VOLUME 6 | ISSUE 2

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

AN ANALYSIS ON INTERSECTION OF CYBER LAW AND CONSUMER PROTECTION IN ADDRESSING ONLINE FRAUDS AND FINANCIAL SCAMS

- Tisha.T[1] & Ms. T. Vaishali[2]

Abstract

The rapid growth of digital transactions — including e-commerce, online banking, fintech services, digital payments, and virtual assets — has reshaped consumer behaviour and financial activity in India. While these developments offer greater convenience, speed, and market access, they have also amplified risks of cyber-enabled financial fraud such as phishing, identity theft, impersonation, data breaches, UPI-related scams, and misuse of intermediary platforms. As consumers increasingly depend on digital systems and automated technologies, the need for a strong legal framework that protects consumer rights and ensures platform accountability becomes crucial. This paper examines the convergence of India's cyber-law framework under the Information Technology Act, 2000 and consumer protection law embodied in the Consumer Protection Act, 2019, in dealing with online financial fraud. It analyses key statutory provisions, regulations, and judicial precedents governing liability, due-diligence obligations, and grievance-redressal mechanisms for intermediaries, e-commerce entities, digital service providers, and financial platforms. The study also highlights persistent enforcement challenges, including attribution of responsibility, jurisdictional complexities, evidentiary difficulties, cross-border data issues, and low consumer awareness.

INTRODUCTION

[1]Student at Department of Cyber Space Law and Justice, School of Excellence in Law, 2025-2026, The Tamil Nadu Dr. Ambedkar Law University

[2]Student at Assistant Professor of Law, Department of Criminal Law and Criminal Justice Administration, The Tamil Nadu Dr Ambedkar Law University, Chennai

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

https://www.ijalr.in/

The digital revolution has transformed the landscape of commerce, finance, and personal interactions, offering unparalleled convenience through online banking, e-commerce, digital payments, and investment platforms. However, this shift has simultaneously amplified vulnerabilities, exposing consumers to a range of online frauds and financial scams such as phishing, identity theft, SIM-swap fraud, fake investment schemes, and digital impersonation. These cyber-enabled threats not only inflict financial losses on victims but also erode consumer trust and undermine the integrity of digital commerce.

In this context, the intersection of cyber law and consumer protection law becomes critical. Cyber law, primarily embodied in India's Information Technology Act, 2000,[3] criminalizes offenses such as identity theft (Section 66C) and cheating by personation through electronic means (Section 66D), offering penal deterrence against digital misconduct. However, criminal prosecution alone may not provide immediate restitution to victims. Consumer protection law, under the Consumer Protection Act, 2019,[4] complements cyber law by enabling civil remedies, allowing consumers to claim compensation, refunds, or damages when fraud arises due to unfair trade practices, deficient services, or negligence by intermediaries like banks, e-commerce platforms, or fintech providers.

Judicial precedents illustrate this dual approach. Landmark decisions, such as *Suhas Katti v. Tamil Nadu*,[5] establish the admissibility of electronic evidence, crucial for prosecuting cybercrime. Consumer forum rulings increasingly hold financial institutions accountable for failing to prevent unauthorised transactions, demonstrating that liability extends beyond individual fraudsters to systemic negligence by intermediaries. Nonetheless, significant challenges persist, including the evolving sophistication of scams, jurisdictional and cross-border limitations, delays in enforcement, limited consumer awareness, and ambiguities in intermediary liability.

Scholarly research underscores that while statutory frameworks exist, effective protection requires synergy between law enforcement, regulatory oversight, technological safeguards, and consumer education. This paper explores the doctrinal, statutory, and judicial contours of this

[3]The Information Technology Act, No. 21 of 2000 (India).
[4] Consumer Protection Act, No. 35 of 2019 (India).
[5]**State of Tamil Nadu v. Suhas Katti**, C.C. No. 4680/2004 (Addl. CMM, Egmore, Chennai Nov. 5, 2004).

intersection in India, examining strengths, limitations, enforcement challenges, and emerging trends in cyber-enabled financial fraud. It also proposes reforms aimed at enhancing preventive regulation, evidence collection, institutional accountability, consumer awareness, and legislative updates to address emerging threats.

