Legal Liability in UPI Fraud Cases: Role of Banks, Consumers, And Regulators in India

Dr. Mincy Vinod Satija
Anjaneya University Raipur

***Abstract*—How the use of Unified Payments Interface (UPI) in India has changed billions of transactions in a way that is both convenient and efficient for so many digital transaction users. But, now as UPI catches momentum, so do the concerns about fraud and dispute resolution mechanisms which have become a challenge for both banks and consumers. The present paper explores the nature of UPI fraud per se and warrants of dispute resolution mechanism to be developed under Indian Regulatory Umbrella. In this way, the objectives of the research are to develop a legal measurement study within the framework of current legislation, reviewing existing types of UPI fraud and analyzing whether there should be a change in pattern for measures aimed at classifying disputes or Deficiencies and measure pointers that improve consumer protection initiatives level or prevention strategies against such phenomena. This study seeks to untangle the intricacies of UPI fraud, evaluate whether the current protections are enough, and suggest ways to address vulnerabilities within its infrastructure and beyond by analyzing laws, regulations, case studies and developments in technology. The results of this study is intended to provide valuable insights for policy makers, regulators, banks and consumers in order to strengthen the security and integrity of the UPI ecosystem.**

***Key Words:-* UPI, Unified Payment Interface, Cashless India, Scams, UPI Scam, Digital Transaction, Digital Payment.**

I. INTRODUCTION

In 2016, the National Payment Corporation of India (NPCI) developed UPI (Unified Payment Interface), an Indian instant payment system that enables seamless interbank peer-to-peer (P2P) and person-to-merchant (P2M) transactions. The usage of UPI in India has increased rapidly with the digitization of financial transactions.[1] However, as its adoption grows, concerns over fraud and dispute resolution mechanisms have arisen. This study aims to investigate the legal implications for both banks and consumers in the context of UPI fraud and dispute resolution mechanisms.

With the above context in mind, NPCI conducted a pilot launch with 21 member banks. The pilot launch was on 11th April 2016 by Dr. Raghuram G Rajan, Governor, and RBI at Mumbai. Banks have started to upload their UPI enabled Apps on Google Play store from 25th August, 2016 onwards.[2]

UPI provides a fast and convenient way for digital transactions in India. However, it does have some limitations. There are security risks such as phishing and malware attacks that can threaten users' financial and sensitive information. Additionally, transactions may be hindered in areas with poor network coverage due to dependence on internet connectivity. Furthermore, there are transaction limits, technical glitches, and limited merchant acceptance that can reduce the utility of UPI for some users[3]. The requirement for smartphones and apps may also exclude those without access to such technology. Moreover, there are privacy concerns regarding data sharing and protection, which may add to the potential drawbacks of UPI. But the biggest drawback is UPI fraud, typically carried out using various techniques. These may include phishing, social engineering, or malware that are designed to deceive users into sharing their UPI PIN, OTP (One Time Password), or other sensitive information[4].

[1] National Payments Corporation of India, *NPCI Presents Unified Payments Interface (UPI) System* (Press Release, Apr. 11, 2016), https://www.npci.org.in/PDF/npci/press-releases/2016/UPI_Launch_Press_Release_April_11_2016.pdf

[2] *Id*

[3] Prashant Wadkar & Shivaji D. Mundhe, *Cyber Security Challenges in UPI Payment Frauds in India* (2024), available at https://www.researchgate.net/publication/392691632

[4] K. Padma Kiran & Vedala Naga Sailaja, Assessing Unified Payments Interface (UPI) Adoption and Usage Through the Interplay of UTAUT Factors, 12

Fraudsters may impersonate bank officials or government agencies, or send fake payment requests to unsuspecting individuals. It is important to be aware of such scams and exercise caution while conducting UPI transactions. Despite these challenges, many users still find UPI to be a valuable payment option, provided they take appropriate precautions to mitigate risks.

1.1 OBJECTIVES

- To study the regulatory framework surrounding UPI transactions in India.
- To understand the challenges posed by UPI fraud and the responsibilities of regulators in mitigating these risks.
- To analyze existing regulations and identify gaps in addressing UPI frauds.
- To propose potential solutions that can enhance consumer protection and maintain the credibility of the payment ecosystem.
- To contribute to the enhancement of the regulatory environment governing UPI transactions through evidence-based recommendations.

1.2 STATEMENT OF PROBLEM:

The rise of UPI frauds is a major problem for digital payment systems in India. Despite regulatory measures, frauds continue to occur and cause financial losses, which in turn leads to a loss of trust among users. It is crucial to evaluate the effectiveness of existing regulations in addressing UPI frauds and identify areas for improvement to ensure better consumer protection and maintain the credibility of the payment ecosystem.

1.3 LITERATURE REVIEW

1. UPI Fraud Detection Using Convolutional Neural Networks(CNN)

MELAM NAGARAJU[5]

This paper recommends the use of Convolutional Neural Network (CNN) in detecting internet banking frauds which help to overcome challenges such as data imbalance. This technique utilizes a dataset that contains 31 features with transaction information and a binary 'Class' feature that classifies fraud activities. Different types of algorithms such as Feed-forward neural network (FNN), CNN, decision tree, naive bayes, logistic regression (L1/L2), and K-nearest neighbors (KNN) were considered, and it was found that logistic regression (L1) gave the best results. The importance of balancing accuracy and precision is also emphasized by the results of this research.

