INDIAN JOURNAL OF LEGAL REVIEW [IJLR]

Volume 3 and Issue 1 of 2023

ISSN - 2583-2344 *(and)* ISBN - 978-81-961120-2-8

Published by

Institute of Legal Education

https://iledu.in

UPI PAYMENTS AND THEIR ATROCITIES

Author - Sinrella Mittal, Student at Bharati Vidyapeeth (Deemed to be University) New Law College, Pune.

BEST CITATION - Sinrella Mittal, UPI PAYMENTS AND THEIR ATROCITIES, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 3 (1) OF 2023, PG. 834-839, ISSN - 2583-2344.

ABSTRACT

The Barter system was a blotchy method of exchange of goods and services for consideration. Since ancient time money transfigured itself into many forms and today it had finally emerged in the form of currency. In the United Nations (UN) member states, UN General Assembly non-member observer states, partially recognized or unrecognized nations, and their dependent entities, 180 currencies are now accepted as legal money. Since independence, currency has made up at least two-thirds of the total amount of money in circulation. The amount of currency in circulation increased dramatically from Rs 1,230 crores in July 1951 to Rs 3,052 crores by the end of June 1967. Gold coins, bullion, foreign securities, and other precious metals made up 54% of the Issue Department's assets in July 1951, with Government of India rupee securities making up the remaining 42%. By June 1967, the former proportion had come down to less than 10 per cent, while the latter had risen to 88 per cent and the trend is incessant.[2441] The behaviour of people using currency in developing nations that are facing various socio-political and economic difficulties has been examined. While each of these nations faces unique difficulties, they all share a heavy reliance on cash and an extremely low adoption rate of other payment methods. India, where, 60% of individuals lack banking access, is a country with a cash-heavy economy that relies heavily on gold as a store of wealth. However, there is always a cost that the nations must bear for their strong reliance on finance.[2442] To cope up with such a calamitous problem, the domestic economy welcomed a revolutionizing step towards easing out the reckoning activities and was named as Unified Payments Interface. But along with easing the payment activities, it has somewhere made these activities prone to attack with a fear of losing out data and of course, financial delinquency.

Keywords: UPI transactions, OTP/ PIN, Digital Payments, Attack and Fraud.

I. INTRODUCTION

United Payments Interface (UPI) is an immediate real-time payment system that enables inter-bank transactions on a mobile. It was introduced on April 11th, 2016 with the goal of changing India into a "less-cash" society. The RBI is in charge of overseeing digital payments. National Payment Corporation of India (NPCI) created UPI, which is like an email ID that the bank uses for each person to send money via the Immediate Payments Service (IMPS), which is more rapid than NEFT and available all day. In other words, it is a form of payment, similar to cash, checks, debit cards, and mobile wallets. The UPI system is different and practical for users since it can communicate with different banks. Additionally, it supports "Peer-to-Peer(P2P)" or "Person-to-Merchant (P2M)" requests that may be planned and paid for based on need and convenience. Some Third-Party Apps that facilitate UPI payments include Google Pay, PhonePe, PayTM, and BHIM. In addition, WhatsApp Pay functions as a Third-Party App enabling user-to-user payments.[2443]

Utilization of mobile payment services for smartphone users, financial institutions, and

[2441] *Currency: Changes and Challenges*, RESERVE BANK OF INDIA (Jan 22, 2023, 07:04 PM), https://rbidocs.rbi.org.in/rdocs/content/PDFs/90042.pdf.

[2442] Bhaskar Chakravorti, *The Hidden Costs of cash*, HARVARD BUSINESS REVIEW (Jan 31, 2023, 12:23 PM), https://hbr.org/2014/06/the-hidden-costs-of-cash.

[2443] Harshita Chawla vs WhatsApp Inc. And Others, (2020) (Competition Commission of India).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR]

Volume 3 and Issue 1 of 2023

ISSN - 2583-2344 *(and)* ISBN - 978-81-961120-2-8

Published by

Institute of Legal Education

https://iledu.in

banks, has been signalled by the replication of smartphones, technological advancements, and efficient internet connections. Demonetization and the "Digital India" efforts have given the Indian banking industry more propulsion as they work hard to spread the use of digital payments. It is a wonderful and economical innovation that makes it possible for anyone to use digital payment services. It has been demonstrated that elements including usability, app layout, inclinations, feasibility, availability, services, and pricing play a significant role in determining whether a firm succeeds in the digital payment sector.