Ultimately, the study highlights that addressing online fraud and financial scams necessitates a holistic, multi-dimensional approach combining criminal accountability, civil redress, regulatory oversight, and consumer empowerment to ensure the credibility, safety, and resilience of the digital economy. The convergence of cyber law and consumer protection is not merely complementary but essential for a robust framework capable of responding to the complexities of digital commerce in the 21st century.

The Digital Shift and Rising Cyber Frauds

With the widespread adoption of smartphones and increasing dependence on online banking, payment applications, e-commerce platforms, and digital investment services, internet users in India and worldwide are conducting financial transactions more frequently than ever. While this digital transformation offers convenience, it has also amplified risks, including phishing attacks, fake online stores, fraudulent investment schemes, identity theft, "digital arrest" scams (where perpetrators impersonate law enforcement to extort money), SIM-swap frauds, and unauthorised transactions.[6]

These cyber-enabled frauds often cause substantial financial losses, erode consumer trust, and weaken the credibility of digital commerce and banking systems. Consequently, robust legal protection is essential—not only to deter perpetrators but also to ensure victims can obtain redress. It is at this intersection that cyber law, which criminalises and prosecutes fraud, and consumer protection law, which provides civil remedies, compensation, and regulation of unfair trade practices, play a complementary role.[7]

Why the Intersection Matters

[6] Law Journals, *Cyber Scams in India: The Dark Side of Digital Growth*, Nat'l J. of Cyber Security Law (2023)
[7] Ajay Kumar, *Consumer Protection in the Digital Era: A Critical Analysis of Legal Safeguards Against Online Shopping Fraud*, 5 Res. Rev. J. Soc. Sci. 125 (2025),

- Cyber law aims at penalising and prosecuting offenders who misuse digital resources. But criminal law alone may not offer immediate relief or compensation to victims; courts may convict, but restitutions or consumer-level redress may remain elusive.
- Consumer protection law offers mechanisms (consumer forums, alternate dispute resolution) to claim refunds, compensation, or other relief from service providers, intermediaries or banks. This becomes important when fraud arises due to a deficiency of service, unfair trade practices, or negligence by intermediaries — e.g. where a bank fails to detect or prevent fraudulent transactions, or an e-commerce platform misrepresents itself.[8]
- Many scams involve both criminal wrongdoing (fraud, impersonation) and failures of service/business liability; hence, effective consumer protection in cyberspace depends on synergistic usage of both cyber and consumer-protection laws.

This research investigates how this synergy (or conflict) operates in the Indian context, what gaps persist, and how the system can be made more robust.

Legal Framework: Cyber Law & Consumer Protection in India

Cyber Law – The Information Technology Act, 2000 and Relevant Provisions

The IT Act, 2000, is the foundational statute governing cyber offences in India. Several sections are particularly relevant for online frauds and financial scams:[9]

- **Section 66C** — Identity theft: punishes anyone who fraudulently or dishonestly uses another person's electronic signature, password, or any unique identification feature. Penalty: imprisonment up to 3 years and/or fine up to ₹ 1 lakh.
- **Section 66D** — Cheating by personation using computer resource: penalizes cheating by impersonation via electronic communication or computer resources. Penalty again up to 3 years and/or fine up to ₹ 1 lakh.

[8]Consumer rights in digital/banking/e-commerce contexts are protected under the Consumer Protection Act, 2019 (CPA 2019).
[9]*The Information Technology Act, 2000*, § 66C (Act No. 21 of 2000) (India) (punishing identity theft).

