The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2024

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

DATA PRIVACY CONCERNS OVER UPI

INTRODUCTION

Cash has been the primary source of payments for consumers in India. However, witnessing the recent trend, the nation has embraced digital payments with wide acceptance and some of the biggest players are increasingly in competition. In addition, the global impact of COVID-19 on e-commerce sector encouraged online payments and strengthened the need for policies regulating such digital payments. For purpose of this paper, the study is only limited to Unified Payments Interface (UPI) sector. UPI works on both Person-to-person (P2P) and person-to-merchant (P2M) model allowing bank transfers through mobile applications as per convenience with no bounds to effort of visiting banks or time of the day. As of now, the Indian industry for UPI payments has a handful of big names contending like Facebook owned WhatsApp, Walmart owned PhonePe, GooglePay, et cetera. As of recent reports, the UPI is about to enter the Europe through the MoU signed between NPCI International and Lyra Network, which in effect would allow seamless payments in France. For initial stages, UPI will only be working as P2M model to allow Indians to make payments to French merchants. The UPI system requires customers to link their bank accounts to the software applications, requires personal information like name, phone number and it also stores history of all transactions made through the UPI. Since, there is so much data being collected, controlled and processed by various organisations, there is bound to be risk of privacy. Indian legal system does not have codified data privacy law so far and this gives unfair advantage to data processors. However, the EU has global benchmark in data privacy law in form of General Data Protection Rules (GDPR) which are applicable at any organisation collecting and/or processing data of EU citizens. The study intends to highlight the data privacy concerns over UPI transactions by analysing the application of data protection and privacy laws on UPI digital payment providers in India and European Union.

RESEARCH METHODOLOGY

The researcher has done a doctrinal research and relied on secondary sources for understanding and analysing data privacy law in both European Union and India individually and to further study their application to UPI. No empirical research or survey has been conducted.

LITERATURE REVIEW

1. “Study on New Digital Payment Methods” , ECB

The study was commissioned by European Central Bank (ECB) and reported by Kantar public. It aimed at gaining thorough understanding of the current payment habits of citizens of euro area countries and specifically their attitudes towards digital payment methods. The concept of “digital euro” was introduced to respondents and their views were recorded on the same. The respondents were divided into different target groups as per their profession and access to manual banks and banking services.

2. “Evaluating Drivers of Fintech Adoption in the Netherlands” , Sage Publication

The main aim of the paper is to study and determine the factors influencing adoption and usage of mobile payments in Netherlands. The paper reflects on worldwide researches on mobile payments to explain the interlink of mobile payments and customer experience followed by exploring Dutch banking systems and finance industry. It also studies the impact of social distancing rules on increase in digital payments. The study is empirical and concludes that primary factors affecting adoption of mobile payments by Dutch consumers are safety and trust, ease of use and perceived usefulness.

3. “Legal Constants and the 'Constant' outside of the Law: Mobile Payments in Comparative Perspective under European Union Law” , Daniele D’Alvia

The article aims to determine whether mobile payments can be characterized by a legal constant, or common legal meaning. Generally, they are part of the Fintech phenomenon, and they are specifically regulated in Europe, inter alia, under the Payment System Directive and the Regulation on Multilateral Interchange Fees. Nonetheless, those secondary hard law acts do not include any compulsory legal definition for mobile payments, which remain undefined and conventionally identified as means of proximity or remote payments.

4. “Digital payments and European sovereignty” , SUERF

The author in his paper recognises the acceleration in digital payments which has been further charged by coronavirus and the role of international non-europeans players in the space like Apple Pay. The author calls for “a pan-European payment solution that is governed at the European level and needs to be useable at the physical point of sale as well as in e-commerce and between individuals”.

