REVIEW OF RESEARCH
ISSN: 2249-894X
IMPACT FACTOR : 5.7631(UIF)
VOLUME - 15 | ISSUE - 2 | NOVEMBER - 2025

FINANCIAL CYBERCRIMES IN INDIA AND SAFE GUARD POLICY

Prof. Narendra Kumar Dhaka[1] and Navaneet Kumar[2]
[1]Professor and Guide at Nirwan University, Jaipur, Discipline – Law.
[2]Research Scholar at Nirwan University, Jaipur, Discipline – Law.

ABSTRACT :

The exponential rise of digital payments in India has been accompanied by a sharp increase in financial cybercrimes, particularly in online banking, ATM/card, and Unified Payments Interface (UPI) frauds. Despite regulatory measures by the Reserve Bank of India (RBI) and law enforcement, the frequency and sophistication of such crimes continue to escalate. Based on data from the RBI, state cybercrime cells, and government reports from 2023–2025, this paper analyzes the scope, trends, and institutional responses to financial cybercrimes in India. In FY 2024-25, RBI recorded over 13,500 card/internet fraud cases amounting to ₹520 crore in losses, while UPI frauds surged by 85% to 13.42 lakh cases, with losses exceeding ₹1,087 crore. The study examines major typologies of fraud, phishing, skimming, QR-code scams, SIM swaps, and mule accounts, and evaluates preventive frameworks including RBI's Master Directions on Digital Payment Security Controls (2021), the MuleHunter AI tool, and the Financial Fraud Risk Indicator (FRI) system. It also explores initiatives like the Indian Cyber Crime Coordination Centre (I4C), Citizen Financial Cyber Fraud Reporting System, and the National Cyber Crime Reporting Portal. The paper identifies persistent challenges: inadequate inter-agency coordination, under-reporting of cases, jurisdictional hurdles, and limited technical capacity in law enforcement. Policy recommendations emphasize legal reforms to strengthen the IT Act, improved coordination between RBI, NPCI, and police, enhanced consumer literacy, and adoption of AI-driven fraud detection systems. The paper concludes that only a cohesive, technology-driven, and internationally coordinated approach can effectively mitigate India's growing digital financial fraud crisis.

KEYWORDS: *Financial Cybercrime, UPI Fraud, Card and ATM Fraud, Mule Accounts, Fraud Risk Indicator (FRI), MuleHunter AI Tool, Regulatory Framework, Information Technology Act, 2000, Indian Cyber Crime Coordination Centre (I4C), Law Enforcement, Cyber Fraud Prevention, Cross-Border Cybercrime, Inter-Agency Coordination, Policy Recommendations, Digital Financial Security.*

I. INTRODUCTION

Recent years have witnessed an explosive growth of digital payment platforms in India, accompanied by a parallel surge in cyber-enabled financial frauds. Internet banking frauds, ATM/debit-card and credit-card scams, and Unified Payments Interface (UPI) frauds now dominate the landscape

of cybercrime. Data released by the Reserve Bank of India (RBI) and state cybercrime cells confirm that fraud continues to climb dramatically, even as regulators and law enforcement scramble to keep.[1]

In FY 2024–25 alone, RBI reported 13,516 cases of "card/internet" fraud (which includes ATM, debit/credit card and online banking losses), involving ₹520 crore a 53.5% decline in cases from FY24, but still the largest fraud category (56.5% of all bank frauds) in absolute numbers.[2] In contrast, UPI-specific fraud has been rising sharply: official data show UPI fraud incidents jumped from about 7.25 lakh in FY23 to 13.42 lakh in FY24, with losses of ₹1,087 crore in 2023–24. In sum, India's cybercrime reports surged to 86,420 cases in 2023, up 31.2% year-on-year of which nearly 69% (59,526 cases) were fraud-related.[3] These trends underscore the urgent need to analyse institutional responses, expose systemic gaps, and recommend policies to mitigate digital financial frauds.