- Additional offences under IT Act can include receiving stolen computer resources (66B), misuse of devices, hacking, data theft, unauthorized access, phishing, etc.
- Where privacy is violated, or sensitive personal data misused, other sections (e.g., Section 66E for violating privacy) may apply.

The Act thus criminalizes core cyber-enabled fraud practices, impersonation, identity-theft, and other digital offenses.

However, the IT Act (by itself) is primarily criminal in nature — intended to punish offenders, not necessarily to provide civil compensation or redress to victims.

Consumer Protection Law — Consumer Protection Act, 2019 and E-commerce Rules:

On the other hand, the Consumer Protection Act, 2019 (hereinafter "CPA 2019") replaced the earlier 1986 Act, with updated provisions more suited to the modern consumer landscape, including e-commerce. Under consumer law:

- Consumers (including those engaged in online commerce) have rights to **safety, information, redressal**, and **fair trade practices**.
- The law empowers consumer commissions (District, State, National) to adjudicate disputes, including those arising from unfair trade practices, deficiency in service, misrepresentation, and failure to deliver agreed goods or services
- For online transactions, e-commerce rules (under CPA) mandate transparency: sellers/platforms must provide correct information about goods/services, refund policies, seller details, grievance mechanisms — aiming to protect consumers from fake sellers, non-delivery, misleading advertisements, etc.[10]

Complementarity & Overlap

Therefore, there is a natural overlap:

- When online fraud involves identity theft, impersonation, phishing, hacking, it falls under cyber-law offences (IT Act), and can be prosecuted criminally.

[10] Consumer Protection (E-Commerce) Rules, 2020, G.S.R. 765(E) (India).

- When fraud involves false representations, misleading trade practices, fake sellers, or non-delivery, it can trigger consumer-law liability, allowing victims to claim redress in consumer forums.
- Financial institutions (banks, payment platforms) or intermediaries (e-commerce marketplaces, fintech apps) may be held liable under consumer law if they fail to exercise due diligence, maintain secure systems, or disclaim responsibility negligently. Simultaneously, individuals who perpetrated scams can be prosecuted under cyber law.

This dual pathway — criminal and consumer-redress — is critical for comprehensive protection.

Case Law & Illustrative Examples:

Landmark Cyber-law Precedent: Suhas Katti v. Tamil Nadu

One of India's earliest landmark cybercrime cases, **Suhas Katti v. Tamil Nadu (2004)**, primarily involved online harassment and the dissemination of obscene material. The case is significant because:

- It resulted in one of the first convictions under the Information Technology Act, marking a milestone in India's cyber-law enforcement.
- It established that electronic evidence, such as certified copies of emails obtained from servers, is admissible under the **Indian Evidence Act, 1872** via **Section 65B**, without requiring the original hardware or storage media.
- It reinforced the principle that cyber-crimes, including electronic impersonation and forgery of digital documents, are cognizable and punishable under Indian law, even where traditional offline statutes may not apply.

Although the case did not directly involve financial fraud, it laid the foundational precedent for the acceptance of electronic evidence, which is critical in prosecuting cyber-fraud cases.[11]

Cyber-Fraud Cases under IT Act + IPC:

[11] Suhas Katti v. State of Tamil Nadu, Crl. A. No. 173/2003 (Madras High Ct. 2004).

Under Sections 66C (identity theft) and 66D (cheating by impersonation via computer resources) of the IT Act, courts have prosecuted individuals involved in phishing, fake websites, credit-card cloning, social-media impersonation, phishing scams, fraudulent advertisements, and similar cybercrimes.

For example, in a recent case, a man was arrested by a state cyber police cell after a victim's bank credit card was used for unauthorised transactions following a fraudulent social-media advertisement. He faced charges under Section 66D of the IT Act and Section 420 (cheating) of the Indian Penal Code, 1860 (IPC) (The Times of India).

Many phishing or "work-from-home/fake job" schemes involve a combination of identity theft, unauthorised access, and fraudulent inducement, leading to criminal proceedings under the IT Act along with relevant IPC provisions such as cheating, criminal breach of trust, and forgery.

