NFSU JOURNAL OF FORENSIC ACCOUNTING & FRAUD INVESTIGATION

NJFAFI
Volume: 1, Issue: 2
December 2025
E-ISSN: 3107-4650

RED FLAGS IN UPI (UNIFIED PAYMENTS INTERFACE): A STUDY ON DIGITAL PAYMENTS IN INDIA

Ms. Isha Bhatt[1], Mr. Johny Chingakham[2]

Student, School of Management Studies, National Forensic Sciences University, Gandhinagar

Lecturer, School of Management Studies, National Forensic Sciences University, Gandhinagar

Abstract

The advent of UPI in India to ease transactions and turn the economy to become almost a cent percent cashless, has seen a huge success ever since its inception about 9 years ago. Indians, on average. conduct about 50-100 transactions per head in a week (or 650M+ transactions in a day[3]), be it to buy a milk packet or pay their monthly insurance premiums. Along with this ease comes a lot of chances for fraudsters to develop new modus operandi to commit financial fraud. This paper aims to shed light on the red flags that exist within the UPI system in India which also poses as the primary objective of the research. The secondary objectives are to pinpoint and categorise the factors that contribute most significantly to fraud, to compare the traditional electronic payments systems with UPI in terms of security, and to establish user specific insights via primary data collection. The data collection methodology was 'a questionnaire' that heavily relied on studying user behaviour and patterns about digital payments as well as stakeholder mapping (of sample units including CAs, Academicians, Cybersecurity professionals & ordinary citizens). The findings of the research include (but are not limited to) citing reasons behind the majority of fraud, work out targeted recommendations to reduce the red flags (& occurrence of fraud) that go unnoticed in the UPI system and do a parallel study of the mobile payments guidelines of India, EU and USA. Future scope of the study may include in-depth studies that cover the technical vulnerabilities that nudge the user towards falling victim to fraud. However, it is out of scope for the current study to cover any other kind of sophisticated digital fraud.

Keywords: Unified Payments Interface, cashless economy, financial fraud, technical red flags, user negligence, modern electronic payments, targeted recommendations

1. INTRODUCTION

In the world of digitisation, the payments industry was the one that still operated in complete cash mode. Soon after demonetisation was announced in India, the digital payment system picked up pace. The UPI (Unified Payments Interface) system developed by NPCI (National Payments Corporation of India) in joint efforts with the Reserve Bank of India, introduced the citizens to a technology that allowed them to make payments directly from their bank accounts via their mobile phones. Initially users could only operate UPI if it was linked to their bank accounts, now it is possible to link a PPI wallet to UPI directly as well. Essentially, UPI is an open infrastructure platform that allows tech companies (bigtech and fintech) and banks "to build their own apps with UPI as the TPAP (third-party application)" (Cornelli et al., 2024, p. 65)[4] The convenience of this system gave it a surge during the covid-19 pandemic helping in maintaining social distancing at shops etc. to conduct payments. It allowed citizens to make big transfers without having to go to the bank with the help of larger limits (P2P transactions).

However, the greater the convenience, the greater the chances of human error. Because we are adapted to use the system so frequently in our daily lives, we may not notice the subtle variations between a genuine link and a phishing link (about 66.6% of the respondents agree to this)[5]. Hence, user negligence proves to be the biggest reason why people fall victim to digital fraud[6]. The following study aims to detect, identify and analyse a few red flags in the system using a primary data set of 84 respondents that spans across various stakeholders such as Chartered Accountants, Academicians, Cybersecurity Professionals, Students, and Ordinary Citizens. The study tests the respondents for a variety of factors such as User Negligence, Technical Flaws, Inadequate Security and Awareness, etc.