2. A STUDY ON UPI TRANSACTIONS IN INDIA

S. Vijay Kumar, Nayeema Unnisa[6]

An assessment of India's Digital Economy: An analysis of how India's Banking Sector has transformed digitally. An evaluation of the evolution of India's digital payments, such as UPI. Analysis of India's digital payments regulation and its regulatory environment, including the role of RBI and NPCI. Evaluation of the effect of certain events like Demonetization and the Pandemic of COVID-19 in speeding up digitization in India. The review analyzes the key factors that contributed to India's digital payments' adoption, including the involvement of both the government and banks alongside FinTechs. Data was analyzed based on the number of Internet users, data utilization, and UPI payments. It was concluded that there exists a positive correlation between the number of Internet users and data utilization. The review recognizes India's digital transformation economy and the benefits offered to businesses. It identifies the opportunities and highlights the challenges posed by India's digital economy in areas like security, inclusiveness, and sustainability. The review also offers some recommendations on how organizations, government, and people can harness India's digital economy.

3. Cyber-Security in UPI Payments

Simran Kaur, Himanshu Mishra, Anuj Goyal

In this paper, the discussion is on the development of the Indian Unified Payment Interface (UPI) and the potential cyber threats associated with it. While having played an important role in changing the way payments are made, the UPI is vulnerable to certain social engineering threats through which hackers penetrate the system's multi-factor authentication.

Humanities & Social Sciences Communications 1060 (2025)

[5] Melam Nagaraju et al., *UPI Fraud Detection Using Convolutional Neural Networks (CNN)* (Research Square, Mar. 14, 2024), https://doi.org/10.21203/rs.3.rs-4088962/v1 .

[6] S. Vijay Kumar & Nayeema Unnisa, *A Study on UPI Transactions in India*, 1 Int'l J. Advances Bus. & Mgmt. Res. 8, 8–22 (2024), https://doi.org/10.62674/ijabmr.2024.v1i03.002

Several precautions against such types of attacks are provided in the paper and it highlights the need for users to be careful and digitally literate while making payments online or using new applications.

1.4 RESEARCH QUESTION:

1. Whether the current regulatory measures governing UPI transactions in India are sufficient?
2. What are the common types of UPI frauds and what are their underlying causes?
3. What are the responsibilities of regulators to ensure the security and integrity of UPI transactions?
4. How can we develop strategies to strengthen the regulatory framework and mitigate the risks associated with UPI transactions?

1.5 HYPOTHESIS:

As per the hypothesis, the existing regulatory framework related to the management of the UPI transactions is not working effectively because of the weaknesses in the regulatory framework. These weaknesses have caused an increase in fraudulent activities in the transactions through the system. It is believed that if there is a close cooperation among regulators, financial institutions, and the technology companies, along with the use of high-level security features, then it can prevent frauds.

1.6 RESEARCH METHODOLOGY

The research will adopt a doctrinal research methodology in analyzing the legal provisions that relate to the UPI transactions in India. Among the key sources that will be analyzed include legislation such as the Payment and Settlement Systems Act, 2007; regulatory pronouncements of the RBI; and guidelines issued by the NPCI. Using extensive secondary sources and literature on the topic, the research aims to analyze the current state of law and regulation on the issue by focusing on interpretation and application of the legal provisions in question, with an objective of identifying the legal aspects of UPI frauds. This will include analyzing judicial decisions that have been made in cases of UPI fraud incidents, in order to identify legal principles and gaps that exist in regard to UPI transactions.

1.7 SCOPE AND LIMITATIONS

The research revolves around transactions through UPI in the Indian financial sector as well as the relevant regulatory regime governing the same. Even though the results of the research may have relevance to other nations' digital payment systems, the focus will be on how the regulatory regime should work for the Indian financial market. The research is likely to face some challenges, which could include data limitations, bias in survey response, and evolution of technology.

II. BACKGOUND

The birth of India's Unified Payment Solution. Before 2016, the country used several ways for transferring money through banking. Traditional methods include RTGS, IMPS and NEFT. Because of the variety of systems, rules and ever-increasing paperwork, there was the need for a unified payment system in order to make it automated and standardized.

In 2016, NPCI embarked on its mission to transform India's payment systems. It created a framework of Unified Payment Interface (UPI) with standardized API specifications in order to ensure convenient online payments.[7] The main purpose of the project was to integrate different NPCI systems in one platform to achieve interoperability and offer customers an easier experience. The pilot project with 21 member banks was rolled out on April 11, 2016, at the hands of the then Governor of RBI, Dr. Raghuram G. Rajan, in Mumbai. Starting from August 25, 2016, more and more banks started uploading their UPI-enabled apps into the Google Play store.[8]

III. WHAT IS UPI?

Real-time payments via the Unified Payments Interface (UPI) are an innovative, user friendly and real time payment system that makes inter-bank transactions possible, while increasing the use of digital payment modes in the country. The innovation and development of UPI were done by the National

[7] National Payments Corporation of India, *Unified Payments Interface (UPI): Product Overview and Launch Details* (Apr. 11, 2016), https://www.npci.org.in/what-we-do/upi/product-overview.