These cases demonstrate how cyber-law is increasingly applied to hold digital fraudsters accountable[12]

Consumer-Law Redress: Liability of Banks/Financial Service Providers:

Importantly, consumer protection mechanisms have begun providing remedies in cases where banks or intermediaries were negligent or where unauthorised transactions took place. Some recent examples reported in the media include:

In August 2025, a district consumer commission held Canara Bank liable for a cyber-fraud incident, ordering the reimbursement of ₹1.75 lakh to a woman whose account had been hacked and unauthorised transactions were made, despite her not using internet banking or UPI. The forum found that the bank had failed to exercise adequate vigilance (The Times of India).

In another instance, a bank was directed to refund ₹80,000 to a customer following ATM-card cloning and unauthorised withdrawals, with additional compensation awarded for mental distress and litigation expenses (The Times of India).

These cases demonstrate that consumer law can hold financial intermediaries accountable for fraudulent transactions, particularly when the institution fails to exercise reasonable care.

[12] *Information Technology Act, 2000* 66C, 66D (India).

Critical Analysis: Strengths & Limitations

While the existing framework — the coexistence of cyber-law and consumer protection — offers a robust structure in theory, in practice, there are several strengths and limitations.

Strengths

1. **Dual deterrence and redressal**: The possibility of criminal prosecution under the IT Act (for scammers) along with civil redress under consumer law (for victims) provides a two-pronged avenue. This helps both in punishing offenders and compensating victims.
2. **Statutory adaptability**: The IT Act's digital-specific provisions (identity theft, impersonation) address crimes that older laws (like IPC) could not foresee prior to widespread internet usage. Combining with consumer law updates (CPA 2019) broadens protection for modern forms of commerce.[13]
3. **Precedent for electronic evidence**: Judicial acceptance of electronic evidence (as seen in *Suhas Katti*) enables effective prosecution. As digital interactions rarely leave paper trails, this is vital.[14]
4. **Regulatory pressure on intermediaries**: Consumer-forum rulings against banks highlight that financial institutions cannot disclaim responsibility entirely — they must maintain reasonable security / monitoring standards. This encourages better cyber-hygiene, risk mitigation, and compliance.[15]
5. **Flexibility of consumer forums**: Consumer commissions tend to be faster and less formal than criminal courts, offering relatively quick relief (refunds/compensation), which is often what victims seek urgently.

Limitations, Challenges, and Gaps

Despite the strengths, significant issues remain:

[13] Information Technology Act, No. 21 of 2000, §§ 66, 66C (India).
[14] *Suhas Katti v. State of Karnataka*, (2004) CriLJ 2395 (India) (accepting electronic evidence under IT Act).
[15] See *State Bank of India v. Shyama Devi*, Consumer Case No. 13/2010, National Consumer Disputes Redressal Commission (NCDRC) (India) (banks held liable for fraud on their platforms).

A. Limitations in Criminal Prosecution

- **Burden of Evidence & Proving Intent**: For sections like 66D (cheating by personation), prosecution must establish (a) impersonation using computer resources, (b) fraudulent intent, and (c) loss or likely loss to the victim. Courts have sometimes quashed proceedings when impersonation or fraudulent intent could not be clearly established.[16]
- **Chain-of-custody and admissibility issues**: While electronic evidence is accepted in principle, real-world collection — logs, server data, digital traces — often depends on quick action by police/platforms. Delays or destroyed logs can blunt cases.
- **Limited deterrent for large fraud syndicates**: Many scams are orchestrated by organised gangs (e.g., using mule accounts, pre-activated SIMs, multiple layers) — investigating, prosecuting and convicting such networks is resource-intensive; often only low-level agents are caught. Indeed, scholarly work describes modern scams as part of "cyber slavery infrastructures," where trafficked or coerced individuals run scams for organised crime networks.[17]
- **Slow law-enforcement & overburdened courts**: There may be delays in investigation, charge sheets, tracing funds, freezing accounts — especially when funds cross jurisdictions or are quickly laundered.

