicates that the main consumer base for digital payments is still concentrated in urban and semi-urban

UNDER PEER REVIEW IN IJAR

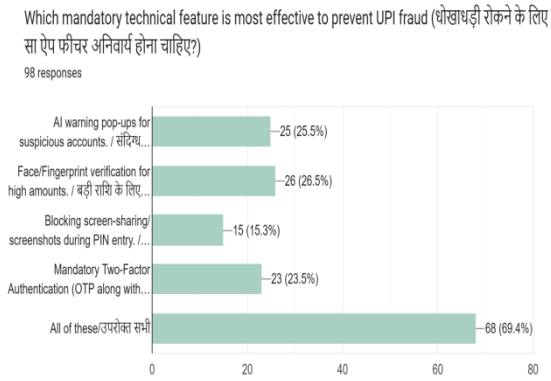
	areas.
 The largest group of respondents were graduate 50%, postgraduate 27%, schooling 13% and others 10%. Overall, this indicates that 77% of respondents were highly educated, whichstrengthens the understandability and reliability of the data and responses.	 63% of respondents use UPI daily, 20% use several times a week, while 17% use it occasionally. This indicates that payments are fully integrated into the daily financial transaction of most respondents.
 PhonePe 77% is the most popular app, 15% followed by Google Pay(GPay), while Paytm, Amazon pay, BHIM, and other collectively	 A majority 84% of respondents check the merchant name before making a payment, while 10% do not and 6% check some times.

account for the remaining share. This reflects PhonePe overwhelming dominance in the market.	This shows that most users have a basis security awareness of QR code payments.
 77% of respondents fully read security warnings provided in bank SMS, 12% only check the transaction amount and 11% rarely check SMS. This reflects the cautious and vigilant attitude of most users.	 91% of respondents are aware of the cyber helpline number 1930, while 9% are unaware. This indicates a fairly high level of public awareness of government cyber security initiatives.
 55.6% of people are aware of this specific government portals, while 44.4% are unaware. This suggests that more awareness campaigns are needed for these specific portals than for cyber helplines.	 Respondents are most aware of fraudulent customer care calls 85%, followed by fake QR codes 50%, phishing links 49%, screen-sharing apps 38%, and collect-request traps 48%. This indicates that people are more vigilant about call-based fraud, while awareness of technology fraud is relatively low.

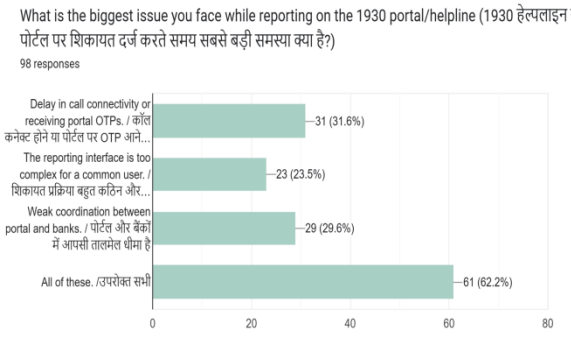
UNDER PEER REVIEW



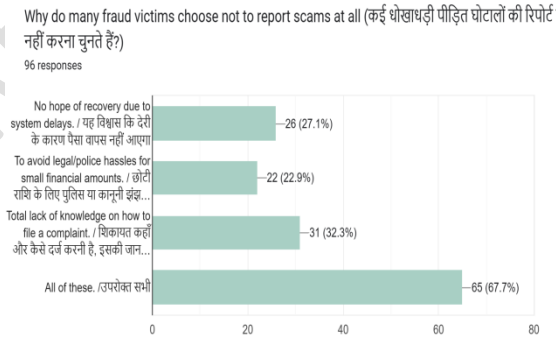
93.9% of respondents verify with a regular call before sending money to an emergency call, while 6.1% make the transfer immediately. This reflects consumer heightened vigilance against social engineering scams.



A majority 69.4% of respondents want all security features mandatory. These includes biometrics 26.5%, AI alerts 25.5%, two-factor authentication 23.5%, and screen sharing blocks 15.3%. This reflects the demand for stronger technical security.