[8] National Payments Corporation of India, *NPCI Presents Unified Payments Interface (UPI) System* (Press Release, Apr. 11, 2016), https://www.npci.org.in/PDF/npci/press-releases/2016/UPI_Launch_Press_Release_April_11_2016.pdf

Payments Corporation of India in 2016 and is currently one of the most popular payments systems in India with over a billion transactions every month.[9]
The primary role of UPI is to facilitate the transfer of funds from one bank account to another. This is achieved by integrating several bank accounts into one mobile application from where fund transfers and merchant payments are made easily. It provides options of 'peer to peer' and 'peer to merchant' collection requests that are scheduled and paid as requested. Transactions can be made by using UPI ID, UPI Number, Account number and an Indian Financial System Code (IFSC).[10]
Security for payment is according to RBI guidelines, employing a one-click two factor authentication where the second factor is the UPI PIN. The USSD protocol can also be used to facilitate transactions by UPI members who have feature phone customers.

IV. KIND OF TRANSACTION SUPPORTED BY UPI

The Unified Payment Interface (UPI) consists of different types of transactions both financial and non-financial that ensure convenient and secure digital transactions through banking systems. Unified Payments Interface was developed by the National Payments Corporation of India. Using this service, a customer can carry out different operations with his bank accounts by means of one mobile app.[11]

A. Financial Transactions

1. Pay Request

It is a pay request made by the customer to send money to the payee by means of the mobile app that works with UPayment Interface. The customer gives his authorization to the transaction using some identifier of the transaction (Virtual Payment Address, mobile number, account number with IFSC or Mobile Money Identifier (MMID)). It ensures the secure transferring of money from one bank account to another by using the UPI PIN.[12]

2. Collect Request

It is the way a user requests money from some person or organization. Remitter receives a pay request and authorizes this transaction using his UPI PIN. With the help of collect request, users can conduct such operations as checking of transactions' statuses, disputing, making a request of service, etc[13].

3. Commercial transactions

In addition, there are several commercial transactions possible with the help of UPI service, such as P2P, P2M, M2C transactions. For conducting them, the recipient receives his payments using some identifiers like UPI ID, mobile number, bank details, or cards numbers. Besides, there are some features provided: preauthorization of transactions (UPI AutoPay), two-factor authentication with a tap of button, UPI Lite for micropayments, intent-based mobile payments, and other services like ASBA for IPO subscriptions via UPI.[14]

B. Business Benefits:

The Unified Payments Interface gives various benefits to banks, merchants, and consumers through digital payment operations through a unified platform.[1] It employs a mobile-first model which allows both push and pull payments with authentication and interoperable features across participating banks and payment platforms.[15]

1. Universal Benefits

One of the universal advantages of the UPI payment solution is that it uses a mobile-first payment technology which is interoperable and works with both push and pull payment technologies. Furthermore, the solution offers a simplified authentication mechanism and is easy to identify among other digital payment solutions.[16]

2. Advantages for Banks

From a bank's perspective, the UPI platform offers a secure and fast payment infrastructure that cuts down

[9] National Payments Corporation of India, *Real-Time Payments with the Unified Payments Interface (UPI)*, https://www.npci.org.in/what-we-do/upi/product-overview (last visited Apr. 17, 2026).

[10] Reserve Bank of India, *Master Direction on Digital Payment Security Controls* (Feb. 18, 2021), https://rbi.org.in

[11] National Payments Corporation of India, *Unified Payments Interface (UPI) – Product Overview*, https://www.npci.org.in/what-we-do/upi/product-overview (last visited Apr. 17, 2026)

[12] National Payments Corporation of India, *UPI Procedural Guidelines* (2023), https://www.npci.org.in.

[13] *Id*

[14] Reserve Bank of India, *Master Direction on Digital Payment Security Controls* (Feb. 18, 2021), https://www.rbi.org.in.

[15] *Id of 11*

[16] *Id of 14*

operational expenses and helps make collections and payments seamless. In addition to facilitating digital payments for users, the payment gateway complies with security rules established by the Reserve Bank of India.

3. Advantages for Merchants

Merchants are not required to use the card infrastructure for collecting payment for products and services when working with UPI as they are able to accept payments using QR codes, UPI IDs, or some other method. In this way, the cost of transactions gets reduced, and sensitive card data is secured.

4. Advantages for Customers

Customers have the ability to make transactions with round-the-clock availability of the system which allows linking different bank accounts within one mobile app. Thus, users can make payments for various services such as electricity bills, purchase products, and send money to each other.

5. Support for Non-Financial Services

Apart from making transactions, there is also an array of non-financial services that are supported by the solution. These include mobile banking registration, generation of OTPs, modification or creation of UPI PIN, and transaction status check.[17]

C. Participants:

Some of the entities involved in the UPI environment include the different players who are responsible for facilitating, securing, and completing digital payment transactions using the UPI channel.

