IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

An Analysis of Cyber Frauds in Digital Payment Platforms

Tausif Raza Firoz Ahmad Shaikh
Student, MCA, D.T.S.S. College, Mumbai

Abstract: *Digital payments have transformed the way people and businesses process money, and are making money move more quickly than ever. However, with the proliferation of these tech-focused approaches, online scams have not fallen behind and attack each new development. The tricks will be the same ones that keep showing up and up again: fake login pages, phone numbers that are stolen, UPI scams, QR code swaps, card details theft, and social manipulation. This paper burrows into the origin of these frauds, how they work, and the cost they impose on individuals and businesses. The statistics are too difficult to disregard: by 2025, the world is going to lose more than $50 billion, and almost 80 percent of businesses claim to have been victims of payment scams. The vices in the existing regulations, the holes in the general know-how, and technological constraints can be more visible by dissolving the existing threats. These discoveries present researchers, legislators, financial institutions, and the common people, with a better picture of the issue- so they can retaliate with more intent.*
With the increase in digital payments, cyber fraud increases.

Keywords: With the increase in digital payments, cyber fraud increases

I. INTRODUCTION

All this has changed with the entry of money online. Today, banks used to do this, now UPI does it, and wallets are phones, not in pockets. Contactless payments, check-out, and paperless transactions are ubiquitous. These methods are increasingly used by more folks annually. Making payments, transferring money, or even shopping- all one has to do is tap a couple of times on a screen. What was uncommon ten years ago is common today.

However, with the increasing number of people going digital, the hackers are not left behind. New holes are discovered with each upgrade, as intelligent scams discover new vulnerabilities. It is not only people who are losing it out, companies and banks feel it as well. By 2025, losses might cross $50 billion (CoinLaw, 2025). That's massive.

Use the example of India, such apps as PhonePe, Google Pay, and Paytm are used by millions every day. A lot of users are novice to the technology and this provides scammers with a loophole. Fraudsters feed on the lack of understanding and the trust people have in their household names. Counterfeit solicitation of money appears so authentic that it can deceive practically anyone. The more you believe in such a tool, the less doubtful you might become about an strange message that confiscates your money.

The focus of this work is on the manner and the reason why these scams occur on online payment systems. The various scams can be sorted to identify patterns. The operation of attacks is demonstrated in real life. The damage extends to wasted finances, the lost trust in the entire system. Although there are measures to prevent scams, there are loopholes. The study here summarizes the recent studies, reports and expert commentary.

DOI: 10.48175/IJARSCT-36701

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

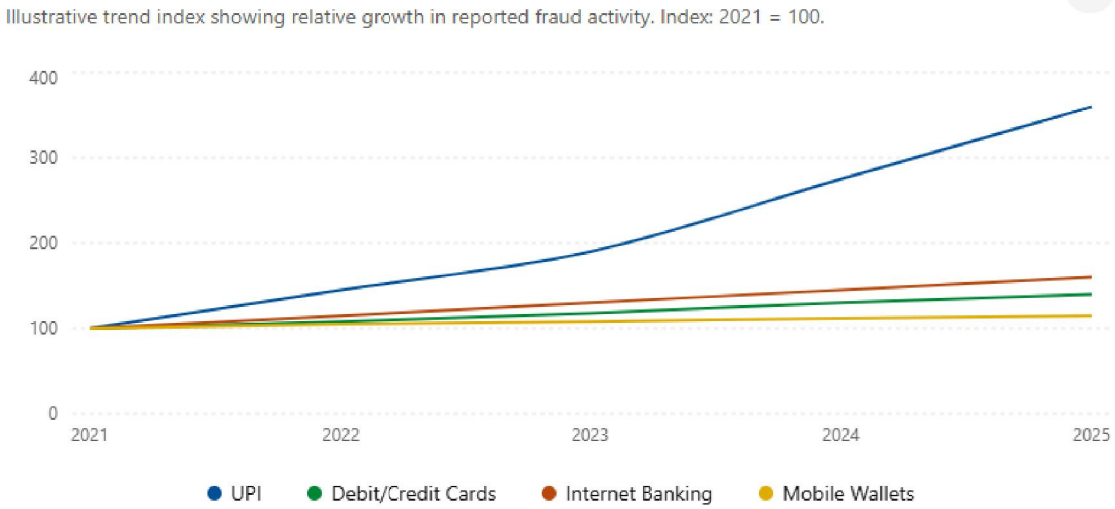

Fig 1. Illustrative trend index showing relative growth in reported fraud activity

II. LITERATURE REVIEW

The literature on online payment scams encompasses much, including tech malfunctions, human errors, haphazard regulations, and others. Every angle uncovered something unique, but none got the full story.