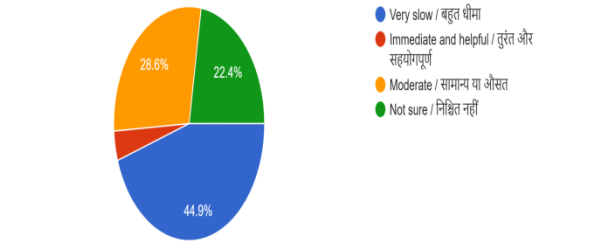
62.2% of respondents believe that delay in call connection aur receiving OTPs 31.6%, slow co-ordinationwith banks 29.6%, and complex procedures 23.5% are all major challenges. This reflects operational inefficiencies and underscores the urgent need for improvement in the helpline portal.



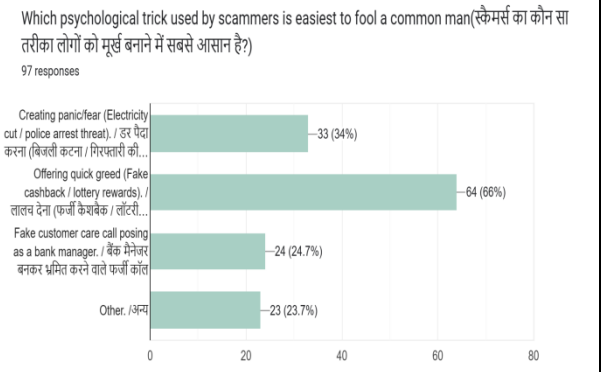
67.7% of victims cited procedural delays, police-legal hassles, and lack of information as the main reason for not reporting. This is driven by systemic delays 27.1% and legal or police hassles for small financial amounts 22.9%. On an individual level, a total lack of knowledge on how to file a complaint a emerged as the most critical personal barrier accounting for 32.3% of responses.

UNDER REVIEW IN IS

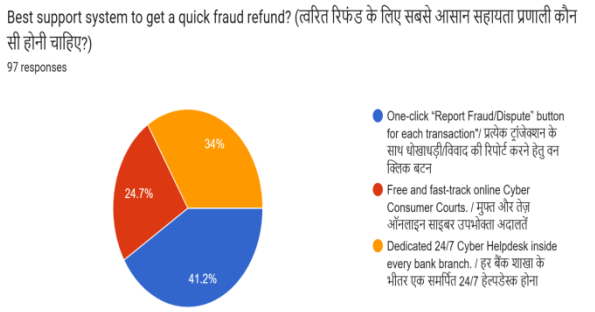
173



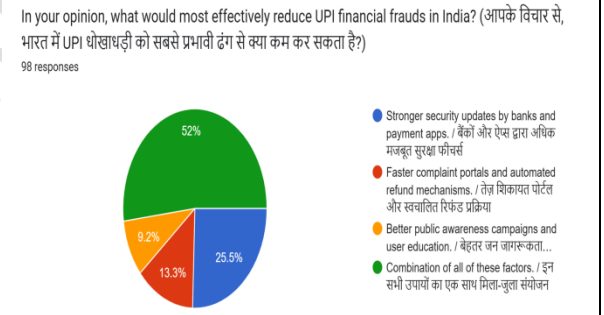
44.9% of respondents consider bank support to be very slow, 28.6% average ,22.4% uncertain and 4.1% consider it to be prompt and helpful. This calls for improvements in bank response mechanisms.



The most common tactics used by scammers to lure people are "lottery offers or cashback offers" 66%. These are followed by "threats of police or power outages" 34%, "other methods"24.7%, and "calling impersonating a bank manager" 23.7%. Evidently,fraudsters use greed and fear the most.



To get a quick refund, the highest number of people 41.2%, want a 'one-click fraud report button' with every transaction. This is followed by a '24/7 cyber helpdesk' 34% in every bank branch and a free and fast 'online cyber consumer court' 24.7%. Simply put, the public wants an easy button to lodge a complaint immediately.



52% of respondents believe that implementing all measures (strong security, fast refunds, and awareness) together is the most effective way to prevent UPI fraud in India. This is followed by 'strong security in bank apps' 25.5%, 'fast complaints and automatic refunds' 13.3%, and 'enhanced awareness campaigns' 9.2%.

UNDER PEER REVIEW IN IJ

6. FINDINGS

1. Basic merchant verification:-As per the survey, 84% of UPI users check the name of the merchant/shopkeeper before scanning the QR code, which indicates that the level of basic vigilance in daily transactions is quite good.