ANALYSIS

Evolution Of UPI

The Unified Payments Interface (UPI) has revolutionized digital payments in India, offering a convenient and secure way for users to transfer money. Dilip Asbe, MD and CEO of NPCI, proudly boasts that UPI has one of the fastest adoption rates in the history of payment systems.[1] The current statistics are equally mind-boggling. After its launch, UPI took over a year to surpass 10 million monthly transactions, and over three and a half years to cross the 1 billion transaction mark. Since then, UPI has grown ninefold, achieving this impressive growth in approximately the same amount of time.[2] Essentially, once UPI gained the trust of the Indian populace, it rapidly gained momentum and became a massive success. In April 2023 alone, UPI recorded 8.9 billion transactions worth INR 14 trillion[3]. Much of the success of UPI can be attributed to its core simplicity. All the users have to do is choose a platform, set up a virtual payment address for their bank account ('VPA', or as is commonly called UPI ID), and remember a transaction pin or what is called MPIN (mobile banking personal identification number). Moreover, if payer and the recipient are using the same third-party platform, things get even easier. Money can be transferred to their phone number without needing that virtual address. Furthermore, if users have multiple accounts at a bank, all of them can be connected to a single virtual ID, providing flexibility and convenience for managing transactions.[4] The transactions are all real-time and can be initiated and processed at any time, providing round-the-clock accessibility to users. Banks and fintech companies joined forces, launching a relentless wave of cutting-edge advancements that transformed the user experience landscape. It was an era of rapid-fire innovations, where each player vied to outdo the other in delivering unprecedented convenience and delight to the users. The UPI system was cleverly crafted to be all about mobiles, making the most of the smartphone revolution and the lightning-fast internet.

Why UPI is a success?

UPI was built with the fundamental principles of introducing ease, speed, and interoperability in payments.

[1] Three-four countries keen on UPI, says NPCI MD & CEO Dilip Asbe, The Business Standard (2023). https://www.business-standard.com/article/finance/three-four-countries-show-interest-in-adopting-upi-npci-s-dilip-asbe-123010901021_1.html .

[2] Explained: How India is outpacing the world in digital payments, Times of India (2021). https://timesofindia.indiatimes.com/business/india-business/explained-how-india-is-outpacing-the-world-in-digital-payments/articleshow/88580555.cms

[3] UPI transactions at record high in April, touch Rs 14.07 trn, The Business Standard (2023). https://www.business-standard.com/india-news/upi-transactions-at-record-high-in-april-touch-rs-14-07-trn-123050100490_1.html .

[4] Considerations and Lessons for the Development and Implementation of Fast Payment Systems, World Bank Report. https://fastpayments.worldbank.org/sites/default/files/2021-11/Fast%20Payment%20Flagship_Final_Nov%201.pdf .

1. **QR Code** - The quest for widespread adoption prompted the introduction of the QR Code, thus revolutionizing the payment landscape. With a mere scan of the QR code, customers could seamlessly complete transactions with merchants. Initially, QR code-based transactions on UPI relied on unique codes generated by individual payment service providers or UPI-enabled apps. Each provider had its own QR code format, necessitating users to scan the code using the corresponding app to initiate a payment. Subsequently, to enhance interoperability and convenience across UPI-enabled apps and payment service providers, a Universal QR Code was launched.[5] Today the merchant can be onboarded by any of the platforms that provide the QR code, but the payment can be initiated by the customer operating from any other platform. QR Codes became a game-changer for small businesses in today's digital economy, offering a cost-effective and user-friendly solution. Further, it found its moment in the spotlight when the demand for cashless payments surged during the peak of the Covid season.
2. **Cross-border Payments** - Expanding beyond borders, one of the initial endeavors of UPI was the introduction of Foreign Inward Remittance, enabling users to receive funds effortlessly and securely from overseas into their UPI-linked bank accounts.[6] In India, UPI stands tall as a leading real-time payment system, while in Singapore, PayNow takes the spotlight. Recognizing the potential for collaboration, the National Payments Corporation of India (NPCI) and the Monetary Authority of Singapore (MAS) joined forces in February 2023. They inked a memorandum of understanding (MoU) to link UPI with PayNow, creating a partnership between two prominent real-time payment systems. This groundbreaking alliance will enable users of UPI and PayNow to engage in instant and cost-effective cross-border transactions, regardless of their location. The mechanism facilitating this seamless connection is known as the Cross-Border Interoperable Payment System (CBIPS). CBIPS acts as a platform, facilitating connectivity between banks and financial institutions, allowing them to exchange payments across borders. Once implemented, users of UPI and PayNow will have the ability to initiate payments to each other by simply entering the recipient's UPI ID or PayNow ID. The system will then process the payment and transfer funds instantly, providing a swift and efficient cross-border payment experience. This development opens up new avenues for seamless cross-border financial interactions.
3. **Digital Signature** - Building upon the foundation of multi-factor authentication, UPI took a leap forward in enhancing transaction security and reliability by introducing digital signatures. This innovative feature is aligned with the concept of public and private keys in cryptography. When

[5] How dynamic QR codes are driving digital payments across businesses, Times of India (2022). https://timesofindia.indiatimes.com/blogs/voices/how-dynamic-qr-codes-are-driving-digital-payments-across-businesses/ .