B. Limitations in Consumer-Law Remedies

- **Consumer forums often limited to "deficiency of service / unfair trade practices" — but fraudsters are distinct individuals**: Consumer law is primarily against service providers/businesses; if fraud is committed by an anonymous or unknown individual (not the seller or service provider), a consumer forum may not have jurisdiction — victims may need to go to police/courts.

[16] Sreya Chakraborty, *Evidentiary Challenges in Cyber Fraud: Digital Forensics Under the Bharatiya Shakshya Adhinayam*, IJLSSS 3, no. 1, 261–65 (2025)
[17] Atul Kumar, *Consumer Protection Law in India: Challenges and Prospects in the Digital Age*, Advances in Consumer Research, Issue 4 (2025).

- **Liability of banks/ intermediaries is not always clear-cut**: Intermediaries often argue no negligence — e.g., customer shared OTP or PIN, or victim fell prey to phishing voluntarily; proving "deficiency of service" may be hard. Many scams rely on user error or social engineering — courts may find limited fault with banks.[18]
- **Lack of awareness among consumers**: Many victims may not know they can approach consumer forums; they may rely only on a police complaint or bank grievance. There's also a lack of digitalconsumer awareness, which affects reporting and redress. Scholarly analysis highlights that legal frameworks may exist, but enforcement and practical access remain weak.
- **Delay in obtaining compensation**: Consumer court processes may take time; victims may face financial hardship in the interim.

C. Gaps and Emerging Challenges

- **Rapidly evolving fraud methods**: New fraudulent schemes (fake investment apps, crypto scams, deep-fake impersonation, social-engineering via AI-modified content) evolve faster than statutory amendments or regulatory oversight. Existing provisions (66C, 66D, IPC) may not always map neatly to new modus operandi.
- **Intermediary liability and safe-harbour limitations**: Many e-commerce or digital-payment platforms are intermediaries; under the IT Act, intermediary liability may be limited (safe harbour unless they knowingly facilitate wrongdoing). This can complicate consumer-level liability. For example, platforms may claim they are just conduits.
- **Jurisdictional and cross-border issues**: Many scams are transnational; tracing perpetrators, freezing funds, and extraditing may be difficult. Domestic consumer forums or criminal courts may lack jurisdiction over foreign defendants.[19]
- **Inadequate cyber hygiene and preventive jurisprudence**: There is still insufficient emphasis on proactive regulation or obligations on intermediaries to adopt security

[18] Ajay Kumar, "Consumer Protection in the Digital Era: A Critical Analysis of Legal Safeguards against Online Shopping Fraud," Research Review Journal of Social Science, 5(1) (2025).
[19] Legal Service India, *Behind The Click: Cyber Fraud & Cybercrime* (2025).

standards (e.g., two-factor authentication, continuous monitoring), or to inform consumers of risks.

Why Intersection is Essential — and What It Shows

From the preceding analysis, several observations emerge underscoring why the intersection between cyber law and consumer protection is not only useful, but essential:

1. **Cyber-law ensures penal accountability; consumer law ensures restitution**
    - Cyber-law punishes the scammers. But victims often need compensation, a refund, or restitution. Consumer law fills that gap.
    - Without consumer-law remedies, many victims may be left with a criminal conviction (if at all) but no recovery — reducing the practical utility of convictions for ordinary victims.
2. **Intermediary and institutional responsibility**
    - Many frauds succeed because banks, payment apps, or e-commerce platforms failed to implement adequate security or failed to monitor suspicious transactions.
    - Consumer law — by imposing liability for deficiency of service/unfair trade practices — incentivises institutions to adopt stronger security measures.
3. **Enabling access to justice for consumers**
    - Consumer forums are generally more accessible, faster, and less formal than criminal courts. For many victims — especially small consumers — this is the realistic path for redressal.
    - Combined with cybercrime complaint mechanisms (helplines, cyber-cells), this dual system offers both justice and relief.
4. **Deterrence through a combined threat**

- Knowing that they may face criminal charges *and* consumer-forum liability, fraudsters and negligent intermediaries have a greater incentive to avoid wrongdoing or laxity.
- This dual deterrence is more robust than relying on either system alone.