In 2007, Bhattacherjee and Hikmet demonstrated that the fear of scams consumes trust in online payment. In poor areas, Yeboah-Boateng and Essandoh research email cons and discovered that user education is equally important as technical security.

Quick forward a notch- machine learning is now employed in flagging frauds. In 2017, Awoyemi and his colleagues demonstrated that a combination of detection strategies is much more effective when it comes to detecting fake card activity. Although this paper does not establish a new system, such findings are included in the current discussion.

The 2025 survey of the Association for Financial Professionals found that almost 80 percent of companies became caught up in some form of payment fraud last year. Email cons continue to prevail, although individuals may be envisioning flashier approaches when imagining digital frauds. Their survey over a long period of time reveals the transformation of threats in the last 20 years.

In its most recent report, Sift estimates the global payment fraud to be approximately 3.3% in early 2025. Nevertheless, banks and fintechs received almost three times the number of fraud attempts as last year. There's more—a Recorded Future study found more than 269 million stolen card details floating around on the dark web. Digital skimers, embedded in the places of weakness of the shopping sites, are propagating at an unprecedented rate, as well.

The Reserve bank of India issues frequent warnings on increasing UPI scams. Voice phishing, or vishing, is trapping more victims and SIM swaps are allowing thieves to steal numbers and bank alerts. Layered logins, real-time monitoring are helpful, but user awareness is always a significant portion of the puzzle.

The vast majority of studies concur that it is not a single vulnerability that leads to digital payment fraud. It is a mess of technological malfunctions, lax policing, and a population that is still in training. The only solution to fixing it is improved systems, smarter rules, and more education.

III. DIGITAL PAYMENT PLATFORM TYPES OF CYBER FRAUD.

3.1 Phishing Attacks

Bank message email scams attempt to steal passwords and one-time codes, and they are the perpetrators of nearly 40 percent of the thefts of digital payments, according to the 2025 report of ZIGRAM. These counterfeits appear not only

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

on texts (smishing) but also on the phone. Shiny websites appear to be genuine and fool individuals into leaking personal data. These messages are now influenced by artificial intelligence making them sound personal and compelling.

3.2 UPI and Mobile Payments Fraud.

UPI is not without its issues particularly in India. One of the typical cons: counterfeit payment requests that appear as incoming funds but actually withdraw funds. Fraudsters occasionally convince users to give them access to their phone screens, which is tantamount to relinquishing control. Replacing actual QR codes with bogus ones, a strategy currently used across cafes or on buses, has escalated in the recent past.

3.3 SIM Swap Fraud

By defrauding the carrier, faking IDs, chatting, anything, scammers steal your phone number. As soon as they get your number, all the security codes designed to you fall into their hands. All two factor safeguards are downed with a flick of a switch. People can gamble away a lot of money without noticing that their number is stolen.

3.4 Card-Not-Present (CNP) Fraud

The majority of online payment fraud do not require the real card, just the numbers. Fraudulent purchases are made with stolen credentials, which are purchased or leaked over the Internet. This one-trick takes up almost 80 percent of digital store losses (ZIGRAM, 2025). All that a scammer requires when going on a virtual shopping spree is the numbers.

3.5 Social engineering and vishing.

Most of the thefts do not involve advanced technology, but psychology. Fraudsters impersonate figures of authority and manipulate your sense of urgency or fear and persuade you to send money or divulge secrets. Humanity follows the directive of authoritative-sounding voices and trust is the primary vulnerable point.