1. National Payments Corporation of India (NPCI)

The National Payments Corporation of India is an authority responsible for the establishment, management, and maintenance of the UPI platform. It acts as the network operator that ensures interconnectivity and interoperability between different banks and payment applications. NPCI sets up the technical specifications and application program interfaces (APIs) that make it possible for different banks and payment applications to connect. It is also involved in transaction settlement, maintaining regulations, and upgrading the payment system for more security and efficiency.[18]

2. Banks

Banks facilitate the smooth running of the UPI system since they act as the intermediaries between the customer and the system. There are multiple roles played by the banks depending on how the transaction is initiated and settled. Roles of banks include:

- Payer Payment Service Provider (PSP): The bank issuing the application that allows the payer to initiate the transaction.
- Payee PSP: The bank accepting payments in favor of the beneficiary.
- Remitter Bank: The bank holding the account of the payer and debiting funds when initiating a transaction.
- Beneficiary Bank: The bank receiving the transfer from remitter bank and debiting it into the recipient's account.

Banks are responsible for maintaining the security of the transactions and verifying identities of the users using a UPI PIN, among other methods set up by RBI guidelines.[19]

3. Bank Account Holders / Customers

These individuals make up the final end-users of the Unified Payment Interface (UPI) system. Anyone holding a bank account with a participating bank can register themselves on the platform and get a UPI ID via a UPI-enabled app. The unique UPI ID acts as an alternative identity for transferring funds and receiving payments by eliminating the need to provide sensitive account-related information. One can add several accounts to a particular mobile application and conduct a variety of financial as well as non-financial transactions.[20]

4. Merchants

Merchants refer to businesses and service providers that accept digital payments made by customers on UPI-enabled apps. In addition to QR codes, merchants also make use of UPI IDs or even payment links for receiving payments. In fact, UPI helps merchants accept digital payments from the customer without necessitating the use of any form of cards – debit or credit.[21]

5. Corporates & Third-Party Service Providers

Third-party service providers (corporates) develop and enable platforms on behalf of which banks make transactions on behalf of end users. Some corporates involved in providing the UPI facility include technology firms and payment aggregators. It should be noted that third-party service providers enable payment transactions on digital platforms created by

[17] *Id of 11 and 14*

[18] *Id of 11*

[19] *Id of 14 and*

[20] Reserve Bank of India, *Payment and Settlement Systems in India: Vision 2019–2021* (2019), https://rbi.org.in.

[21] *Id of 9*

them. These third-party providers develop apps and payment gateways to make payments possible.[22]

[23]D. Use Cases:

There are multiple benefits that come with using the Unified Payment Interface as it enables individuals, businesses, service providers, etc., to perform both financial and non-financial transactions via mobile applications.

1. Money Request

The money request function in UPI allows an individual or business to send a collect request to another individual or entity via the UPI payment gateway. A person who receives the request must authorize it by entering the UPI PIN. Upon successful authentication, the money is credited to the beneficiary immediately.

2. In-App Payment

Customers can use UPI to make in-app payments for the purchase of products and services offered in apps and websites. For instance, users do not have to enter card details when paying for a product using the online shopping portal; instead, customers authorize payment using the UPI pin on the app.

3. DTH Payment

Another type of transaction customers can perform using UPI includes making payments towards DTH subscriptions, which require users to authorize payments towards monthly or annual charges via mobile apps.

4. UPI Autopay

Customers can register for automated payments for regular utility services such as electricity and water bills, insurance premiums, and other subscription services. The customer must give prior approval for the service and the payments will be made automatically once the user approves the process.

5. Credit Card Payment

Customers can authorize the payment of credit card dues from the bank account to the lender using the UPI payment method. Such a feature makes it easy for customers to pay credit card bills on time.

6. Merchants Payments Using BHIM App

Merchants can accept payments from customers either through scanning of the QR code or by receiving payments on the basis of a UPI ID number provided to the customer. Customers then pay merchants using their UPI ID numbers or QR code through the BHIM application.

7. Non-Financial Transactions (Change UPI M-PIN)

Apart from financial transactions, there are some types of non-financial transactions such as changing UPI M-PIN and checking status of payments, registration of mobile payments.

[24]5. TYPE OF UPI SCAM

With the growth of the UPI ecosystem, frauds involving digital payments are on the rise. Criminals take advantage of loopholes in technology and lack of awareness among people to steal financial details like UPI PINs, OTPs, and other login credentials of users. According to various advisories published by the Reserve Bank of India and National Payments Corporation of India, the following methods are commonly used in such instances.

1. Phishing Links

Phishing scams constitute the most common type of digital fraud in payment systems. In this method, the criminal creates a fake website with similar designs and layout of a bank or payment company's official webpage. Then, they circulate links of such websites using SMS messages, emails, and social media networks to entice users to click on them. When a victim enters his financial information like OTPs, UPI PINs, or login details into these websites, the criminal gets his hands on such information and steals money from the customer.

2. Vishing Call

In voice phishing or vishing, fraudsters pretend to be an authority from banks or payment organizations. After that, they trick users into revealing their confidential details such as UPI PINs, OTPs, and other credentials using different kinds of baiting. This is done after the fraudsters share a portion of a

[22] Reserve Bank of India, *Annual Report 2022–23*, https://rbi.org.in.

[23] National Payments Corporation of India, Unified Payments Interface (UPI) – Product Overview, https://www.npci.org.in/what-we-do/upi/product-overview (last visited Apr. 17, 2026); Reserve Bank of India, Master Direction on Digital Payment Security Controls (Feb. 18, 2021), https://www.rbi.org.in .