2. 1930 helpline awareness vs "Sanchar Sathi" awareness:- 91% of users are aware of national cyber helpline 1930. However, 44.4% of users are still completely unaware of the government's "Sanchar Sathi" and "Chakshu Portal" indicating that widespread publicity of dedicated complaint portals is still lacking.

3. Inefficient bank cooperation:- 44.9% of victims found the banks response and cooperation to be very slow. In contrast only 4.1% of users considered it to be prompt and helpful highlighting an urgent need for the improvements in bank response mechanisms.

4.Technical and administrative bottlenecks of the 1930 portal:-62.2% people faced problems like delay in call/OTP, complicated process and poor coordination with banks while registering a complaint on 1930 helpline. The biggest problem is delay in receiving call and OTP, which alone bothers 31.6% people.

5.Under-reporting traps:- 67.7% of respondents, do not report fraud because they have "no hope" of getting their money back due to systemic delays, and they want to avoid police/legal hassles for small amounts.

6. Psychological exploitation:-Scammers use tactics that easily fool 66% of people with the lure of a "fake cashback/lottery" and 34% with the fear of "power outage or police arrest".

7. Demand for instant dispute mechanism:-41.2% of users demanded a one-click "Report Fraud/Dispute" button in every UPI application to expedite the refund process, while 34% wanted a dedicated 24/7 cyber helpdesk within every bank branch.

8. The need for a holistic solution paradigm:-52% of respondents believe that legislation or awareness alone will not suffice, a combination of robust app security, a fast complaint portal and public awareness is essential to effectively prevent UPI fraud in India.

UNDER PEER REVIEW IN IJAR

7. SUGGESTION

1.Victim-centric refund mechanism:- The legal system should prioritize providing quick compensation and refunds to fraud victims, rather than limiting itself to punishing criminals.

2.In-App 'One-Click Dispute' button:- NPCI should mandate a "Report & Freeze Fraud" button with every transaction in all UPI apps, allowing victims to freeze funds during the golden hour.

3.Automated fund freezing upon call registration:-API-based automation should be implemented between the 1930 cyber helpline and bank servers, ensuring that fraudulent funds are automatically frozen upon a complaint being filed.

4.Tiered security:- For transactions involving higher amounts, stringent security measures, such as mandatory biometric or secondary OTP verification, should be implemented.

5.Mandatory cyber security briefing at the time of account opening:- It should be made mandatory to provide customers with a brief overview of cyber security and a one-page security card when opening a new bank account or setting up UPI.

6.Strict bank timelines (Mandatory Bank SLA):- RBI should set a strict timeline of 24-48 hours for banks to process fraud complaints in the first instance.

7. Simple and regional complaint channels:-The interface of the 1930 portal and online complaint system should be simplified and available in regional languages so that even rural and less educated people can easily file a report.

8.24/7 cyber assistance kiosks:- 24/7 Cyber Assistance Kiosks can be set up outside bank branches where victims of UPI fraud can immediately lodge a complaint and, where possible, a fund-hold/freeze request can be sent to the concerned bank immediately.

9.In-app warnings on suspicious accounts (AI Fraud Alerts):-UPI apps should use Artificial Intelligence (AI) to show a clear red warning pop-up before sending money to suspicious or first-time transaction accounts.

UNDER PEER REVIEW IN IJAR

8.CONCLUSION

This study presents a comprehensive analysis of the problem of UPI financial fraud in India, in the context of user awareness, preventive behavior, consumer protection, and the existing legal framework. The primary objective of this research was to understand the key security and consumer protection challenges faced by users amid the growing use of digital payments, and the difficulties they face in accessing prompt assistance in the event of fraud. Survey data revealed that 91% of users are aware of the national cyber helpline 1930, while 44.4% are unaware of channels like Sanchar Saathi and Chakshu. Additionally, 44.9% of respondents found bank response times to be too slow, while the complaint filing process also faced challenges such as complexity, delays, and lack of coordination between various institutions. These findings indicate that action against perpetrators alone is not enough; providing timely assistance and effective grievance redressal to victims is also essential.