This study explores the recent patterns of fraud involving online banking, ATM and credit cards, and UPI transactions in India. It primarily utilizes information published by the Reserve Bank of India (RBI), the cybercrime divisions of Maharashtra and Punjab, along with publicly accessible materials such as RBI publications, official government announcements, and media reports from 2023 to 2025.

We summarize total fraud cases and losses, typologies, reporting and resolution rates, consumer education initiatives, and regulatory actions. The analysis identifies key trends and challenges including rapid digital payment growth, social engineering scams, institutional coordination gaps, and cross-border enforcement hurdles and concludes with policy recommendations to bolster cyber-fraud prevention.

II. SCOPE AND TRENDS OF FINANCIAL CYBERCRIME

India's financial cybercrimes broadly fall into three categories: **online banking frauds**, where attackers use phishing or malware to exploit bank accounts or internet banking credentials; **ATM/debit/credit-card frauds**, involving skimming, cloning, or unauthorized transactions; and **UPI frauds**, where fraudsters exploit India's real-time mobile payment system (e.g. by fake QR codes, social-engineering UPI requests, or compromised merchant apps). Together, these crimes target consumers and financial institutions alike. The overall scale is staggering. NCRB data indicate that frauds were the motive in 59,526 of 86,420 cybercrimes reported nationwide in 2023 (68.9%), a sharp rise from 2022. State-level data (Maharashtra, Punjab) confirm hundreds of thousands of fraud cases.

According to RBI and government figures, **UPI fraud has doubled in a single year**. The Union Home Ministry informed Parliament in early 2025 that UPI-related fraud incidents rose from approx. 725,000 in FY 2022–23 to 1,342,000 in FY 2023–24, an 85% increase with losses over ₹1,087 crore (against ₹573 crore the prior year)[4]. Likewise, overall digital-payment (card/internet) fraud spiked in FY 2022–23, then fell by 53% in FY 2024–25 as anti-fraud controls took effect. Nevertheless, RBI's annual report (2024–25) emphasizes that digital-payment frauds dominate banking-sector fraud: card/internet frauds accounted for 56.5% of all bank fraud cases in FY25.[5] Thus, although card/internet frauds declined in FY25 (after a 4x jump in FY24), they remain numerically the largest category.

State cybercrime data reinforce these national trends. For example, Maharashtra's cybercrime cell reports thousands of fraud FIRs annually across categories, including online banking and UPI, and similarly Punjab's data show rising bank and UPI scam cases. Meanwhile, Delhi reports by mid-2023 suggested over 24,000 cyber complaints (up 200% YoY)[6], though much of that included phishing and social media scams, the largest share of digital theft cases. In short, **fraud is surging nation-wide**, underpinned by India's enormous digital-payment growth (which saw UPI transactions exceed 18,000 crores in FY 2024–25)[7] and pervasive social-engineering scams.

In the recent years the **types of frauds** have also evolved. Online-banking frauds now often involve *mule accounts* (fraudulent accounts used to collect stolen funds) and *SIM swap* attacks. ATM/card frauds still occur (skimming, cloning, phishing for OTPs), but RBI notes that many "card-not-present" thefts (OTP/CVV compromises) typically do not cost banks directly because liability shifts to customers once misbehaviour is established.[8] UPI frauds include fake payment requests (fraudsters

generating phony "collect" requests), fraudulent apps/websites mimicking legitimate wallets, and QR-code manipulations. Law enforcement also flags the rise of *"pig-butchering"* scams (online romance/love-baiting leading to investment fraud) and fake-loan or investment schemes while not strictly payment frauds, these often end with UPI or banking transfers to fraudsters.