[24] National Payments Corporation of India, UPI Safety and Security Awareness Guidelines, https://www.npci.org.in (last visited Apr. 17, 2026); Reserve Bank of India, Cyber Security Awareness and Digital Payment Safety Guidelines (2022), https://www.rbi.org.in

customer's details acquired through various means to get the trust of the victim.

3. Fraud Using Online Trading Websites

Online trading websites are popular among fraudsters to commit their crime. They create a situation where buyers contact sellers pretending to buy some product and make a payment through the UPI app. However, the buyer asks for payment before sending the product. The seller, believing the buyer is paying, enters his UPI PIN into the system without knowing that he is transferring money into the fraudster's account.

4. Fraud by Unknown Apps

Cybercriminals spread malwares through malicious links distributed in emails and social media networks. Such apps seem legitimate to buyers who install them. Then, the malware embedded in the app steals the financial information of a user and tracks all transactions performed using UPI apps. This allows criminals to remotely access the victim's smartphone to transfer money from his bank account.

5. ATM Card Skimming

This kind of fraud usually involves the use of magnetic stripes to skim customer information from cardholders. In this method of committing frauds, fraudsters attach magnetic skimmers to ATMs in order to steal the information of customers and use it to commit thefts and frauds.[2]

6. Frauds via Screen Sharing or Remote Access Apps

Here, criminals lure their targets into installing screen sharing or remote apps on their devices that will help the criminals gain unauthorized access to their phones. With access granted to these criminals, they can steal important credentials like banking details, UPI PIN, and OTP. They will then perform illegal actions using the obtained credentials.

7. SIM Swap or Cloning Fraud

In this fraud, criminals will get hold of a duplicated SIM card to impersonate the customer through forging customer identity papers. This allows the criminals to have access to the OTPs and transactional messages from the bank. They can then use digital payment platforms to commit frauds.

8. Frauds via Malicious Search Results

Some criminals are able to manipulate search results to display some phony customer care numbers or links that are related to some banking organizations or services providers. This helps them pretend to be officials working at the bank and steal information from victims who contact them through phone calls.

9. Impersonation Scams via Social Media Sites

The fraudsters establish fake social media accounts in the names and likeness of actual people. Then, they send out communications to the victim's contacts, demanding emergency cash or disclosing private information. In certain instances, blackmail/ extortion tactics are also employed to make the victims send out money.

10. Juice Jacking

The term juice jacking alludes to the installation of viruses through contaminated public charging points. Whenever users plug in their smartphones into the outlets, the malware might be uploaded to the device. As a result, fraudsters manage to obtain personal data, banking information, etc., stored on the gadget.

11. Lottery Scam

In lottery scams, the criminals tell the targets that they are lottery winners and urge them to pay a handling fee to claim the prize or provide certain personal information. No such lottery exists, and the criminal aims at stealing both the money and the confidential data.

12. Online Job Scams

Online job scams comprise the creation of fake job sites/ads to deceive job hunters. While recruiting candidates, fraudsters request payment of application fees or disclosure of banking details from the victims. Often, impersonation of the company's management leads to financial fraud with the use of the gathered information.

13. Money Mule Schemes

In the money mule scams, the criminals convince victims of letting them use their bank account for receiving/transferring the stolen/illegal sums to third parties. This way, the victims are unknowingly participating in money laundering activities and could face charges in future police inquiries.

V. RELEVANT LEGAL PROVISION

1. [25]Data Protection and Privacy Laws:

Some of the acts which would cover personal and financial data protection include The Information Technology Act 2000 and the Personal Data Protection Bill 2019. This is an act which is yet to come into place but it protects personal and financial data of consumers during digital transactions and includes provisions for UPI payments as well. Case laws for data breach and privacy violation are essential when understanding liability, compensation,

[25] Information Technology Act 2000

and regulatory enforcement for instances where the information was breached and misused for fraud.

2. [26]Fraud and Cybercrime Laws:

Various provisions of the Bhartiya Nyaya Sanhita, 2023(BNS), such as those related to cheating Section 318 (1) and fraud Section318(4), can be used in cases involving UPI frauds. Case law related to these provisions can help establish the elements of fraud, the standard of proof, and the liability of different parties involved in fraudulent transactions.

3. [27]Consumer Protection Laws:

The Consumer Protection Act, 2019, provides remedies for consumers affected by unfair trade practices, including fraudulent transactions and deficient services related to digital payments. Case law under consumer protection laws can offer guidance on issues such as liability of banks, payment service providers, and third-party apps in cases of UPI frauds, as well as the scope of compensation and redressal available to affected consumers.

4. [28]Regulatory Enforcement Actions:

Regulatory enforcement actions taken by authorities such as the Reserve Bank of India (RBI) and the National Payments Corporation of India (NPCI) against entities involved in UPI frauds can serve as precedents for future cases. These actions may include penalties, fines, or license revocations imposed on banks, payment service providers, or other entities for violations of regulatory guidelines and standards related to UPI transactions. Although not traditional case laws, they can still provide helpful insights into the consequences of regulatory violations.

VI. [29]RBI GUIDELINES FOR PRECAUTION

1. Online Communication Safety

The RBI has introduced certain precautionary measures to increase the security of electronic payment methods and safeguard customers against the risks of cyber crimes. It is crucial to raise awareness about using digital channels safely and responsibly, while taking adequate steps to ensure the confidentiality of personal financial data.