[6] Deepa Baliyan & Neha Singh, *Unified Payments Interface (Upi): A Digital Transformation In India*, IJCRT, Vol. 3, Issue 3 (2023). ISSN 2320-2882.

a sender system digitally signs a transaction request, it involves the use of a digital signature algorithm, which relies on a pair of cryptographic keys: a private key and a corresponding public key. The digital signature serves as proof of the authenticity and integrity of the transaction request[7]. It ensures that the transaction has not been tampered with and can be verified using the corresponding public key. The public key is available to the verifying party, which can be a participant bank or the UPI central infrastructure.

4. **Recurring Payments** - Introducing a hassle-free solution for recurring payments, UPI Autopay revolutionized the way users authorize and manage pre-approved debits from their bank accounts. This innovative feature allows users to establish a one-time authentication process for automatic payments. With UPI Autopay, users can effortlessly link their bank accounts and set up instructions to authorize recurring payments at designated intervals. Whether it's daily, weekly, monthly, or annually, users have the flexibility to specify the frequency of payments. Once the authorization is in place, the predetermined amounts are automatically debited from the user's account on the specified dates, eliminating the need for any further action. From utility bills and online subscriptions[8] to loan EMIs and insurance premiums, UPI Autopay simplifies the payment process, ensuring timely and seamless transactions without the hassle of manual intervention.
5. **Digital Invoice** - UPI Invoice in the Inbox simplifies the process of generating, delivering, and managing invoices by leveraging the UPI infrastructure. It streamlines the billing and payment experience for businesses and customers. Customers can now receive the invoices directly on the UPI platform, swiftly review the itemized details, and initiate seamless payments without any hassle. The UPI-linked app keeps a record of received invoices in the inbox or notification section, ensuring easy access and reference whenever needed.
6. **One-time Mandates** - The One-Time Mandate feature, released as part of the UPI 2.0 package, allowed users to set up one-time or recurring payments with a predefined validity period. This feature simplifies the payment process for various use cases such as rent, insurance premiums, and donations. It found wider use in the travel industry as mandates were used to book tickets, cabs, and hotel reservations for future-dated travel. One of the excellent uses of mandates came in bidding for IPOs. Under Applications Supported by Blocked Amount (ASBA), investors can block the amount they want to invest in an IPO before the bidding process begins. This ensures that the investor has the funds available to pay for the shares if they are allotted. The investor creates a UPI mandate with their broker, which authorizes the broker to debit the investor's bank account, if and when the IPO is allotted.

[7] NPCI Circular NPCI/UPI/OC 123/2021-22 dated Nov. 03, 2021.

[8] Deepa Baliyan & Neha Singh, *Unified Payments Interface (Upi): A Digital Transformation In India*, IJCRT, Vol. 3, Issue 3 (2023). ISSN 2320-2882.

In addition to the above points, UPI expanded its reach beyond smartphones with the introduction of UPI 123Pay, enabling payments without the need for a smartphone. This innovative method operates by initiating payments through missed calls or SMS sent to a designated short code. Users simply need to enter the desired payment amount and their UPI PIN.[9] Subsequently, the payment is processed seamlessly. UPI Aadhaar Pay presents a convenient feature that empowers users to effortlessly make payments utilizing their Aadhaar number. This functionality operates by establishing a secure link between the user's Aadhaar number and their bank account.[10] To initiate a payment, the user simply needs to enter the desired payment amount along with their Aadhaar number. Subsequently, the payment is securely processed, ensuring a seamless transaction experience.

Innovative additions like these further enhance the versatility and appeal of UPI, making it a preferred choice for a wide range of users with varying requirements and preferences. UPI continues to evolve, adapting to changing demands and delivering an exceptional payment experience to its ever-growing user base.

Vulnerabilities & Cybercrime In Digital Payments

However, like any digital system, UPI is not without limitations or vulnerabilities that may pose risks to users' data privacy. Cybercrime is major limitation to any digital platform. 'Cybercrime' As cyber threats and attacks are on the rise, cyber security is the most pressing worry. Fraudsters are now using more advanced techniques to target the systems. Individuals, small enterprises, and major corporations are all affected. Frauds can be like duplicating customer IDs and profiles, trapping credit/debit cards, fraudulent SMS and emails to customers, fake calling on behalf of bank authorities, and sharing OTPs with family and friends. Therefore, these entire practices open door for cyber assaults and consumers suffer huge financial losses. According to the World Economic Forum, fraud and financial crime are a trillion-dollar business, with private companies spending $8.2 billion on anti-money laundering (AML) procedures alone in 2017.[11] As a result, all companies have recognized the requirement of cyber security and are working on implementing all available countermeasures.