A. Incident and Loss Statistics

i. **Total cases and losses:** The financial magnitude of these crimes is large. Government data show that in 2023–24, UPI scams alone caused over ₹1,087 crore in losses. The RBI's annual report cites ₹520 crore lost to card/internet fraud in FY25. Notably, these cases represent only those detected and recorded; large-scale under-reporting is believed, given that many victims never file complaints.

ii. **Channel breakdown:** Internationally, NCRB data have begun separating fraud by channel. For instance, a recent NCRB release (Ans. Data of Rajya Sabha Q262, Aug 2024) categorizes cases of credit/debit-card fraud, ATM fraud, online banking fraud, and OTP fraud by state (2018–2022). Although Delhi's open data portal shows that ATMs and card frauds remain significant across states, UPI frauds are now rising faster. Media reports confirm that UPI fraud cases jumped by 85% in FY24, vastly outpacing the growth of card/ATM frauds. Indeed, according to NCRB related news, **ATM fraud is now being overtaken by digital scams**. For example, one 2025 report notes that in Bihar (a surprising current hotspot), ATM fraud topped at 895 cases, but fraud in general drove most cybercrime growth.

III. REGULATORY FRAMEWORK AND RBI INTERVENTIONS

The Reserve Bank has responded with a multi-pronged regulatory approach. On the preventive front, RBI's **Master Directions on Digital Payment Security Controls (Feb 2021)** set minimum security standards for all banks, covering internet banking, mobile apps, card payments, etc.[9] It requires two-factor authentication, device-binding, transaction limits and more, specifically to thwart frauds on UPI and card channels.[10] RBI's earlier **Cyber Security Framework (2016)** mandated periodic audits and incident reporting. RBI also enforces **customer liability caps**: after October 2022, banks must bear losses from unauthorized transactions if customers report fraud promptly and did not contribute to the negligence (subject to small initial liability) a policy intended to bolster trust, though it has triggered debate over the definition of "negligence."

RBI has issued **advisories and circulars** on banking frauds. For example, RBI circulates regular instructions on ATM security (skimming prevention, PIN confidentiality) and alerts on SIM-swap frauds. A 2023 Lok Sabha reply notes various RBI advisories on ATM/Debit-card skimming, SIM Swap frauds, mobile banking scams, etc., and highlights RBI's 2016 cybersecurity circular and the 2021 Master Direction.[11] In effect, RBI has gradually tightened controls over how banks must authenticate transactions. One timely example: RBI's "Digital Payment Landscape and Security Guidelines" of February 2024 (a master direction update) now explicitly includes UPI and QR fraud risk mitigation, and mandates banks to develop robust fraud-risk management frameworks. In addition, RBI's 2023 "Payments Vision 2025" strategy emphasized fraud-prevention and customer education (RBI's reports stress that banks must undertake real-time fraud detection and reimburse victims fairly).

i. **MuleHunter AI tool:** Another major RBI initiative is the **MuleHunter AI tool**. In March 2025, RBI launched this AI-based system to detect and flag money-mule accounts (bank accounts used as intermediaries in fraud). According to government press releases, MuleHunter has since identified suspect accounts across banks.[12]

ii. **Financial Fraud Risk Indicator (FRI) tool:** This complements an earlier step in 2024. The RBI mandated that all banks and payment providers use DoT's new **Financial Fraud Risk Indicator (FRI)** tool, which shares telecom-based risk signals about suspected fraud. Through FRI, banks can automatically blacklist suspicious numbers or devices at the time of banking transactions.[13] These

technological controls are part of RBI's move to integrate cross-sector fraud intelligence (telecom and finance).

iii. **Consumer Protection and Education:** RBI has also focused on awareness. The RBI's *Secure Digital Transactions* portal and periodic circulars urge consumers not to share OTPs, not to use public Wi-Fi for banking, and to verify payment URLs. Banks are directed to send SMS alerts on transactions and to educate customers on fraud patterns. In March 2025, RBI and NPCI jointly launched a nationwide awareness campaign via SMS, social media, radio and TV on the Do's and Don'ts of UPI and digital payments.[14] These campaigns remind users about device-binding (linking UPI apps to registered smartphones), two-factor authentication, daily transaction caps, and official fraud reporting channels. NPCI's **Chakshu SMS system** (launched late 2022) helps users identify fraudulent messages. Despite these efforts, RTI responses indicate that consumer education remains a work in progress as the Maharashtra's police have conducted some outreach (police stations issue advisories, police-run websites list fraud alerts), but often cite lack of manpower for broader education campaigns.