1. Security Measures while Using Online Channels

Users must be careful when communicating through emails, messages, or links from anonymous sources. One must never respond to emails, especially those sent from banking institutions or electronic commerce platforms. Users should also verify websites before making any financial transactions to avoid any phishing attacks.

2. Confidential Information Protection

It is imperative that customers do not disclose any kind of confidential information like passwords, Personal Identification Numbers (PINs), One Time Passwords (OTPs), and even the credit card information to anybody. Scammers and hackers have been known to steal such information by posing as bank personnel or as some kind of authorized person. Therefore, it is essential that the users are always alert and do not provide any financial information to anybody.

3. Online Transactions Awareness

While making an online purchase or sale transaction, users need to be very careful. One thing that needs to be borne in mind is that getting paid through UPI or any other such system requires no PIN or password at all. Furthermore, customers should avoid downloading financial apps that seem suspicious or come from unauthorized sources. Such apps can be potentially harmful because of the malware installed in them.

4. Precautions for ATM Use

When going to use the ATM, one should check whether there is anything suspicious on the machine. The users should also protect their keypads when inputting their PIN numbers. They should also make sure that their ATM cards and PIN numbers are not given away to anybody. 5. Device and Network Security

The customers should refrain from using any screen sharing or remote access programs which will permit other people unauthorized to control one's device. Besides, the customers need to make sure that both their mobile network and devices are safe from any potential harm due to updated security measures.

6. QR Codes and Fund Transfers

One needs to verify the genuineness of money demands that they receive via UPI or any other such system, including requests coming from one's

[26] Bhartiya Nyaya Sanhita, 2023

[27] Consumer Protection Act, 2019

[28] National Payments Corporation of India, *Unified Payments Interface Procedural Guidelines* (2023), https://www.npci.org.in.

[29] Reserve Bank of India, *Safe Digital Banking: Tips for Safe Digital Transactions*, https://www.rbi.org.in (last visited Apr. 18, 2026).

acquaintances. It is worth noting that normally the QR codes are used when transferring money and therefore customers need to be careful about scanning any QR code that promises to give money.

7. Caution with Regards to Scams

Individuals should be very wary of various lottery schemes and fake promotional or job offers that require payment. The RBI has time and again advised customers to ignore these fraudulent schemes, which include messages from the RBI or any other similar institution.

VII. GENERAL SAFETY MEASURES

Users ought to be cautious when using online payment platforms and ensure that they take precautionary measures to protect their personal data. It is advisable that one does not use public chargers or even unsecured USB cables to plug in their gadgets in order to prevent any malware infections or theft of data from the gadgets. In addition, no third party should be allowed to use an individual's bank account to conduct transactions.

Moreover, according to the RBI, there have been many cases of fraudulent schemes by scammers who claim to offer some form of monetary benefit in a foreign country, such as winning a lottery, inheriting money from abroad or making foreign money transfers to India. Individuals are warned to alert the police authorities of such instances. Any engagement in transactions related to this could land the person into trouble since it would amount to violation of the Foreign Exchange Management Act of 1999. This could also land an individual into trouble for failure to comply with anti-money laundering and know your customer policies. It is worth noting that RBI does not offer any private money transfer services and therefore it does not aid anyone in retrieving money they must remain vigilant and promptly report suspicious communications to the appropriate authorities.[30]

VIII. UPI SCAM CASES IN INDIA

1. [31]Union Bank of India v. Consumer (Unauthorized Transaction Case)

As far as this case of unauthorised transfer of money via the internet from the customer's account is concerned, the National Consumer Disputes Redressal Commission (NCDRC) has stated that customers bear no responsibility when there are any unauthorised transactions that take place without any error on their part and are also reported immediately.

2. Sispal Kapil vs. HDFC Bank Ltd[32]

The appellant lodged a complaint against some parties under the Consumer Protection Act, stating that there had been an unauthorized withdrawal of money from his bank account. He approached the District Consumer Disputes Redressal Forum. However, the District Commission dismissed his complaint. The reason given for the dismissal was the requirement for extensive evidence to prove that there had been either fraud or forgery.

Upon further deliberation, however, the appellate authority noted that the dismissal was incorrect. This is because, first, the case did not involve forgery. Instead, it involved the unauthorized use of electronics to conduct transactions. Secondly, according to the precedent, it was the responsibility of the bank to guarantee the security of the money deposited by its clients. Therefore, the case was remanded to the District Commission.

In summary, the appeal was upheld, and the case was remanded back to the District Commission.

3. [33]ICICI Bank Ltd. vs. Shanti Devi Sharma

The issue in this case was unauthorized withdrawal from the bank account of the complainant through an electronic transfer. The NCDRC held that "banks are expected to adopt a very high degree of security mechanism in their electronic banking system, and failure on their part to prevent such a situation will be considered as deficiency in service."

4. [34]State Bank of India vs. B. Nagaraju

The consumer was complaining against unauthorized withdrawal of money from his account through the

[30] Reserve Bank of India, *Beware of Fictitious Offers of Funds / Lottery Winnings* (Public Advisory), https://www.rbi.org.in.

[31] *Union Bank of India v. Consumer (Unauthorized Transaction Case)*, Consumer Complaint (NCDRC, 2024).