But just as the idiom goes, "Every coin has two sides," so too has this been true of every advancement made in the era of the internet. Bank frauds committed through social engineering have significantly increased as a result of the surge of UPI-based transactions. Because UPI is a very secure platform and secure transactions depend on smartphones and the internet, every user must be sufficiently tech-savvy to avoid being duped by scammers, fraudsters, and hackers into providing their financial information to enable UPI IDs or providing their UPI PIN to receive payments.[2444]

II. ATTACK PRONE UPI

The app-design of Unified Payments Interface possess certain loopholes which can make it prone to attacks, leakage of authentic data of the user, misuse of the data on part of the attacker and financial loss to the ultimate users. Various such attacks are as follows:

A. UNAPPROVED REGISTRATION USING THE USER'S MOBILE PHONE [2445]

This attack exposes confidential information, including the list of banks where a user has accounts as well as the account numbers. Given the victim's cell phone number, a remote attacker in this attack can set up a UPI account. He simply needs one thing for the attack to be successful: the victim's cell phone must have UPI app loaded.

B. UNAUTHORIZED BANK ACCOUNT TRANSACTIONS USING A USER'S MOBILE NUMBER AND A SHORTENED DEBIT CARD NUMBER [2445]

Both in-person and online debit card purchases in India require the customer to confirm the transaction by entering a personal identification number (PIN). In this attack, an attacker can make transactions on a user's bank account even if they have never used a UPI app for payments by knowing the user's cell phone number and the debit card information (the last six digits and expiration date, without the PIN), which is printed on the card.

C. TRANSACTIONS THAT ARE NOT PERMITTED AND USE STOLEN DEBIT CARDS [2445]

This attack demonstrates how an attacker can learn all the necessary components to perform unauthorised transactions on a user's bank account even if they initially have no knowledge of that user's authentication factors. Such a user would already have a passcode set up for BHIM[2446] login and a UPI PIN for transaction authorization. As a result, this can be used to transfer money out to arbitrary UPI-based accounts in India.

III. DIFFERENT WAYS OF FRAUDS USING UPI

A. OTP/PIN FRAUD (Case Study)

People unknowingly share their UPI OTP/PIN to fraudsters, scammers or even their relatives, friends, family members which later proves to be devastating for their bank balance. Upon these instances, they cannot even seek legal remedies as they consensually share this data and even banks can only help then up to a

[2444] Mitesh Thakker, *How can fraudsters trap you? Beware of Cybercrimes through UPI transactions*, TIMES OF INDIA (Feb 03, 2023, 08:50 PM), https://timesofindia.indiatimes.com/blogs/voices/how-can-fraudsters-trap-you-beware-of-cybercrimes-through-upi-transactions/.

[2445] Renuka Kumar; Sreesh Kishore; Hao Lu and Atul Prakash, University of Michigan, *Security Analysis of Unified Payments Interface and Payment Apps in India*, USENIX (Jan 29, 2023, 01:23 AM), https://www.usenix.org/system/files/sec20-kumar.pdf.

[2446] Represents all UPI transactions.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR]

Volume 3 and Issue 1 of 2023

ISSN - 2583-2344 *(and)* ISBN - 978-81-961120-2-8

Published by

Institute of Legal Education

https://iledu.in

certain extent. We can substantiate the statement by way of the case study explained below.

1. Tarabai v. Bajaj Alliance General Insurance [2447]

In this case, the complaint is the owner of the opposing party's current account which is a bank. The complainant received a message from his bank stating that Rs. 5,000 had been illegally debited from his account. However, the amount in question was not actually debited by the complainant, but rather by an unidentified hacker who pretended to be from Club Factory, an online retailer, and asked for the complainant's account information in order to refund the amount of returned goods that the complainant had sent to Club Factory. The complainant was very shocked when Rs. 5,000 was deducted from his account rather than refunded as the return amount. The complainant immediately informed the offending bank, i.e., the opposite party, about the illegal act and requested that it take appropriate action to secure the complainant's account.