Cyber Security Laws in India for digital payments

The Information Technology (IT) Act, 2000, is the primary legislation dealing with cybersecurity, data protection and cybercrime.

[9] 123Pay, NPCI website. https://www.npci.org.in/what-we-do/upi-123pay/product-overview .

[10] Google Pay introduces Aadhaar-based UPI activation, Hindustan Times (2023). https://www.hindustantimes.com/business/google-pay-introduces-aadhaar-based-upi-activation-heres-how-it-works-101686276892520.html .

[11] Anichebe, Uche, Combating Money Laundering in an Age of Technology and Innovation, SSRN (2020). http://dx.doi.org/10.2139/ssrn.3627681 .

- Sec. 43 of the Act applies to individuals who indulge in cyber crimes such as damaging the computers of the victim, without taking the due permission of the victim. In such a situation, if a computer is damaged without the owner's consent, the owner is fully entitled to a refund for the complete damage.[12]
- Sec.66 of the Act Applies to any conduct described in Section 43 that is dishonest or fraudulent. There can be up to three years of imprisonment in such instances, or a fine of up to Rs. 5 lakh.[13]
- Sec. 66C is quite relevant to this research. "The focus of this section is digital signatures, password hacking, and other forms of identity theft. This section imposes imprisonment upto 3 years along with one lakh rupees as a fine".

Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013, established the Computer Emergency Response Team as the administrative agency responsible for collecting, analysing and disseminating information on cybersecurity incidents, and taking emergency response measures. These rules also put in place obligations on intermediaries and service providers to report cybersecurity incidents to the CERT-In. The said 2013 rules require organisations to report incidents to the Computer Emergency Response Team within a reasonable time. Incidents include denial of service attacks, phishing and ransomware incidents, website defacements, and targeted scanning of networks or websites.

Further, IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 require companies that process, collect, store or transfer sensitive personal data or information to implement reasonable security practices and procedures [14].

Further, as part of Digital Payments Awareness Week (DPAW) 2023, RBI had proposed guidelines "Draft Master Directions on Cyber Resilience and Digital Payment Security Controls for Payment System Operators" which state "*To effectively identify, monitor, control and manage cyber and technology related risks arising out of linkages of PSOs with unregulated entities, who are part of their digital payments ecosystem, PSOs shall ensure adherence to these Directions by such unregulated entities as well, subject to a mutual agreement*". Regarding data security, the draft stipulates that PSOs must implement a comprehensive data leak prevention policy to ensure the confidentiality, integrity, availability and protection of business and customer information, both within the PSO's control and at vendor-managed facilities.[15]

[12] The Information Technology Act 2000, Section 43.

[13] The Information Technology Act 2000, Section 66.

14 Neha Chaudhari, Vijayant & Anand, A comparison of cybersecurity regulations: India, Asia Law Business Journal (2022). https://law.asia/india-cybersecurity-regulations-2022/ .

[15] *RBI proposes norms on cyber resilience, digital payment security controls for PSOs*, The Economic Times, June 2, 2023.

However, even after having above privacy provisions in place, digital payments are still very much prone to cybercrimes, as is elaborated below. This is so because of lack of proper data protection & privacy framework in India. While people have been granted right to privacy as fundamental right today, there are no legal provisions to directly hold an entity responsible for data frauds or breaches. It provides a major window to fraudsters to getaway. The term cybercrime as defined in the Oxford Dictionary is "*Criminal activities carried out using computers or the Internet*". In the growing rate of cybercrime, devices also played a major role. A report has shown smartphones are 18% vulnerable to cybercrime and wifi are 15%.[16] These two devices, smartphones and wifi, are both used for digital payments and therefore, there is a risk of monetary cybercrime as well.

The percentage of fraudulent digital banking transactions made using android apps has gradually increased over the previous several years. In the last two quarters of 2021, the entire proportion of fraud perpetrated via smartphones was expected to become more than 50%.