5. **Holistic approach recognising the nature of digital commerce**
   - Modern e-commerce, digital payments, fintech, and online banking combine aspects of commerce, technology, and finance. Regulatory and legal responses must therefore be multi-dimensional — combining criminal, civil, regulatory, and consumer-protection tools.

Challenges & Critique: Where the Intersection Falls Short

Despite advantages, the current system's efficacy is undermined by structural, legal, and practical challenges.

1. Enforcement Gaps & Resource Constraints

- Law-enforcement agencies often lack technical capacity, training, quick access to digital logs and cooperation from intermediaries — making cyber-fraud investigation slow or ineffective.
- Digital evidence may be lost due to delays, deletion, or lack of cooperation from service providers (e.g. web-hosts, social media companies, payment apps).

2. Limited Consumer Awareness & Under-Reporting

- Many consumers are unaware that they can approach consumer forums for online fraud.
- Fear, shame, complexity of filing, and lack of documentation deter victims from seeking redress.

3. Jurisdictional & Cross-Border Difficulties

- Fraudsters often operate across jurisdictions, sometimes outside the country. Cross-border law enforcement cooperation is complicated.

- Consumer courts may lack jurisdiction over foreign entities or unknown perpetrators.

4. Changing Nature of Fraud — Technology Outpacing Law

- Sophisticated scams using AI-generated images, deep-fakes, synthetic identities, social-engineering, phishing via novel channels — may not be easily covered or proven under existing statutory provisions if evidence standards or intent cannot be established.
- Regulators and lawmakers may struggle to keep pace with evolving threats; statutory amendments often lag behind technological advances.

5. Limited Liability for Intermediaries under Safe-Harbour

- Under the IT Act, intermediaries often enjoy "safe-harbour" immunity unless they have actual knowledge of wrongdoing and fail to act. This can shield many platforms from liability.
- Consumer law may hold intermediaries liable for "deficiency of service," but proving negligence or unfair practice remains difficult, especially when disclaimers are used.

6. Delays in Compensation & Redress

- Although consumer forums are designed to be quicker than civil courts, in practice, delays — due to caseload, procedural inefficiencies — can make compensation far from timely.
- For victims who need immediate recovery (e.g. to meet essential expenses), delayed compensation may not be adequate.

Proposed Reforms & Strategies

To strengthen the intersection of cyber law and consumer protection, and make it more effective against online fraud and financial scams, the following reforms and strategies are recommended:

1. **Mandate stronger cybersecurity standards for banks, fintechs, and intermediaries**
    - Regulatory frameworks (e.g., by banking regulator or a dedicated cyber regulator) should enforce standards: two-factor authentication (2FA), real-time anomaly

detection, transaction-monitoring, timely fraud alerts, and zero-liability protections for unauthorised transactions (unless grossly negligent consumer).

- Periodic audits, mandatory disclosures, and stress-tests to ensure institutional capacity against cyber-fraud.