In this regard, the opposite party blocked the complainant's ATM card and gave the complainant the assurance that his account was now completely secured and that nobody could deduct money from it. But again, the accounts of the complainant got debited for amounts of Rs. 19,999, Rs. 18,800, and Rs. 400. The complainant filed a FIR under Section 420 of the IPC after receiving an unsatisfactory response from the bank. It was stated that the bank is not liable because the complainant himself gave the fraudulent individual the UPI (Unified Payments Interface) Secret Code/OTP, which is only known to him. It was held by the court that; it is wrong and denied that an amount illegally debited from the complainant's account is a result of negligence on the part of the Bank. It is further wrong and denied that the Bank did not perform his duty as alleged. It is further wrong and denied that the concerned Bank is totally liable to pay the amount to the complainant. There is no deficiency of service on the part of the Bank but the complainant himself is responsible for alleged amount that has been debited by the unknown hacker to whom the complainant shared the UPI PIN, might be because of lack of knowledge of online payment or in rush of getting amount credited to his account as alleged by the complainant. The complainant has failed to prove any deficiency in service and unfair trade practice on the party of the opposite party.

Thus, due to his own mistake of not changing the UPI PIN and thoughtlessly sharing it with the fraudster, the complainant's sensitive information got exposed to UPI scam.

B. LOAN DECEPTIONS INCLUDING PRIVATE DATA ATTACKS, BLACKMAILING etc. (Case Study)

Due to trouble-free access to credit facilities, a lot of players have entered into the market to provide economical and instantly available loans which are just a click away and the person availing them do not even have to mortgage anything. This activity seems like an opportunity to the online financial fraudsters, who lure people into such hoax offers and people fall prey to them and end up compromising their personal and authentic data to the online poachers, who later blackmail and extort these people.

1. Sunil Kumar Chauhan v. State of UT [2448]

In this case, the complainant reported to the police that he had received an SMS on his telephone number with a URL link that requested the installation of the Hugo loan application. When he clicked the link, the application requested access to his phone's gallery and all of his contacts, and he granted it. On the Hugo loan app, he then verified his

[2447] Tarabai v. Bajaj Alliance General Insurance, Complaint case no. CC/48/2020, (District Consumer Disputes Redressal Commission).

[2448] Sunil Kumar Chauhan v. State of UT, (Punjab and Haryana High Court) (Jan 2023).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR]
Volume 3 and Issue 1 of 2023
ISSN - 2583-2344 *(and)* ISBN - 978-81-961120-2-8
Published by
Institute of Legal Education
https://iledu.in

eligibility for a loan and entered all of his information. According to the application, he qualified for a loan but didn't submit a loan application. Later, he began receiving threatening phone calls and texts from the numbers +37125218379, +6283146262636, and +919910429137, as well as naked photographs on WhatsApp. Additionally, he claimed that his family members had received the images, and they began demanding money through blackmail. He sent the blackmailer some money, after feeling intimidated, but the accused kept threatening him, posted the photographs on social media, and demanded more money. Six people from various locations in North India were detained during the course of the inquiry. During questioning, they admitted that some other people—their bosses—were the ones who used to transfer money through various UPIs into the victim's accounts as a loan amount before extorting money from them by hacking their data (Contacts, Gallery), taking the money via UPI, and transferring it to accounts that weren't in the victim's names. The arrestees told the police that the loan apps were being operated from China to India and the people involved delivers the payment after confirmation from both sides. The bank statements exhibited multiple transfer of the same amount from different bank accounts of different banks through various UPI transactions. When information about alleged fraudulent bank accounts and electronic devices is sent through the 14C (Integrated Cyber Crime Coordination Centre) portal run by the Ministry of Home Affairs, it was discovered that the aforementioned data had links to more than 1575 complainants and 89 FIRs of fraud across the nation.

Hence to substantiate, initially the black-mailers demand as paying capacity of the people. Mostly the people do not report under the fear of being exposed in front of their family members and relatives. Malefactors take advantage of big loop-holes in identification and procuring Aadhar Cards and Sim Cards and take active participation in the gang activities by alluring the people to download the app by sending on their mobile phone and subsequently enticing them to pay money.