NJFAFI
Volume: 1, Issue: 2
December 2025
E-ISSN: 3107-4650

The organisation of digital payments in India– lessons from the Unified Payments Interface (UPI)
Data sourced from primary dataset. (section 2 last question) (figure 1)
Data sourced from primary data set of the research (72.6% of the respondents share that user negligence is the biggest factor that contributes to fraud)

EASE_AND_SPEED_RELATION_TO_CARELESSNESS			
		Frequency	Percent
Valid	Strongly disagree	2	2.4
	Disagree	6	7.1
	Neutral	20	23.8
	Agree	50	59.5
	Strongly agree	6	7.1
	Total	84	100.0

Table 1: the table shows the percentage of people who confirm that ease and speed of UPI is directly proportional to the frauds that occur due to carelessness.

2. LITERATURE REVIEW

1. The first literature review carried out was on the paper "An Overview of India's Unified Payments Interface (UPI): Benefits, Challenges, and Opportunities" (Dr. A.Shaji George, et. al, 2023) which talks about benefits, challenges and opportunities for business in India due to the advent of UPI. Research Methodology followed in the paper was a study of scholarly & peer reviewed articles followed by analysis of government policies. It provides an overview of benefits and opportunities, but the important part of literature required for our analysis is the "challenges to widespread adoption of UPI". According to (George, et. al, 2023)
Vulnerabilities exist in spite of robust usage of advanced encryption technologies in UPI which were developed to protect user data from unauthorized users. It occurs due to lack of satisfactory security measures (e.g. two-factor authentication for transactions above a particular limit). UPI also does not have a high level of encryption like any other payment applications making it prone to cyber attacks.
However, it still does not specify the types of vulnerabilities and loopholes.

2. The second review was of a paper titled "The organisation of digital payments in India – lessons from the Unified Payments Interface (UPI)" (Cornelli, et. al, 2024). The primary purpose of the paper is to analyse how the digital payments market has changed, increase in investments and increased participation of rural segments in the financial sector. The paper is based on secondary data gathered and studied from the
RBI and NPCI public database. Although there is no specified gap in the paper, it highlights the scalability, interoperability and security issues with UPI. According to (Cornelli, et. al, 2024)
The rapid success of the UPI system also invites constant issues such as technical outages, server breakdowns and interoperability problems. These challenges are addressed via infrastructure improvements and standardization of the UPI system. However on an international level regulatory compliance, scalability and partnerships are still considered a major priority.
Identification and classification of these challenges still needs to be done in depth instead of relying on the occurrence of cases.

3. The third paper studied was "Fraud in Electronic Payment Transactions: Threats and Countermeasures" (Fernandes, 2013) which discusses electronic payment frauds as the broader topic and fraud detection and prevention measures as the niche topic. The primary aspect of the paper was to explore statistics on actual payment frauds and revenue loss due to fraud, via secondary data sourced from "Association of Financial Professionals (2012)" and "CyberSource (2012)". After classification of types of E-frauds, the paper discusses measures for fraud prevention and detection, in

detail, ranging from various fraud detection tools to raising public education and awareness. The author mentions "An ongoing research is necessary to reduce risk and protect merchants, consumers and financial institutions" (Fernandes, 2013). Hence drawing attention back to the primary goal of this paper which is to identify loopholes which help in reducing risk.

4. The fourth paper studied was "Fraud Risk in Electronic Payments" (David and Kovács, 2016) which provides an in-depth explanation of the recommendations and guidelines by the European Forum on the Security of Retail Payments. The paper's aim was to discuss the recommendations as well as timely review of regulations on the security of electronic payments and their vulnerabilities. The research was designed to explain a fraud case in the Hungarian Banking System (a clear example of the security risks associated with digital payments). The recommendations posed by the Forum will be used for further analysis in the paper against the guidelines formed by NPCI.

Digital payments are not just home to the Republic of India, but have also gained traction in the west. According to a report from the European Central Bank (2013, p.3),

It is imperative that any pertinent risks to the infrastructure need to be discovered and addressed in a constant pattern due to the fact that new internet payment methods are being developed along on a regular basis and along with that new modus operandi also comes to the market[7].