In conclusion, the Information Technology Act, 2000, the BharatiyaNyayaSanhita, 2023 and RBI guidelines provide an important legal and regulatory framework, but further improvements are needed at the practical level to effectively address UPI fraud. Measures such as easy fraud reporting/dispute feature in UPI apps, additional security based on transaction amount, better coordination between banks and related institutions and cyber security awareness at the time of account opening can be useful. Punitive action alone is not enough to secure India's digital payment ecosystem; rather, a three-pronged integration of Prevention, Protection and Prompt Victim-Centric Redressal can prove to be the most effective solution to this problem.

9. REFERENCE

1. Reserve Bank of India, *Annual Report 2024–25*, ch. IV, para. IV.1 (2025).
2. National Payments Corporation of India, "UPI: Unified Payments Interface," available at: npci.org.in (last visited on Sept. 19, 2026).
3. National Payments Corporation of India, "Unified Payments Interface (UPI) Product Statistics," available at: npci.org.in (last visited on Sept. 19, 2026).
4. National Payments Corporation of India, "Fraud Awareness," available at: npci.org.in (last visited on Sept. 19, 2026).
5. Mukhopadhyay, Nibedita and MahadebMukhopadhyay, "UPI Frauds: A Study on UPI Usage, Awareness and Impact in India," 6 *International Journal of Research in Commerce and Management Studies* 179–197 (2024), available at: doi.org (last visited on Oct. 11, 2026).

UNDER PEER REVIEW IN IJAR

6. Reserve Bank of India, *Reserve Bank–Integrated Ombudsman Scheme, 2021* (2021).
7. *The Information Technology Act, 2000 (Act 21 of 2000)*, available at: indiacode.nic.in (last visited on Sept. 19, 2026).
8. Gochhwal, Rahul, "Unified Payment Interface—An Advancement in Payment Systems," 7 *American Journal of Industrial and Business Management* 1174–1191 (2017), available at: doi.org (last visited on Oct. 11, 2026).
9. Kakade, RadhikaBasavaraj and Nupur A. Veshne, "Unified Payment Interface (UPI) – A Way Towards Cashless Economy," 4 *International Research Journal of Engineering and Technology* 762–766 (2017), available at: irjet.net (last visited on Oct. 11, 2026).
10. Lakshmi, K. Krithiga, Himanshu Gupta and JayanthiRanjan, "UPI Based Mobile Banking Applications – Security Analysis and Enhancements," *Proceedings of the 2019 Amity International Conference on Artificial Intelligence (AICAI)* 903–908 (2019), available at: doi.org (last visited on Oct. 11, 2026).
11. Madwanna, Yash, MayurKhadse and B. R. Chandavarkar, "Security Issues of Unified Payments Interface and Challenges: Case Study," *Proceedings of the 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC)* 1–6 (2021), available at: doi.org (last visited on Oct. 11, 2026).
12. Lonkar, Ameya, S. Dharmadhikari, *et al.*, "Tackling Digital Payment Frauds: A Study of Consumer Preparedness in India," 32 *Journal of Financial Crime* 257–270 (2024), available at: doi.org (last visited on Oct. 11, 2026).
13. Edburg, B. Franklin, K. Umadevi, *et al.*, "Role of UPI Application Usage and Mitigation of Payment Transaction Frauds: An Empirical Study," 2 *MDIM Journal of Management Review and Practice* 7–22 (2024), available at: doi.org (last visited on Oct. 11, 2026).
14. National Payments Corporation of India, *Unified Payments Interface (UPI) Product Booklet* (NPCI, Mumbai, 2023).
15. Reserve Bank of India, "Frequently Asked Questions: Payment and Settlement Systems Act, 2007," available at: https://rbi.org.in (last visited on Oct. 11, 2026).
16. Reserve Bank of India, "Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions," Circular No. RBI/2017-18/15, DBR.No.Leg.BC.78/09.07.005/2017-18 (RBI, Mumbai, July 6, 2017).
17. *The Information Technology Act, 2000 (Act 21 of 2000)*, ss. 66C–66D.
18. *The BharatiyaNyayaSanhita, 2023 (Act 45 of 2023)*, s. 318.
19 Ministry of Home Affairs, Government of India, "National Cyber Crime Reporting Portal / Citizen Financial Cyber Fraud Reporting and Management System," available at: https://cybercrime.gov.in (last visited on Oct. 11, 2026).

UNDER PEER REVIEW IN IJAR