C. SOCIAL ENGINEERING AND PHISHING ACTIVITIES

A highly widespread scam is Phishing in which scammers send SMS messages containing payment links. These phoney bank URLs will resemble the genuine URL. When you click it, your phone's UPI payment app will open, allowing you to select any app for an auto-debit. The funds will be promptly taken out of the UPI account after your approval. Additionally, a virus or malware will infiltrate the phone, allowing it to steal any saved financial information. Such SMS messages must be recognised by users, who should then ignore or delete them.[2444]

Financial fraud has increased significantly since 2018, according to research from Fidelity National Information Services, with victims across all age groups increasing to a share of 27%. Compared to other age groups, the 27 to 37 age group has been the most affected by financial fraud. Attacks using social engineering to obtain private data, including bank account numbers and one-time passcodes, are frequent. Indians have embraced digital transactions, but the fifth annual PACE research from FIS shows that despite the prevalence of social engineering and phishing emails, they have not yet mastered the do's and don'ts of giving personal information. In India, there is a striking association between the rapid uptake of mobile apps, the growth of digital payments, and the rate of financial fraud. 96 percent of Indian consumers who experienced financial fraud throughout the year switched to a mobile app, and the country's efforts to achieve financial integration have been greatly impacted by

INDIAN JOURNAL OF LEGAL REVIEW [IJLR]
Volume 3 and Issue 1 of 2023
ISSN - 2583-2344 *(and)* ISBN - 978-81-961120-2-8
Published by
Institute of Legal Education
https://iledu.in

the shift away from cash payments to digital payments.[2449]

D. REMOTE OBSERVATION

A privacy breach and data leak can occur when users download an untrusted software like Pegasus or a trojan that is covertly packaged with other apps from the app store. These third-party apps have the ability to access UPI app information and gather personal data from your phone, which might result in UPI fraud. Upon downloading, these malicious apps want a lot of access to the data. The user is in charge of double-checking each programme and the access they are granting after downloading.

E. FAKE CALLS

Customers are occasionally contacted by scammers posing as bank officials and asked for UPI PINs, OTPs, or the download of a third-party app for the purpose of verification. They can use this to access both their account information and personal data. Unless they come from reliable sources, the clients should reject such enquiries.[2444]
In order to verify your identity, the fraudsters will call you pretending to be bank employees and ask for your UPI pin or that you download a third-party app. They will say that this is required. If you do this, they will be able to access your data and account details.[2450]

IV. FASTag INIQUITIES

For Indian drivers, excessive traffic is a regular occurrence, thus having to wait in long lines at toll booths is always a hassle and a waste of time. The government has implemented FASTag, an RFID-powered tag, to address this issue and make using toll plazas less difficult. All you have to do is drive through the toll booth, attach the tag to your windscreen, and you're done! The tag will be recognized by the plaza's scanner, which will then automatically deduct the toll fee from your bank account. This is quite an easy way to pay hassle-free on toll gates. With that said, the system is relatively new and hence prone to some errors and setbacks.[2451] Various challenges faced by those use FASTag as a means of toll payment are as follows:

A. LOST, MISSING, OR RUINED TAGS

One of the challenges faced is that the card might be easily lost, destroyed, or stolen because it is attached to the windscreen of the vehicle. This is a typical issue that many FASTag users encounter. Make a formal complaint about the missing tag right away if this is the situation with your IndusInd Bank-issued tag. It's advisable to take this action right away because your lost or stolen tag can be used inappropriately. However, if your tag is broken in any way, please send it back to us, and we'll give you a new one.

B. DOUBLE-DEDUCTIONS

Another devastating challenge includes deduction of toll fee twice from your account. Mostly, this happens due to a technical glitch. Some banks provide customer care to apply for double-deduction reimbursement through their customer portal.