Organizations experience the following type of cyber-attacks on digital payment methods[17]:

- Phishing
- DDoS (Distributed Denial of Service)
- Exploits of Vulnerability
- Spam
- Malware
- Cyber espionage
- Social engineering
- Identity theft
- Merchant Fraud

Vulnerabilities Of UPI

From above mentioned cyber attacks, following are possible cyber-attacks on UPI and hence highlights potential limitations or vulnerabilities in UPI's framework in the Indian context:

1. **Phishing and social engineering attacks**: Phishing and social engineering attacks are common threats in the digital payments space. Attackers may attempt to trick users into revealing their UPI credentials or sensitive personal information through fraudulent websites, emails, or phone calls. These attacks exploit human vulnerabilities rather than specific weaknesses in UPI itself.

[16] Cremer, F., Sheehan, B., Fortmann, M. et al. Cyber risk and cybersecurity: a systematic review of data availability. Geneva Pap Risk Insur Issues Pract 47, 698–736 (2022). https://doi.org/10.1057/s41288-022-00266-6 .

[17] Agrafiotis, I., J.R.C.. Nurse, M. Goldsmith, S. Creese, and D. Upton. 2018. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity* .

2. **Third-party app permissions**: UPI allows integration with various third-party apps, including banking and payment apps. When users authorize these apps to access their UPI data, there is a potential risk that these apps may mishandle or misuse user data. Users need to exercise caution and review the permissions they grant to third-party apps.
3. **Unauthorized access to UPI PIN**: UPI uses a personal identification number (PIN) as a security measure for transactions. If an attacker gains unauthorized access to a user's UPI PIN, they can potentially initiate fraudulent transactions. Users should keep their UPI PIN confidential and avoid sharing it with anyone.
4. **Data breaches**: While UPI itself has not experienced any major data breaches to the best of my knowledge, data breaches at banks or third-party apps that integrate with UPI could potentially expose user information. Such incidents highlight the importance of robust security measures and adherence to data protection standards by all entities involved in the UPI ecosystem.

Data from the Ministry of Home Affairs shows a 34% higher occurrence of cybercrimes via UPI compared to other categories like card and e-banking fraud[18]. According to Union Finance Ministry, more than 95000 UPI related fraud cases were reported in 2022-23.[19]

These case studies highlight incidents or vulnerabilities related to digital payments in India, which can help illustrate potential risks to UPI's data privacy framework:

A. **BHIM data leak incident**: In 2020, it was reported that a security vulnerability in the BHIM UPI app, potentially exposed the personal data of millions of users. The vulnerability allowed an attacker to access sensitive user information, including names, phone numbers, email addresses, and transaction details. It was promptly fixed after it was brought to their attention, but this incident demonstrated the risks associated with data breaches in digital payment systems.[20]

B. **Sim-swap fraud and UPI**: This fraud is kind of attack wherein an attacker manages to convince a mobile network operator to transfer a victim's mobile number to a SIM card under their control or Using social engineering techniques such as phishing, vishing, and smishing, the fraudster acquires the victim’s banking information and registered mobile phone number. In some instances, sim-swap fraud has been used to bypass UPI's two-factor authentication and initiate unauthorized transactions. Such incidents highlight the importance of robust identity verification

[18] UPI frauds contribute to 15.3% rise in cybercrime complaints between Q1 and Q2 of 2022, Moneycontrol (2022). https://www.moneycontrol.com/news/business/upi-frauds-contribute-to-15-3-rise-in-cybercrime-complaints-between-q1-and-q2-of-2022-9461531.html

[19] 95,000-plus UPI-related fraud cases reported last year: Finance Ministry, The Times of India (2023), https://timesofindia.indiatimes.com/gadgets-news/95000-plus-upi-related-fraud-cases-reported-last-year-finance-ministry/articleshow/98975930.cms .

[20] Data of more than 7 million BHIM site users leaked: Report, Economic Times (June 2020). https://economictimes.indiatimes.com/tech/software/data-of-more-than-7-million-bhim-site-users-leaked-report/articleshow/76144061.cms?from=mdr .

measures and the need for users to be vigilant about securing their SIM cards and promptly reporting any suspicious activity to their mobile network operator.

C. **Malware Attack**: There was a report in March 20203 of cybercriminals looting INR 1 crore from 81 people in Mumbai.[21] It had emerged that the fraudster deliberately sends money to user's account using UPI apps. He/she then asks to repay the money on pretext that it has been sent by mistake. If user repays that amount to the caller's number, they would end up being a victim of a malware attack. When the user repays the money using UPI apps, then his/her entire data including bank and other KYC details including PAN, Aadhaar etc become available to the fraudster and such details are enough to hack the bank account.

These case studies emphasize the need for continuous improvement in security measures and user awareness to ensure the privacy and protection of UPI transactions and user data.