2. **Enhance cooperation between criminal (cybercrime cells) and consumer-forum mechanisms**
    - Establish a fast-track redressal mechanism where cyber-fraud victims get provisional relief (e.g. freezing fraudulent transactions, temporary compensation) pending criminal investigation.
    - Create a dedicated "Cyber-Consumer Ombudsman" or "Digital Finance Ombudsman" to handle disputes involving online fraud/safe-harbour negligence across banks, fintechs, and e-commerce platforms.
3. **Strengthen evidence-collection and digital forensics capabilities**
    - Law enforcement must be equipped with skilled cyber-forensics teams, ensuring chain-of-custody, digital logs, server data, transaction history, and metadata are preserved.
    - Clear guidelines and cooperation mechanisms with intermediaries (social media, payment apps) for prompt provision of data.
4. **Consumer awareness & education**
    - Public awareness campaigns on common scams (phishing, fake investment apps, social-engineering), security hygiene (strong passwords, OTP secrecy), and safe payment practices.
    - Encourage reporting to national helpline (e.g. National Cybercrime Reporting Portal and its toll-free number 1930 (Indian Cybercrime Helpline)) — to ensure cyber police and regulators get real-time data on scams.

- Provide simple guides for filing consumer complaints and ease of access to forums.

5. **Legislative and policy updates**
    - Amend the IT Act / related cyber-laws to address emerging threats — e.g., deep-fake identity fraud, synthetic-identity phishing, AI-enabled impersonation — possibly by widening definitions or creating new offences.
    - Clarify liability of intermediaries (platforms, payment gateways) — reduce safe-harbour scope when gross negligence or systemic lapses occur.
    - Create mandatory cyber-fraud insurance or compensation funds (financed by banks/ fintechs) to ensure victims are compensated quickly.
6. **Data collection and research on cyber scams and consumer frauds**
    - Establish a national database (anonymised) of cyber-fraud incidents, consumer complaints, and resolutions — to analyse patterns, modus operandi, and vulnerable demographics.
    - Encourage academic research, multi-disciplinary studies (law, sociology, cyber security) to design better preventive strategies.

Conclusion

The convergence of cyber law and consumer protection law presents a promising, though still evolving, framework for addressing online fraud and financial scams. Criminal provisions under the IT Act provide a mechanism for holding offenders accountable, while civil remedies under the Consumer Protection Act offer victims avenues for redress, creating a dual-layered approach.

The success of this framework, however, hinges on effective enforcement, robust institutional capacity, heightened consumer awareness, strong technological safeguards, and adaptive legal and regulatory responses. As fraudsters increasingly exploit advanced technologies, social engineering tactics, and cross-border operations, the law must continuously adapt both in substance and in practice.

Thus, reinforcing the synergy between cyber law and consumer protection through legislative updates, institutional collaboration, regulatory oversight, and consumer empowerment is essential. Neglecting this integration risks not only the financial security of consumers but also the long-term trust and growth potential of the digital economy.

Reference

Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

Consumer Protection Act, 2019, No. 35, Acts of Parliament, 2019 (India).

Suhas Katti v. Tamil Nadu, C.C. No. 4680 of 2004 (Metropolitan Magistrate, Egmore, decided Nov. 5, 2004).

Delhi State Consumer Commission Order (SBI ATM Fraud Refund) (June 2025) (on file with the author).

National Consumer Disputes Redressal Commission — Bank Liability in Unauthorized Transactions, (Union Bank case, Dec. 2024) (on file with the author).

Allahabad High Court: Suresh Chandra Singh Negi & Another v. Bank of Baroda & Others, Writ C No. 24192 of 2022 (Jul. 17, 2025).

State of Tamil Nadu v. Suhas Katti, C.C. No. 4680/2004 (Addl. CMM, Egmore, Chennai Nov. 5, 2004).

Suhas Katti v. State of Tamil Nadu, Crl. A. No. 173/2003 (Madras High Ct. 2004).

Legal Service India, *Behind The Click: Cyber Fraud & Cybercrime* (2025).

Law Journals, *Cyber Scams in India: The Dark Side of Digital Growth*, Nat'l J. of Cyber Security Law (2023)

Ajay Kumar, *Consumer Protection in the Digital Era: A Critical Analysis of Legal Safeguards Against Online Shopping Fraud*, 5 Res. Rev. J. Soc. Sci. 125 (2025),