iv. **Regulatory Gaps:** Despite all the above efforts, gaps remain in the legal framework. RBI's authority covers banks and regulated payment providers, but many frauds now exploit weaknesses in unregulated apps or foreign platforms. The IT Act, 2000 and the Penal Code (BNS) cover cyber frauds, but neither has been fully updated for modern payment systems. For instance, as RBI itself noted to an RTI (Mar 2024), the laws applicable to some UPI-related interfaces are not clearly enumerated under RBI's purview. Furthermore, RBI's jurisdiction is domestic: many frauds originate via offshore call centres (e.g. "call centre fraud" rings) or foreign SIMs. The RTI responses show RBI often defers to NPCI or law enforcement for UPI fraud details, and the RBI cannot directly investigate cross-border cases. Thus, significant challenges arise in prosecuting fraudsters located abroad, even under mutual legal assistance treaties.

IV. LAW ENFORCEMENT AND INTER-AGENCY COORDINATION

Law enforcement of financial cybercrimes falls mainly to police cyber cells and federal agencies. Key institutions now include the state **Cyber Crime Cells** (e.g. Maharashtra State Cyber Crime Department, Punjab Cybercrime Cell, Delhi Police Cyber Unit) and the central Ministry of Home Affairs (MHA) initiatives. The RTI data from Maharashtra and Punjab demonstrate active engagement: their cyber cells have registered thousands of fraud cases in recent years. The states report special units or task forces dedicated to e-fraud, with trained officers handling online banking and UPI complaints. The RTI from Punjab noted that cybercrime action relies "substantially under IT and IPC laws (BNS)", meaning officers use provisions like IT Act Section 66C/66D and IPC sections 420/467/468 to prosecute fraud.)

At the **national level**, the government has launched several coordinated mechanisms. The MHA set up the **Indian Cyber Crime Coordination Centre (I4C)** to streamline cybercrime response, including thematic verticals for payment fraud.

In March 2025, the government announced the **Citizen Financial Cyber Fraud Reporting and Management System**, a unified portal for bank fraud complaints and so far it has handled 13.36 lakh complaints and reportedly helped recover about ₹4,386 crore by routing reports to banks (MHA data).[15] The **Cyber Fraud Mitigation Centres (CFMCs)**, a network of cell groups comprising banks, telecoms, and police – provide round-the-clock action on high-value fraud cases. Home Ministry data to Parliament note that CFMCs have led to blocking of thousands of suspect WhatsApp/SKYPE IDs and SIMs (7.8 lakh SIMs, 2.08 lakh IMEIs blocked) and identification of mule accounts (20 lakh mule accounts flagged, saving ₹2,889 crore). The *National Cyber Crime Reporting Portal* (cybercrime.gov.in) further allows citizens to lodge fraud complaints which auto-forward to local police. In short, India has built a multi-agency framework (banks, NPCI, RBI, telecom, and police) to combat cyber fraud.

i. **State Coordination:** Within states, however, coordination can be uneven. The Maharashtra RTI shows that the State Cyber Crime Department does have special squads, but often refers to ED (Enforcement Directorate) or EDPS (Economic offences) for certain investigations. Punjab's RTI noted that trends/patterns are hard to track due to data gaps ("records are not maintained as per these points"). According to media sources, the Delhi Police established a dedicated Cyber Police Station in 2023 to address e-banking frauds, working in coordination with the Crime Branch. However, structured data exchange between city, state, and central authorities is still in progress. Significantly, an RTI filed with the RBI in December 2023 sought details about its collaboration with law enforcement and payment service providers. The RBI's reply referred to its existing fraud-reporting framework and partnerships through entities such as I4C, though comprehensive inter-agency standard operating procedures are still being developed.

ii. **Cross-Border Enforcement:** A major concern is the rise of cross-border financial fraud. Numerous UPI and banking scams either originate from or are coordinated through foreign locations, such as call centres abroad using Indian telecom SIM cards. To pursue offenders operating outside the country, Indian authorities depend on Mutual Legal Assistance Treaties (MLATs) or Interpol cooperation, both of which are often time-consuming. Reliable data on international fraud prosecutions remain scarce; an RBI response to an RTI query indicated that the bank held "no information" regarding UPI-related frauds committed overseas. Likewise, when foreign banks are implicated such as a fraudulent account in Singapore receiving stolen UPI funds issues of jurisdiction complicate investigation and recovery.