1. Honey Garg vs Dareri Jattan Toll Plaza (Case study)[2452]

The instant appeal has been filed by the appellant- complainant, against the order passed by District Consumer Disputes Redressal Forum, Patiala, whereby the complaint of the complainant was allowed and opposite party was directed to refund Rs.35/- and to pay

[2449] *Financial Cybercrime and Identity Theft in India are Increasing: FIS*, EXPRESS COMPUTER (Feb 01, 2023, 09:44 AM), https://www.expresscomputer.in/news/financial-cybercrime-and-identity-theft-in-india-are-increasing-fis/35099/.
[2450] *UPI Payment Fraud: Here are Safety Measures to Protect Your Money,* HDFC ERGO (Feb 02, 2023, 10:20 PM), https://www.hdfcergo.com/blogs/cyber-insurance/safety-measures-to-protect-your-money-from-upi-payment-fraud.
[2451] *FASTag-Related Challenges Faced by People in* India, INDUSIND BANK (Feb 03, 2023, 11:34 PM), https://www.indusind.com/iblogs/categories/trends/fastag-related-challenges-faced-by-people-in-india/.
[2452] Honey Garg vs Dareri Jattan Toll Plaza, (November 2020) (State Consumer Disputes Redressal Commission).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR]

Volume 3 and Issue 1 of 2023

ISSN - 2583-2344 *(and)* ISBN - 978-81-961120-2-8

Published by

Institute of Legal Education

https://iledu.in

another sum of Rs.2000/- as compensation inclusive of costs for causing harassment and mental agony inclusive of litigation expenses within the period of 45 days. The complainant had travelled from Mohali to Patiala via Banur by his car and crossed Dareri Jattan Toll Plaza. The operator of the Toll Plaza, Dareri Jatta charged Rs.35/- for single journey which was paid by the traveller by way of cash. It is averred that the complainant is holding Fastag card and received an email from Bank that Fastag account has been debited for Rs.35/-. He came to know that Rs.35/- has been deducted again though he had paid the same vide separate cash receipt. It is averred that he has been charged twice for crossing the Toll Plaza for the same single journey.

During the next visit, the employees of the Toll Plaza were asked to return the amount but they refused to return the same and simply denied the fact and to resolve his genuine request. The employees of Toll Plaza had spoken in a rude and unprofessional manner. Charging of the amount twice is unfair trade practice and deficiency in service on the part of opposite party. Hence, consumer complaint was filed with the prayer for claiming compensation and cost of Rs.50,000/- on the ground of deficiency in service and charging excessive amount, resultant mental agony and harassment.

The complainant has contended that lot of people have suffered similar problem due to the such act and also due to rude behaviour of the opposite party. The complainant has spent Rs.10,000/- on engaging a counsel and miscellaneous expenses of Rs.10,000/- before the District Commission for filing the consumer complaint and claimed Rs.30,000/- on account of mental agony but the District Commission has awarded only Rs.2,000/-. Unsatisfied with decision, the complainant appealed to the State Consumer Dispute Redressal Commission where the appeal was dismissed.

V. SUGGESTIONS AND CONCLUSION

1. UPI being an evolution in the Indian history, still need a lot of filtering and legal enforceability in a broader and more serious sense and specific legislations should be made for UPI transactions.

2. There are a lot of loopholes in the designing and functioning of UPI 1.0 and UPI 2.0 which should be tackled as well at a technical level in a momentous manner.

3. Education and Awareness about the usage of UPI and potential and probable attacks and threats to the data should be dispatched at a macro level to the end user.

4. Payment gateways should be more secure and fastened with 3-way Authentication.

5. There is a question as to whether the attacks discovered are due to limitations of Android's permission model or due to flaws in the UPI design and who should fix them. There are problems with both. It is noted that no bank-related credentials are required to get a user's bank account number, given the user's cell number. For example, the attacker uses the last six digits of a debit card number and expiry date, a weaker threshold than for online and in-store purchases using debit cards where the entire number and the PIN is typically required. Alternate workflows in the UPI protocol contribute significantly to enabling the attacks. It is leveraged upon Android's security limitations as well, just as any good attacker would be expected to.[2445]

6. Thus, this study is a deep and intense assessment and scrutinization of "UPI and its Atrocities". It inhibits various malpractices along with the real-life cases for the better understanding of the readers. It also includes suggestions from the researcher's point of view