3.6 Business Email Compromise

Fake emails, which are usually disguised as orders by employers or business associates, persuade workers to divert funds. More than 60 percent of businesses claim that this is their number-one fraud concern and counterfeit bank transfer requests are becoming an increasing trend.

3.7 Account Takeover (ATO)

Someone accesses your account with the leaked or phishing websites login information. They move money, alter settings or make more scams in your name. Such attacks are more frequent as hacking has never been easier, thanks to the black market tools.

IV. MECHANISMS AND ROOT CAUSES.

The combination of technological vulnerabilities and human fallacy is behind most digital payment scams. The meaning of software flaws is only relevant when individuals are somehow tricked or in a hurry. Quick- click behaviour and flaky code work together to allow the attacks to pass.

4.1 Technical Vulnerabilities

Weak passwords (without two factor authentication), vulnerabilities in the code used in the back-end (such as the CosmicSting bug), or transfer instant (without being able to look into it) they all provide scammers with an opportunity.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

4.2 Humans and Behavioural Factors.

People are the ones that usually work scams, not systems. It is less difficult to target older adults or people who are not well-acquainted with technology. When somebody speaks in an official tone and forces you to do something without time, fear or uncertainty can make you obey them. Scam rates can be reduced by 15 by educating the users on warning signs.

4.3 Democratization of Cybercrime

It has never been that easy to become a cybercrook. Ready made scam packages, counterfeit logins and hacking tools are readily available in the dark corners of the internet and anyone can easily join the game. Voice and video deepfakes, which increased by a quarter last year, enable crooks to pose as real people convincingly.

V. EFFECTS OF ONLINE PAYMENT SCAMS

5.1 Financial Impact

The price tag is steep. The number of payment fraud may rise to over 50 billion by 2025. In the previous year companies lost approximately 6.5 percent of their income to frauds. Getting money back is not easy- less than 25 percent of the businesses recovered majority of the money, compared to 40 percent the previous year. In 2023, IBM lists that firms lost an average of 4.5 million per breach.

5.2 Psychological Impact

The aftermath? Stress, embarrassment and fear of digital banking. The most struggling users are older and those new to such platforms. There are victims who cease to use digital payments completely, which makes them not use financial technology at a faster pace.

5.3 Impact on companies and banks.

It's more than lost money. Frauds hurt businesses and banks with loss of their trust, loss of customers, and fines by regulators. The number of attempts at fraud by fintech companies increased almost 90 percent last year--new platforms, new targets. and it is cheaper to clean up a mess than to prevent it in the first place, and it is cheaper to plan up front than to clean up afterwards.

VI. EXISTING PREVENTION STRATEGIES

6.1 Multi-Factor Authentication (MFA)

Fraud is reduced with additional measures such as texted codes or fingerprint scans. CoinLaw reports that a reduction in transactions by scams was 22 percent because of one-time passwords. Nevertheless, this protection can be bypassed by SIM swaps and malware.

6.2 Machine-Learning Fraud Detection

An alert system powered by AI identifies suspicious actions immediately. Instant examination of the expenditure patterns reduced Internet fraud by one-third when larger sales were on. The system smashes patterns, detects anomalies and erects blocks before the money moves.

6.3 Regulatory Frameworks

Stricter rules help. India, and, in particular, its RBI, requires higher checks in identification and provides regulations on reporting and payouts to customers. The new European standards introduce stricter steps to the log-in process and transfer the responsibility to the sellers in the event of a theft, which helps to promote stronger measures.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

6.4 Consumer Awareness and Education

They can be as simple as a reminder regarding red flags and their avoidance. International collaborations are reducing the delay on cross-border scam response by almost 25 percent. Dissemination of the right information is time consuming, yet has a carving effect on the rates of fraud success.

6.5 End-to-End Encryption

Through encryption, messages are secured at all times and it is way too difficult to intercept payment information. CoinLaw says that this method reduces fraud in digital wallets by almost a fifth.

VII. PROBLEMS FIGHTING ONLINE PAYMENT SCAMS

Despite new technology and more challenging regulations, there are still obstacles. Scammers adapt quickly, always hunting for weak spots. Policymakers enhance regulation, but there are still loopholes. The development is a reality, yet full safety remains unattainable.