Government statements highlight efforts toward greater international collaboration, noting India's participation in the Budapest Convention on Cybercrime through the EDMC and its growing coordination with agencies like the Singapore Police and the U.S. FBI. Nevertheless, enforcement challenges persist. According to an NDTV report citing parliamentary data, the government is developing a global database of known cyber offenders (a "suspect registry") to facilitate cross-border tracking and has also worked with banks to freeze multiple mule accounts. Despite these initiatives, cybersecurity specialists point out that the absence of integrated international databases and comprehensive extradition treaties continues to allow cybercriminals to exploit foreign safe havens an institutional deficiency that requires urgent policy intervention.[16]

V. CONSUMER EDUCATION AND PREVENTIVE MEASURES

Regulators and law enforcement have stressed the importance of consumer awareness to curb fraud. The RBI/NPCI press release (March 2025) highlights the use of SMS advisories, radio/TV campaigns, and online 'phony transaction' alerts to educate the public. Banks now display anti-fraud tips in branches and apps. At the same time, victim-support is recognized as crucial. The Banks are mandated to have grievance redressal cells for fraud complaints, and the new DoT-FRI system helps telecom operators cut off fraudsters' SIMs even before banks see the transaction. Under RBI's *"Zone of Trust"* initiative, banks monitor the device and network used for UPI transactions, warning or blocking suspicious attempts. NPCI's *fraud monitoring solution* (an AI/ML engine deployed to banks) similarly flags anomalies in real time.[17]

Despite these steps, **consumer complacency** and misinformation remain huge challenges. The truth is that the users still fall for phishing and social-engineering scams. Media watchdogs and consumer groups periodically publish lists of current fraud tactics, but noted that, *"nearly half of UPI fraud victims never report the crime"*, creating blind spots. State police units have launched fraud-awareness drives (e.g. Maharashtra Police's cyber cell issues alerts on WhatsApp groups), but their scale is limited. There is a general consensus that **more proactive outreach** is needed. Stronger consumer literacy in recognizing fake calls, links and requests for payments is repeatedly emphasized in RBI circulars and press statements.

VI. CHALLENGES AND INSTITUTIONAL GAPS

There are Several recurring challenges and gaps weaken India's ability to combat financial cybercrime:

i. **Rapid Technology Change:** Fraudsters rapidly adjust to new payment technologies. For example, the RBI's initiative to implement tokenization for card transactions substituting CVV codes with dynamic tokens will require time for full adoption, during which card data theft continues. Similarly, new UPI functionalities such as "autopay mandates" and "international UPI" demand updated security evaluations. In response to an RTI query, the RBI acknowledged that it lacks complete information regarding newer UPI interfaces like BillPay and Autopay, citing NPCI's regulatory framework. This highlights a noticeable gap between financial technology innovation and regulatory supervision.

ii. **Fragmentation of Rules:** Payment fraud cases typically involve multiple stakeholders, including banks, e-wallet service providers, the NPCI, telecom operators, and law enforcement agencies, making coordination a challenging task. For instance, banks classify such incidents as "Frauds" when reporting to the RBI, whereas the police register FIRs under relevant sections of the IPC or IT Act. The research also revealed significant consumer confusion regarding the proper reporting channels — victims are often uncertain whether to contact their bank branch or the local cybercrime unit. Hence, the development of unified Standard Operating Procedures (SOPs) for seamless case coordination, such as when the police require bank transaction details, remains an ongoing effort.