From above discussion of cybercrime in digital payments in India, it can be inferred that there is an immediate need to tackle the issue of cyber frauds. The common cyberattacks identified are phishing, identity theft, tampering with payment application. The payment instrument of UPI has two factor authentication model and is claimed to be a secure payment platform, yet it has been prone to cyberattacks and data frauds. It has been established through UPI providing digital invoice that the payment system records data on both ends, payer and receiver. The receiver here includes persons, merchants, payments made through PoS systems and like. On one hand, The EU is a developed economy with strict data protection policy and on another hand, India is a growing economy with currently no defined data protection and privacy policy. The digital payments are on the rise and especially with growing economy like India, the surge in transaction numbers is multifold, however, so is the increase in cybercrime. The RBI has time and again introduced guidelines and directions to regulate data protection in fintech industry but the implementation becomes an issue due to legal ambiguity on data privacy.

One of first EU countries to collaborate with NPCI for UPI is France. The majority of French consumers feel unsafe when shopping online, with 8 out of 10 consumers (80%) concerned about becoming victims of payments fraud when shopping via mobile phone or a computer, according to a new survey of more than 1,100 French consumers by ACI Worldwide (NASDAQ: ACIW). Nearly all French consumers (98%) now shop online, with one in three consumers doing so regularly (34%), the survey reported. But recent industry efforts to fight online payment fraud only reassures a minority of French consumers. Strong Customer Authentication (SCA) was introduced in 2020, a new

[21] Received money on your UPI app from a stranger? here's what you should do next, Hindustan Times (2023), https://www.hindustantimes.com/technology/received-money-on-your-upi-app-from-a-stranger-here-s-what-you-should-do-next-101679137602393.html .

European-wide requirement under which consumers and businesses must verify their identity with at least two authentication measures to make online payments more secure. But only 37 percent of respondents of ACI's survey said that "SCA is a reassuring factor for them when shopping online, followed by the presence of a 'secure payment 'logo (17%) and website addresses beginning with 'https '(13%)"[22]. Given these statistics, The issues of cybercrime in UPI may pose a hurdle in its introduction in EU region.

[22] "*80 percent of French consumers fear ecommerce payments fraud, new survey by ACI Worldwide and OpinionWay reveals*", ACI Worldwide (2021), https://investor.aciworldwide.com/news-releases/news-release-details/80-percent-of-french-consumers-fear-ecommerce-payments-fraud .

CONCLUSION

The UPI system has almost all of the desired features when it comes to ease of use working mechanism. The payments are made through QR codes, processed within seconds of time and provides digital invoices. The marketing activities vary with the software application being used. For instance, bonus points schemes and similar activities would be different on say GooglePay and PayTm UPI. However, there is some grey area when it comes to security measures in UPI system.

The digital payment platforms are more sensitive to cybercrimes as fraudsters gain both money and personal information of the victim. To prevent such attacks, UPI has two-factor authentication and as claimed by NPCI, the privacy is ensured by default working of the system. This default privacy mechanism is termed ‘privacy by design’ as is also enlisted in Art.25 of GDPR. Further, the Central Government of India has also introduced National Cybercrime Reporting Portal (NCRP) to report cases of cybercrime, including UPI frauds. It is also to be taken into consideration that the fraud numbers are in thousands against over 74.05 billion transactions yearly. If compared, number of fraud cases are very few. However, the lack of data protection framework at central level becomes a challenge against implementation of other data security measures.

As this article attempts to study working of UPI in EU, it is crucial to understand EU perspective on cybercrime and cybersecurity as well. The European Payments Council (EPC) conducted research in 2021 with the aim “to provide an insight in the latest developments on threats affecting payments, including cybercrime.” Strong Customer Authentication (SCA) was introduced in 2020, a new European-wide requirement under which consumers and businesses must verify their identity with at least two authentication measures to make online payments more secure.

Given this requirement of two-factor authentication under SCA (and the same is part of UPI’s working mechanism) and the presence of GDPR to grant privacy and hold fraudsters accountable, the researcher opines that UPI-led frauds may not be high in number whenever it comes into operation in EU. Though, India does need to introduce data privacy & protection policy soon in order to make UPI a global payment instrument. With technology advancing everyday, it is becoming increasingly difficult for the legal system to keep track of all the data breaches that occur and serve justice to such incidents. Adding to this difficulty is lack of personal data protection policy in India. In such situation, the best action of plan for the companies, government bodies and even individuals is to take operational security measures to avoid these attacks such as application security, passwords, multi-factor authentication et cetera.