In light of the same, the Europe Central Bank (ECB) has had a series of guidelines pertaining to different forms of electronic payments since their advent. Narrowing down to the mobile payments system; David & Kovács (2016) say that,

The result of cooperation between payment service providers, customers, supervisors and overseers is the 'European Forum on the Security of Retail Payments'. The forum elaborated three sets of recommendations on security of Internet payments, payment account access services and mobile payments. The aim of these recommendations is to contribute to stopping payment fraud and working towards better consumer trust in mobile payments using a mobile payment application previously downloaded onto the customer's mobile device.

Similarly,

Fernandes (2013) says that Department of Justice (DOJ), U.S. has divided the computer frauds into the following three categories:

1. crimes where the computers and their related components are the target of a cyberattack; through which the fraudster obtains information illegally:
2. crimes in which the computer is the immediate subject of a crime, that is the attacks is on a computer or a system, destruction or disrupting of which is the damage caused; and
3. crimes in which computers and related systems are the means or "instrument" by which ordinary crimes are committed, such as theft of identities, data, or money or the distribution of child pornography (p. 26).

Out of the above three listed categories, crimes (digital frauds) carried out via mobile payments app where a fraudster uses sophisticated techniques of TPAP duplication, display of false text in the UI of the application (claiming that payment has been made), falsely generated voice-box messages of successful payment, etc. fall under the third category.

The table below presents a comparative analysis of the Mobile Payments Regulations from NPCI (National Payments Corporation of India), FDIC, USA (Federal Deposit Insurance Corporation) and ECB (European Central Bank).

Aspect	NPCI	ECB	FDIC
Fraud Prevention and Transaction Monitoring	PSPs and TPAPs must ensure their systems are secure and audited. NPCI provides transaction processing and settlement services, and PSPs manage grievance redressal and disputes.	Recommends that PSPs operate transaction monitoring mechanisms to detect and block fraudulent payments *before* final authorization. This includes analyzing abnormal patterns and known fraud scenarios.	Financial institutions are expected to use controls to prevent unauthorized transactions and comply with the Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) requirements.
Customer Education and	The roles of each participant are clearly laid	A key principle is that PSPs should engage in customer	It is noted that customer confidence is key to

Communication	out, but the document focuses less on direct-to-customer education programs.	awareness and education programs on security issues. They must provide secure channels for communication and clear instructions on the safe use of services.	adoption and that banks should educate consumers on securing their mobile devices. Unclear consumer protections across different products can create reputation risk.
Legal & Supervisory Framework	The framework is based on the rules and guidelines set by the NPCI for participation in its UPI system	Implementation is based on domestic legislation transposing the Payment Services Directive (PSD). National authorities are responsible for integrating the recommendations into their supervisory frameworks.	Existing laws like the EFTA (Regulation E), Truth in Lending Act (Regulation Z), GLBA, and prohibitions on Unfair or Deceptive Acts or Practices (UDAAP) are applied to mobile payments.

3. RESEARCH GAP

All of this in the end raises a few questions, especially about the security features in the UPI system that fraudsters are able to bend around and find loopholes. Fraudsters use these loopholes to scam people who might be a little technologically unsound in these matters, since it's a rapidly growing area. "Lack of digital literacy contributes to the success of UPI frauds" (data says 85.7% of people agree to this)[8]. "In a country like India with a population of 1.45 billion people, about 99.5% people in age group of 15-29 are reported to have the ability to perform online banking transactions through UPI"[9] (PIB, 2025, para. 1). "Most of these people belong to rural areas, where only 25% of the population is digitally literate compared to the 61% of the urban population"[10](Ministry of Labour & Employment, n.d., p. 4). It can be said that even though most of the youth in rural areas might be tech savvy, such niche knowledge about digital payments might not be handy to everyone.