iii. **Inter-Agency Cooperation:** Multiple agencies like RBI, NPCI, police, CERT-IN, NCIIPC (National Critical Information Infrastructure Protection Centre) and telecom regulators (DoT, TRAI) tackle fraud. But overlaps exist. For instance, both RBI and MHA have fraud-reporting portals (RBI's FEDAI/large fraud monitoring and MHA's citizen portal); aligning data is difficult. The April 2025 PIB release stresses that I4C and CFMCs create forums for swift action,[18] yet these are relatively new and their inter-state reach is still evolving.

iv. **Investigation Capacity:** Many state cyber cells report severe staff and expertise shortages. The Maharashtra RTI response "What measures has Maharashtra police taken…" answer confirms that formation of special cyber squads and ATF (anti-terrorism) wings investigating fraud cases, but also notes personnel constraints. Similarly, Punjab's cyber branch pointed out training gaps: many investigating officers lack IT training beyond basic police courses. Recruiting and specialized training for cybercrime investigators is often cited as inadequate. Extended family visits by MHA and state governments note the need for more forensic labs and digital evidence management (only a fraction of cybercrimes yield usable digital trails in court).

v. **Victim-Friendly Procedures:** The RBI's own UPI grievance guidelines envisage resolution within 30 days, with banks reimbursing victims by set rules. However, RTI replies (e.g. RBI on "how long for UPI complaint resolution") show mixed data. Victims report that responses vary widely by bank and state, some see refunds in a week, others wait months with repeated follow-ups. Moreover, the procedure for lodging police FIRs is often cumbersome, as victims are typically required to file complaints in person within specific jurisdictions, which discourages reporting. There is currently no unified online platform dedicated to registering payment fraud complaints directly with the police. Enhancing the accessibility and convenience of both bank grievance systems and FIR filing processes is widely recognized as a necessary reform.

vi. **Cross-Border Enforcement:** As mentioned earlier, pursuing cybercriminals operating from foreign jurisdictions remains a major challenge. According to a report, the Indian government has been working to enhance international collaboration through data sharing and the use of INTERPOL notices. However, in the absence of harmonized global cybercrime regulations, offenders continue to exploit countries with weak enforcement mechanisms. Experts consistently advocate for bilateral agreements on cybercrime and stronger engagement in international cyber-surveillance platforms. Although compliance with the Financial Action Task Force (FATF)

standards has improved the monitoring of financial transactions, both the RBI and law enforcement agencies acknowledge that cybercrime remains inherently "borderless" and only partially managed under the existing legal systems.[19]

VII. POLICY RECOMMENDATIONS

To mitigate and prevent digital financial frauds, the following recommendations emerge:

1. **Strengthen Legal Regime:** Revise the Information Technology Act, 2000 to clearly encompass new-age fintech platforms such as UPI, digital wallets, and cryptocurrencies, and to introduce defined offenses for cyber fraud with international applicability. Strengthen clauses related to the admissibility of digital evidence and accelerate the establishment of dedicated cyber courts.
2. **Enhance Coordination:** Establish standardized data-sharing frameworks among agencies. For instance, develop an integrated Financial Cybercrime Reporting Platform that enables real-time fraud reporting by the RBI, NPCI, banks, and law enforcement authorities (expanding upon the existing citizen portal). Strengthen institutions such as I4C and CFMC by granting them explicit powers to coordinate and oversee inter-state investigations.
3. **Invest in Law Enforcement:** Allocate resources to establish additional cyber forensic labs and enhance the training of police personnel in financial fraud detection and investigation. Create specialized cyber units in all major cities and regions with expertise in banking operations. Promote the temporary deputation of technology professionals to assist law enforcement agencies.
4. **Cross-Border Treaties:** Negotiate bilateral and multilateral agreements focused on combating cyber fraud. Partner with Interpol's financial crime divisions to identify and monitor cross-border money mule operations. Work in coordination with international regulatory bodies, such as the Monetary Authority of Singapore, to track UPI-linked accounts located overseas.
5. **Standardize Bank Procedures:** The RBI should implement standardized procedures for handling customer complaints across all banks. For instance, banks should be required to disclose transparent timelines for resolving fraud cases and ensure automatic escalation to the ombudsman if these timelines are exceeded. Additionally, an interim ex-gratia compensation mechanism should be introduced to support victims while the final decision from the bank is pending.
6. **Consumer Empowerment:** Implement continuous public awareness initiatives through schools, community centres, and mass media. Integrate cybercrime prevention and online fraud awareness into compulsory digital literacy programs. Introduce a "Cyber Secure" accreditation for merchants and payment platforms that comply with prescribed safety norms, enabling consumers to identify trustworthy and secure services.
7. **Regulatory Scrutiny of Apps:** The RBI and NPCI should introduce a **"fraud alert registry"** listing known malicious applications and unauthorized UPI payment service providers. They should collaborate with Google and Apple to ensure these apps are **removed or blocked** from their respective app stores.
8. **Use of Technology:** Enhance the use of advanced AI tools (such as MuleHunter and FRI) and motivate banks to implement machine learning systems for comprehensive fraud detection across all payment channels, beyond just cards and UPI. Encourage the adoption of tokenization and biometric verification methods (such as mobile OTPs through authenticator applications) to minimize dependence on traditional SMS-based OTPs.
9. **Data Transparency:** Publish consolidated fraud statistics each year, categorized by type and region, to enhance transparency and accountability. For instance, release a summarized version of RTI data from police records (including FIRs and case outcomes related to ATM and UPI frauds) in a centralized database, enabling policymakers to monitor emerging patterns and trends effectively.
10. **Consumer Redress:** Enhance grievance resolution mechanisms by establishing a unified Digital Banking Ombudsman dedicated to addressing e-fraud complaints. Facilitate the online registration

of FIRs for UPI and banking frauds (as already implemented in certain states) to enable victims to report incidents irrespective of their location.

VIII. CONCLUSION

India's digital payments revolution has significantly reshaped its economic framework, promoting financial inclusion and convenience on an unprecedented scale. As one of the most populous countries in the world with a vast, increasingly tech-savvy population proficient in mobile and Internet usage India holds tremendous potential to emerge as a global leader in the digital economy. However, this rapid wave of digitization has simultaneously exposed millions to new forms of cyber vulnerability.

Although the Reserve Bank of India (RBI) and law enforcement agencies have undertaken notable initiatives such as issuing regulatory directives, launching public awareness programs, and setting up coordination centres cyber fraud continues to rise at a concerning rate. The surge in reported incidents across various states indicates that cybercrime cells remain overburdened, facing shortages of personnel, infrastructure, and technological expertise.

To protect consumers and uphold the stability of the financial system, India must urgently address existing policy gaps, reinforce its investigative frameworks, and foster a culture of cybersecurity awareness and responsibility among all stakeholders. These measures are vital because institutional interventions particularly those involving the formulation and execution of new laws, processes, and preventive mechanisms require considerable time and sustained collaboration. In contrast, cybercriminals are highly adaptive, driven by singular motives, and employ sophisticated methods, tools, and unconventional tactics to exploit both technological and regulatory weaknesses.

Another layer of complexity arises from the challenge of territorial jurisdiction. In the digital realm, physical boundaries have little significance, and fraudulent operations can be executed seamlessly across multiple regions or nations. This borderless nature of cybercrime calls for stronger inter-agency coordination, international collaboration, and harmonized legal standards.

Ultimately, only through persistent vigilance, enhanced capacity building, and unified efforts across institutions, states, and international borders can India hope to effectively counter the escalating threat of digital and financial cybercrime.

REFERENCES

[1] *Internet, Card Frauds Halve in FY25: RBI Data*, *Times of India* (June 12, 2025). Government of India, Ministry of Home Affairs, *Lok Sabha Unstarred Question No. 384*; Neeta Sharma, *Digital Frauds, Including in UPI, Have Doubled: Home Ministry to Parliament*, *NDTV* (Mar. 26, 2025), available at https://www.ndtv.com/india-news/digital-frauds-including-in-upi-has-doubled-home-ministry-to-parliament-8018240.