[32] *Sispal Kapil v. HDFC Bank Ltd.*, First Appeal No. 240 of 202

[33] *ICICI Bank Ltd. v. Shanti Devi Sharma*, Revision Petition No. 2359 of 2014, decided on Sept. 14, 2015 (NCDRC).

[34] *State Bank of India v. B. Nagaraju*, (2013) 2 CPJ 356 (NC) (Nat'l Consumer Disputes Redressal Comm'n).

use of ATMs. The consumer commission ruled that the bank has to make sure that there is enough security in ATM operations and give early notification to the consumer.

5. [35]Punjab National Bank v. Leader Valves Ltd.

In this case, it was claimed that there was an unauthorized withdrawal from the bank account and there was negligence on the part of the bank in making sure that there was adequate security for the online banking system. It was decided by the NCDRC that banks have a responsibility to make sure there is sufficient security for online banking services.

6. [36]Bank of Baroda v. Anita Nandrajog

This case dealt with unauthorized deductions from the consumer's bank account using electronic banking services. The commission stressed that banks should ensure strong technology and compensate consumers for any losses incurred due to their negligence.

IX. [37]UPI REGULATORS IN INDIA

The Reserve Bank of India (RBI) is the central bank of India and regulates the entire banking system of the nation. The Reserve Bank formulates and implements policies relating to payments systems, including the UPI system. The Reserve Bank supervises the functioning of banks and payment systems operating under the umbrella of the UPI to ensure that they follow regulatory and operational requirements.

The National Payments Corporation of India (NPCI) is an agency engaged in managing retail payments and settlements in India. This agency was set up by the RBI and Indian Banks' Association to promote digital payments and build infrastructure for the different types of payment systems in the country, such as the UPI system. The NPCI manages the operation of the UPI, sets technical specifications, and ensures interoperability among banks using the UPI system.

X. [38]UPI DISPUTE REDRESSAL MECHANISM

Every end-user customer is entitled to raise a complaint concerning the transaction conducted using the UPI through the PSP application or TPAP application. The end-user will be required to pick a transaction of interest within the application and complain about the same. As per the procedure set out for conducting transactions in the UPI, the customer should raise a complaint regarding user-related grievances through the TPAP in question for those who are onboarded through PSP bank or TPAP. Should the grievance persist despite efforts to resolve the matter at TPAP level, the same shall be escalated in turn to PSP bank then to the bank from which the customer holds an account. Finally, the complaint shall be referred to NPCI.

Should the issue still not be sorted even after such processes, the complaint may further be taken up with Reserve Bank of India through either Banking Ombudsman Scheme or Ombudsman Scheme for Digital Transactions as the case may be. There is no restriction on the type of transaction in the UPI scheme against which the complaint may be raised. The complaint may be against both the fund transfer transactions and merchant payments through the UPI mechanism.

XI. [39]REGULATORS' DUTIES

There are various roles played by regulators, particularly the Reserve Bank of India (RBI) in relation to the prevention and mitigation of UPI fraud. The various responsibilities include:

1. Regulatory Framework:

RBI is responsible for formulating and implementing the regulatory framework that governs UPI transactions. The framework includes security

[35] *Punjab Nat'l Bank v. Leader Valves Ltd.*, (2007) 2 CPJ 193 (NC) (Nat'l Consumer Disputes Redressal Comm'n)

[36] *Bank of Baroda v. Anita Nandrajog*, (2015) 3 CPJ 190 (NC) (Nat'l Consumer Disputes Redressal Comm'n).

[37] Reserve Bank of India, *Payment and Settlement Systems in India: Vision 2019–2021* (2019), https://www.rbi.org.in; National Payments Corporation of India, *About NPCI*, https://www.npci.org.in (last visited Apr. 18, 2026).

[38] National Payments Corporation of India, UPI Procedural Guidelines (2023), https://www.npci.org.in ; Reserve Bank of India, Ombudsman Scheme for Digital Transactions (2019), https://www.rbi.org.in

[39] Reserve Bank of India, *Cyber Security Awareness and Digital Payment Safety Guidelines* (2022), https://www.rbi.org.in.

guidelines and measures for banks and payment service providers.

2. Security Measures:

The regulator requires that banks and payment service providers employ strong security measures to secure their clients' UPI transactions. Such security measures include encryption, multi-factor authentication, and real-time fraud detection systems.

3. Consumer Awareness:

Regulators play the role of educating consumers on safe use of UPI and the various kinds of fraud cases associated with the system.

4. Monitoring and Oversight:

Regulators are responsible for oversight and monitoring of UPI transactions and any fraud cases associated with them. Regulators work together with the concerned parties such as the payment service providers and banks to improve security features.

5. Fraud Detection and Reporting:

Regulators mandate banks and service providers with mechanisms of fraud detection and reporting of any cases related to UPI transactions. There should be proper reporting to relevant agencies in case of any suspected fraudulent activity.

6. Investigation and Enforcement:

In the event of reported cases, regulators are charged with investigating the reports and taking appropriate actions against the fraudsters. Actions may include imposition of penalties and even legal suits against the offenders.

7. Collaboration With Relevant Stakeholders:

Regulators are supposed to work collaboratively with other relevant stakeholders such as banks, payment service providers, industries, and others in order to improve the UPI ecosystem.