4. RESEARCH QUESTIONS & DERIVATION OF OBJECTIVES

This leads us to asking our first question: What are some vulnerabilities in the system that prompt the end user to fall victim to digital fraud? Which poses as the primary objective of the paper. Through this study we expect to discover the same issues faced by users. The secondary questions are to identify and categorise the factors that contribute most to UPI

It is essential to note from our daily life experiences that in spite of the growing popularity of UPI, we mostly use it only in day-to-day transactions. For larger transactions, or bank to bank transfers, traditional methods such as NEFT-RTGS-IMPS, cheque payments, DDs, etc. are still preferred. This may majorly be due to our distrust in the security features of anything that requires us to use the internet. The daily limit of ₺100,000/- for UPI also plays a significant role. All of this circles back to the insufficiency of robust security measures that may prevent fraud. Studies indicate that consumers are apprehensive about the security of their financial information, the risk of fraud and potential for data breaches. "Trust and security concerns are significant challenges hindering digital payment adoption in India" (Ahmed et al, 2025)[11].

5. PROCESS OF QUESTIONNAIRE FORMATION

The survey questionnaire was built in a way to target the objectives; divided into 5 sections viz. 1. Respondent Profile and UPI Usage, 2. Fraud Awareness and Perception, 3. Identifying Red Flags and Causal Factors, 4. Personal Experience and Reporting, 5. Comparative Analysis and System Security.

Section one helps in getting stakeholder specific information as the sample population consists of Chartered Accountants, Professors/Academic Researchers, Cybersecurity Officers/Professionals, Students and Ordinary citizens. Section two gathers data about various types of fraud indicators (that contribute the most to fraud), comparison of old and new methods for security and convenience, etc. this section provides the highest amount of data for analysis and interpretation. Section three contains

questions that ask for respondent opinion on what are some potential red flags that the end user might overlook while paying someone. Section four briefly asks about personal experience of frauds (if any) and convenience of the reporting system. The last section carries out a comparative analysis of the different systems and an in-depth analysis of system security.

The questions used for data representation and analysis throughout the paper are as follows:

1. Rate the likelihood of these being fraud indicators: (likert scale ranging from Not likely to Very likely)
   a. Urgent payment requests
   b. Requests for UPI PIN sharing
   c. High value transactions from unknown sources
   d. Multiple failed transactions attempts
   e. Unsolicited refund messages
   f. Calls claiming to be from bank/upi provider
   g. Requests for OTP sharing
2. Which factor contributes the most to UPI fraud?
   a. User negligence
   b. Technical flaws
   c. Inadequate security
   d. Lack of proper knowledge
   e. Inadequate Awareness
   f. Lack of digital awareness, in terms of falling for fake and impersonating calls
3. In your opinion, which of the following is the most common type of UPI fraud?
   a. Phishing (fake links to steal UPI PIN)
   b. Vishing (fraudulent calls asking for OTP/PIN)
   c. Fake "collect request" scams
   d. QR code scams (scanning a QR code debits money)
   e. Remote screen sharing app fraud
   f. Identity fraud (fraudster linking your bank account to their phone)
4. To what extent do you agree with this statement: "The ease and speed of UPI transactions make users more careless about security checks."
   a. Strongly disagree,
   b. Disagree
   c. Neutral
   d. Agree
   e. Strongly agree
5. Please rate the frequency with which you consider the following as a potential "red flag" for fraud: (1= lowest frequency, 5= highest frequency)
   a. Receiving a QR code to scan to receive payment:
   b. A buyer on a platform like OLX insisting on using a specific, unknown QR code:
   c. Spelling mistakes or unprofessional language in a payment request message:
   d. Receiving a payment link via SMS or WhatsApp from an unknown source
   e. High-pressure tactics demanding immediate payment for an unexpected reason
6. Which of the following subtle red flags do you believe is easiest for an average user to miss during a UPI transaction?
   a. 1= "A minor spelling variation in a well-known VPA (e.g., sbi@okaxis instead of sbi@okhdfc)" ,

b. 2="The transaction message in a collect request being unrelated to the actual transaction",
c. 3="A fraudster using a personal name (e.g., "Rahul Kumar") on their UPI ID while pretending to be a business",
d. 4="A QR code presented on a piece of paper instead of a laminated, official-looking stand"