[2] *Id*

[3] Neha (Staff Reporter), *NCRB: Bihar Reports 4,450 Cybercrime Cases in 2023, Tops Nation in ATM Fraud*, *Times of India* (Oct. 9, 2025).

[4] Neeta Sharma, *Digital Frauds, Including in UPI, Have Doubled: Home Ministry to Parliament*, *NDTV* (Mar. 26, 2025).

[5] *Internet, Card Frauds Halve in FY25: RBI Data*, *Times of India* (June 11, 2025).

[6] *Cybercrimes Soar in Delhi, Complaints Jump 200% in 2023*, *The Economic Times* (Aug. 15, 2025).

[7] Press Information Bureau (PIB), *Digital Payment Transactions Surge with Over 18,000 Crore Transactions in 2024–25*, Press Release (Mar. 11, 2025), available at https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2110405.

[8] *Internet, supra note - v*

[9] Press Information Bureau (PIB), *Various Measures Have Been Taken by the Government to Strengthen Cyber-Security in the Financial Sector*, Press Release (Mar. 18, 2025).

[10] Government of India, *Various Measures Have Been Taken by the Government to Strengthen Cyber-Security in the Financial Sector*, *Press Information Bureau*, Press Release (Mar. 18, 2025); Neeta Sharma, *Digital Frauds, Including in UPI, Have Doubled: Home Ministry to Parliament*, *NDTV* (Mar. 26, 2025), available at https://www.ndtv.com/india-news/digital-frauds-including-in-upi-has-doubled-home-ministry-to-parliament-8018240.

[11] Government of India, Ministry of Finance, *Lok Sabha Unstarred Question No. 4142: UPI/Cyber Frauds* (answered Mar. 27, 2023), available at https://sansad.in/getFile/loksabhaquestions/annex/1711/AU4142.pdf?source=pqals#:~:text=instructions%20pertaining%20to%20security%20arrangements,pertaining%20to%20various%20aspects%20of.

[12] Press Information Bureau (PIB), *supra note – ix*

[13] Press Information Bureau (PIB), *RBI Advises Banks to Integrate Risk-Based Metrics That Classify Cyber Threats*, Press Release (July 1, 2025).

[14] Press Information Bureau (PIB), *Various Measures Have Been Taken by the Government to Strengthen Cyber-Security in the Financial Sector*, Press Release (Mar. 18, 2025); Press Information Bureau (PIB), *Digital Payment Transactions Surge with Over 18,000 Crore Transactions in 2024–25: RBI, NPCI Launch Awareness Campaigns and AI-Based Solutions to Prevent Financial Cybercrimes*, Press Release (Mar. 11, 2025).

[15] Neeta Sharma, *Digital Frauds, Including in UPI, Have Doubled: Home Ministry to Parliament*, *NDTV* (Mar. 26, 2025).

[16] Press Information Bureau (PIB), *Various Measures Taken by Government to Strengthen Cyber-Security in the Financial Sector*, PR ID 2112323 (Mar. 18, 2025).

[17] Neeta Sharma, *Digital Frauds, Including in UPI, Have Doubled: Home Ministry to Parliament*, *NDTV* (Mar. 26, 2025).

[18] Press Information Bureau (PIB), *Various Measures Taken by Government to Strengthen Cyber-Security in the Financial Sector*, PR ID 2112323 (Mar. 18, 2025); Neeta Sharma, *Digital Frauds, Including in UPI, Have Doubled: Home Ministry to Parliament*, *NDTV* (Mar. 26, 2025), available at https://www.ndtv.com/india-news/digital-frauds-including-in-upi-has-doubled-home-ministry-to-parliament-8018240#:~:text=Due%20to%20continuous%20monitoring%20so,36%20lakh%20complaints.

[19] Neeta Sharma, *supra note – xv*