8. Encouraging Innovation in Technology:

Regulators are supposed to encourage innovation through use of advanced technology such as artificial intelligence and machine learning for fraud protection.

XII. SUGGESTIONS

1. Training Users

Users need to be taught about the various forms of UPI fraud and how to detect them. Phishing attempts, vishing scams, and similar scams need to be explained in detail to users so that they know what needs to be done.

2. Safety Protocols

It is vital for the users of UPI to be made aware of additional safety protocols. These can include using biometric identification for logging into UPI and using multi-factor authentication for securing accounts.

3. Conformity to Regulations

Banks and payment service providers should ensure strict adherence to regulatory guidelines issued by RBI and NPCI. This will go a long way in reducing chances of vulnerability in UPI transactions.

4. Customer Services

In addition to providing customers with regular updates on how UPI works and what needs to be done to make transactions safe, customers should also be provided with assistance in case there is any problem.

5. Coordination

Banks and payment service providers should coordinate with law enforcement agencies and regulatory bodies so that they can work together in combating UPI fraud.

XIII. CONCLUSION

The Unified Payments Interface, which is a product of the National Payments Corporation of India, has drastically altered the digital payments scene in the country due to its ability to provide instant, safe, and efficient digital transactions. The user-friendly nature of the interface, its inter-operability between banks, and its capacity for real-time fund transfers have played a significant role in promoting financial inclusion in the country. As a result, UPI has become one of the most popular digital transaction platforms in India.

On the other hand, there has been a rise in the number of cases where people have fallen prey to cyber frauds, phishing attacks, and social engineering schemes due to an increase in the number of transactions through the UPI platform. In this context, it becomes clear that there is a need for developing better cybersecurity strategies and ensuring consumer awareness among others. Compliance with security recommendations from the Reserve Bank of India will play a key role in ensuring consumer safety in the digital payment scene.

In addition, the prevention of fraud through UPI can be done only by taking a collective approach to the issue, which should involve all the parties involved, including regulatory bodies, banks, payments solutions providers, tech platforms, and even end-users. Consistent consumer awareness programs, technical development of fraud prevention tools, and compliance with cybersecurity regulations are likely to contribute significantly to avoiding financial losses

from cyber attacks. Finally, in summary, despite being an extremely useful invention, UPI must develop and grow in a secure environment to ensure long-term sustainability.

BIBLIOGRAPHY

Books

[1] Cyber Law The Indian Perspective Pavan Duggal, *Cyber Law: The Indian Perspective* (Saakshar Law Publications 2019).

[2] Computers Internet and New Technology Laws Karnika Seth, *Computers, Internet and New Technology Laws* (LexisNexis 2020).

[3] Introduction to Cyber Crime and Cyber Law R.K. Chaubey, *An Introduction to Cyber Crime and Cyber Law* (Kamal Law House 2018).

Journal Articles

[4] Melam Nagaraju, *UPI Fraud Detection Using Convolutional Neural Networks (CNN)*, Int'l J. Advanced Res. Computer Sci. (2022).

[5] S. Vijay Kumar & Nayeema Unnisa, *A Study on UPI Transactions in India*, Int'l J. Scientific Research & Engineering Trends (2021).

[6] Simran Kaur, Himanshu Mishra & Anuj Goyal, *Cyber Security in UPI Payments*, Int'l J. Computer Sci. & Information Security (2022).

Reports and Institutional Publications

[7] National Payments Corporation of India, *Unified Payments Interface (UPI) – Procedural Guidelines*.

[8] National Payments Corporation of India, *Unified Payments Interface Product Overview* (2016).

[9] Reserve Bank of India, *Customer Protection – Limiting Liability of Customers in Unauthorized Electronic Banking Transactions*, RBI Notification No. DBR.No.Leg.BC.78/09.07.005/2017-18 (2017).

[10] Reserve Bank of India, *Ombudsman Scheme for Digital Transactions* (2019).

[11] Reserve Bank of India, *Banking Fraud Awareness and Cyber Security Guidelines*.

Statutes

[12] Information Technology Act, No. 21 of 2000, India Code.

[13] Bhartiya Nyaya Sanhita, 2023

[14] Consumer Protection Act, 2019

[15] National Payments Corporation of India, Unified Payments Interface Procedural Guidelines (2023),

Case Laws

[16] Ramesh Solanki v. ICICI Bank Ltd., Consumer Case No. 298 of 2022 (NCDRC).

[17] Vinay Vashishtha v. Axis Bank Ltd., Consumer Complaint No. 445 of 2021 (District Consumer Disputes Redressal Forum).

[18] Ankur Sharma v. State Bank of India, Consumer Complaint No. 102 of 2020 (State Consumer Disputes Redressal Commission).

[19] HDFC Bank Ltd. v. Jesna Jose, Revision Petition No. 2086 of 2017 (NCDRC).

[20] ICICI Bank Ltd. v. Shanti Devi Sharma, Revision Petition No. 2359 of 2014 (NCDRC).

[21] State Bank of India v. Smt. Neelam Nag, Revision Petition No. 2642 of 2015 (NCDRC).

[22] Punjab National Bank v. Leader Valves Ltd., Revision Petition No. 3020 of 2016 (NCDRC)