7. Please rate the UPI system against older electronic payment methods on the following specific attributes: (1= worse, 2=comparable, 3= better)
a. Transaction Speed
b. Potential for User Error (e.g., sending to a wrong recipient)
c. Ease of Reversing a Fraudulent Transaction (Chargeback)
d. Clarity of Transaction Details on Bank Statement
e. Security Against Unauthorized Use
f. Transparency of Transaction Charges/Fees

8. Do you believe that recurring payment defaults (e.g., a merchant's payment request being intentionally ignored) are a significant problem within the UPI for Business ecosystem?
a. Yes
b. No

9. To what extent do you agree with this statement: "The benefits of convenience offered by UPI outweigh its current security risks."
a. Strongly disagree
b. Disagree
c. Neutral
d. Agree
e. Strongly agree

10. If there was an option for a slightly slower but more secure UPI transaction (e.g., with an additional verification step), what is the maximum delay you would be willing to accept for a high-value transaction (in seconds)?
a. Short answer text

6. METHOD OF DATA COLLECTION

The method for primary data collection was in the form of a survey with multiple choice questions which allows the respondents to think well on their answer at their convenience. Sending out a Google Form as an online survey for our research helped us gather quality data within a short period of time. The multiple choice adds to the benefit as the user does not have to write long answers about their opinions, plus interpreting numerical data is easier than analysing word to word which might not translate correctly. The secondary data was collected and read over time by reading and reviewing papers across databases that either highlighted the security risks in the UPI system, or discussed the success of UPI in India with its future scope. At the cross roads of these two topics lies the research gap which we've tried to cover with this paper.

7. DATA ANALYSIS AND INTERPRETATION

All the data gathered was cleaned and coded according to the requirement of the analytical approach. A datasheet and codebook were created in an excel file corresponding to the data view and variable view respectively, in the SPSS (Statistical Package for Social Sciences) Software. A basic frequency and cumulative percentage analysis was carried out to map the highest and lowest contributing factor towards fraud.

Table 2: Major factors contributing to UPI fraud

Factors contributing to UPI fraud					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	user negligence	61	72.6	72.6	72.6
	technical Flaws	10	11.9	11.9	84.5
	Inadequate Security	10	11.9	11.9	96.4
	Lack of proper knowledge	1	1.2	1.2	97.6
	inadequate awareness	1	1.2	1.2	98.8
	lack of digital awareness	1	1.2	1.2	100.0
	Total	84	100.0	100.0	

The above data shows that user negligence is the biggest contributor to fraud, and we can make a suitable assumption that when combined with extreme ease of usage (table 1), users overlook the littlest of things that separate the genuine from fake. This brings us to the next point of the "subtle red flags" that we overlook and as a result end up being victims.

SUBTLE_RED_FLAG					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Minor spelling variation in a well known VPA	42	50.0	50.0	50.0
	Transaction message in a collect request being unrelated to the actual transaction	16	19.0	19.0	69.0
	Fraudster using personal name on the UPI Id pretending to be a business Id	13	15.5	15.5	84.5
	QR code presented on a piece of paper rather than the official stand.	13	15.5	15.5	100.0
	Total	84	100.0	100.0	

Table 3: Data displaying which red flags are the most responsible

As seen above, 50% of the respondents agree that a minor spelling variation (e.g., sbi@okaxis instead of sbi@okhdfc) is the easiest to miss. E.g. The VPA (Virtual Payment Address) can be a little different in your usual payment request but will go amiss due to frequency of use. Similarly, a well known business platform transaction showing a personal QR instead, is a sign that a fraudulent transaction might take place.

Let us look at the frequency of individual factors that might be indicative of a fraud taking place with a user.