Scammers constantly invent new tricks, outpacing updates in security. International transactions make it difficult to trace or reclaim stolen money, and cross-border collaboration is cumbersome and sluggish.

Increasing the number of steps in the log-in process increases security but can be irritating to users. People value convenience. They may resort to less secure alternatives in case of frustrations of using safer options.

Silence is another obstacle since most individuals do not report being scammed, due to shame or an assumption that nothing will be done. This blinds the officials of the actual extent of the problem and undermines response efforts.

Deepfaked audio and video are now used by scammers to deceive even the most wary users, combining novel tricks with old ones, and overcoming countermeasures developed against previous threats.

Additionally, the elderly and individuals in low-income areas have a limited understanding of the fundamental digital skills that can help identify scams. Lack of strong know-how and confusion translate to greater errors and greater successful attacks.

VIII. ENDING REFLECTIONS AND FUTURE.

The problem of digital payment fraud has become a key problem of contemporary finance. Frauds include phishing and UPI tricks, SIM swaps, invisible card fraud, social manipulation, email hacks, and hacked accounts. Every attack unites tech savvy and human psychology. The outcomes struck wallets and tranquility. The payment companies and regulators are increasing their defences, yet the scammers continue to evolve.

The conclusion: payment fraud continues to expand - by 2021 the world has lost over half a trillion dollars through scams and scams are becoming more sophisticated due to the availability of easy-to-use tools and AI. Striking back will involve combining hard-tech with clever regulations, information exchange between industries, and never giving up on educating the populace.

Areas to monitor: Is it possible to use artificial intelligence to stop scams in the real-time, in various payment systems? Is layering in blockchain-identity identity reduction crime? What can nations learn of the regulations of other nations and how can they collaborate? On the human aspect, how come the scams continue to work when they are warned about severally? New studies can be done--particularly in the field of habits and daily decisions that predispose individuals.

REFERENCES

[1] Association for Financial Professionals (AFP). AFP Payments Fraud and Control Survey Report. AFP.

[2] Awoyemi, J. O., Adetunmbi, A. O., & Oluwadare, S. A. Credit card fraud detection using machine learning techniques: A comparative analysis. International Conference on Computing Networking and Informatics (ICCNI).

[3] Bhattacherjee, A., & Hikmet, N. Physicians' resistance toward healthcare information technology: A theoretical model and empirical test. European Journal of Information Systems, 16(6), 725–737.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 6, June 2026 Impact Factor: 8.2

[4] CoinLaw. (2025). Digital Payment Fraud Statistics 2025. Retrieved from https://coinlaw.io/digital-payment-fraud-statistics/
[5] FNBO. (2025). The Business Cost of Payment Fraud: Identification and Prevention Strategies. Retrieved from https://www.fnbo.com/insights/commercial-business/2025/business-cost-of-payment-fraud
[6] Mastercard / Recorded Future. (2026). Annual Payment Fraud Intelligence Report 2025. Retrieved from https://www.mastercard.com/us/en/news-and-trends/stories/2026/recorded-future-annual-payment-fraud-report.html
[7] Reserve Bank of India (RBI). (2024). Annual Report on Digital Payments and Fraud Management. RBI Publications.
[8] Recorded Future. (2024). 2024 Payment Fraud Intelligence Report. Recorded Future Research.
[9] Sift. (2025). Q1 2025 Digital Trust Index. Retrieved from https://sift.com/blog/tracking-the-evolution-of-payment-fraud-in-2025/
[10] Yeboah-Boateng, E. O., & Essandoh, K. A. (2013). Factors influencing the adoption of cloud computing by small and medium enterprises in developing economies. International Journal of Emerging Science and Engineering, 2(4), 13–20.
[11] ZIGRAM. (2025). Digital Payment Fraud Statistics 2025. Retrieved from https://www.zigram.tech/resources/digital-payment-fraud-statistics-2025/
[12] Checkout.com. (2025). Payment Fraud Trends in 2025 and How to Fight Them. Retrieved from https://www.checkout.com/blog/payment-fraud-trends