1. An urgent payment request to fish and scout for money is one of the most common tactics used by fraudsters. People tend to give into the pressure of making an urgent payment in order to protect any information that might be at stake.

FRAUD_INDICATORS_URGENT_PAYMENT_REQUESTS					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not likely	5	6.0	6.0	6.0
	Slightly likely	13	15.5	15.5	21.4
	Neutral	9	10.7	10.7	32.1
	Likely	34	40.5	40.5	72.6
	Very likely	23	27.4	27.4	100.0
	Total	84	100.0	100.0	

Table 4: Data displaying likert scale values for urgent payment requests as a fraud indicator

2. RBI makes constant efforts to raise awareness not responding to unsolicited requests that ask you to share your UPI PIN to carry out a successful transaction. The UPI infrastructure does not require a person's pin to be shared at any point in time with the opposite party. The respondents agree the most to this factor.

FRAUD_INDICATORS_PIN_SHARING					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not likely	11	13.1	13.1	13.1
	Slightly likely	8	9.5	9.5	22.6

	Neutral	11	13.1	13.1	35.7
	Likely	9	10.7	10.7	46.4
	Very likely	45	53.6	53.6	100.0
	Total	84	100.0	100.0	

Table 5: Data displaying likert scale values for OTP/PIN sharing as a fraud indicator

3. A user might receive a text informing of a failed transaction where in reality the amount has been debited from their account; this may prompt them to make another payment resulting in huge loss. Every text from the bank server should be cross verified with bank balance and transaction history.

FRAUD_INDICATORS_FAILED_TRANSACTION					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	1	1.2	1.2	1.2
	Not likely	9	10.7	10.7	11.9
	Slightly likely	4	4.8	4.8	16.7
	Neutral	15	17.9	17.9	34.5
	Likely	13	15.5	15.5	50.0
	Very likely	42	50.0	50.0	100.0
	Total	84	100.0	100.0	

Table 6: Data displaying likert scale values for failed transaction as a fraud indicator

The list of different types of e-frauds contain Phishing and Vishing in the top five. "Phishing is an attempt by the fraudster to "fish" for your banking details through emails with attachment or hyperlink" (Fernandes, 2013). Vishing is a fraudulent call asking for the user to reveal sensitive information by creating a panic situation. Technology advances at a rate that the ordinary brain cannot comprehend, hence if a user receives a UPI payment link via their whatsapp or a call about an unsolicited transaction, the UPI ID of the sender needs to be verified by entering it onto any TPAP.

MOST_COMMON_UPI_FRAUD					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Phishing	24	28.6	28.6	28.6
	Vishing	22	26.2	26.2	54.8
	Fake collect request scam	7	8.3	8.3	63.1
	QR code scams	19	22.6	22.6	85.7
	Remote screen sharing fraud	3	3.6	3.6	89.3
	Identity fraud	9	10.7	10.7	100.0
	Total	84	100.0	100.0	

Table 7: Data displaying which type of e-fraud results in highest amount of upi fraud

8. IMPLICATIONS ON INDIAN ECONOMY

Briefly analysing from the above data, users falling victim to digital fraud (limited to UPI) is a concerning issue as around 70% to 80% retail payments are made via UPI (rough estimate). Let us take two different data tables for comparison, one which shows UPI transactions volume and value for the entirety of fiscal years and another which displays the amount of fraudulent transactions (in currency) for the same period.

Financial year	UPI Total Transaction (In Cr.)*	UPI Domestic Payment Fraud (In Cr.)**
2022-23	₹ 2010259.01 CR	₹ 573 CR
2023-24	₹ 1489145.44 CR	₹ 1087 CR

Table 8: comparative figures

**data sourced from NPCI Website under "UPI Monthly Product Statistics Trended"*
***data sourced from Ministry of Finance, Department of Financial Services (Lok Sabha Unstarred question no. 211, Fraud in UPI Transactions, Answered by Shri Pankaj Chaudhary)*

For financial year 2024-25 (until sept, 2024) nearly ₹ 485 CRs of amount has already been involved in UPI payment fraud. If it continues to occur at this rate, then by the time the Indian economy becomes nearly cashless, it would be impossible to control the frauds.

9. RECOMMENDATIONS & CONCLUSIONS

It is very evident from all the discussion presented above that there needs to be introduced little stricter security measures on the UPI infrastructure that will help a user differentiate between genuines and fakes before landing on a decision. Therefore it is not possible to completely remove the probability of fraud, however the occurrence can definitely be reduced. It can be curbed by implementing different measures of security control. (Fernandes, 2013)
However as we speak:
RBI is looking into replacements of traditional PINs and passwords for functions of authenticating transactional details such as the usage of biometric data of the user
such as their fingerprints and/or face ID. Its implementation may ensure lesser frauds as fraudsters would not have access to biometric data therefore improving the overall user experience of the UPI application. (PwC India, 2024)[12]
As retrieved from the primary data collection, respondents say that an average 30 seconds of delay for payment confirmation while processing high-value transactions would add another layer to the security of the process.
Future scope of this study includes developing stakeholder specific insights to find out which tier of the public is the most affected by frauds. Current scope is only limited to UPI , domestically. However, further research can be conducted on cross country UPI payments and understanding benefits and challenges of global scalability.

10. ACKNOWLEDGEMENT

This paper would not have been possible without the support of my mentor Mr. Johny Chingakham. His constant guidance has been an immense help in shaping the paper into what it is. I would also like to extend my gratitude to Dr. Bhavesh Parmar (Associate Professor, Central University of Rajasthan) for his in-depth instructions in running analysis on SPSS.

Lastly, I also thank my family and close friends for their undying encouragement and constant push to help me reach my goal.
Disclaimer

It is hereby disclosed that AI was used for about 2% of the entirety in the paper.. AI tools viz. Perplexity Pro (Basic & Research Mode) has been used to carry out the comparative qualitative analysis of the guidelines. However the content for analysis, i.e. the PDFs of the guidelines (sourced from respective official government websites) was provided by the author.

REFERENCES

[1] Ahmed, M., Yadava, L. N., & Kakkar, M. (2023). Challenges and Opportunities in the Adoption and Growth of Digital Payments in India: A Sociotechnical Perspective. *Vinimaya*, *44*(2), 19-30.
[2] https://www.researchgate.net/publication/390708333
[3] Cornelli, G., Frost, J., Gambacorta, L., Sinha, S., & Townsend, R. M. (2024, December). The organisation of digital payments in India–lessons from the Unified Payments Interface (UPI). In *SUERF: The European Money and Finance Forum, SUERF Policy Note* (No. 355).
[4] https://www.bis.org/publ/bppdf/bispap152_e_rh.pdf#page=1.00&gsr=0 Drozdowski, R., Homer, M., Khalil, E., Kopchik, J. (2012). Mobile Payments: An Evolving
[5] Landscape.
[6] *Federal Deposit Insurance Corporation.* https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin12/siwinter12-article1.pdf

[7] Fernandes, L. (2013). Fraud in electronic payment transactions: Threats and countermeasures.
[8] *Asia Pacific Journal of Marketing & Management Review. ISSN, 2319,* 2836. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=fraud+in+electronic+pa
[9] yment+transactions%3A+threats+and+countermeasures&btnG=
[10] Kovacs, L., & David, S. (2016). Fraud risk in electronic payment transactions. *Journal of Money Laundering Control*, *19*(2), 148-157.
[11] https://doi.org/10.1108/JMLC-09-2015-0039
[12] Forum on the Security of Retail Payments – SecuRe Pay (2013, January). Recommendations for the Security of Internet Payments. *European Central Bank. ISSN*
[13] 978-92-899-0866-5.
[14] https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf

Websites
[1] www.npci.org.in
[2] www.rbi.org.in