Page 487 - 504 **DOI:** *https://doi.org/10.63108/IJLMH.12868*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 5

2026

Online Financial Fraud in India: A Legal and Criminological Study

POLISETTI SATYADEVI*

ABSTRACT

India's rapid transition to digital banking, mobile wallets, payment cards and the Unified Payments Interface has expanded financial inclusion while creating new opportunities for online financial fraud. This paper examines the principal forms of online financial fraud in India and evaluates whether the existing criminal, procedural, evidentiary, regulatory and consumer-protection framework can deliver timely prevention, investigation and victim redress. It adopts a doctrinal and qualitative analytical method, supported by criminological perspectives including routine activity, rational choice, differential association and victimology. The analysis covers phishing, vishing, smishing, UPI fraud, identity theft, account takeover, investment and loan-app scams, digital-arrest schemes and mule-account networks. It finds that India has a broad but fragmented framework. Its effectiveness is reduced by delayed reporting, interstate jurisdictional barriers, uneven electronic-evidence practices, weak coordination among institutions and uncertainty concerning fraudulently induced authorised payments. The paper argues for an authorised push-payment framework, rapid fund interception through 1930 and the National Cyber Crime Reporting Portal, continuous mule-account monitoring, proportionate account-freezing procedures, stronger platform and telecom cooperation, specialised investigation, and meaningful restitution. Effective control requires a coordinated model that treats fraud prevention, digital evidence, institutional accountability and victim protection as parts of one legal system.

Keywords: *Online Financial Fraud, Cybercrime, UPI Fraud, Social Engineering, Digital Payments, Authorised Push-Payment Fraud, Mule Accounts, Victim Protection*

I. INTRODUCTION AND RESEARCH FRAMEWORK

A. Introduction

The expansion of internet connectivity, smartphones, digital banking and real-time payment systems has fundamentally transformed financial transactions in India. Banking services that once required physical presence, written documentation and considerable processing time can now be accessed within seconds through mobile applications and online platforms. The Unified

* Author is a Student at Aurora Deemed to be University, Bhongir, Telangana, India. ORCID: https://orcid.org/0009-0001-4127-6914

 [ISSN 2581-5369]

Payments Interface, internet banking, mobile wallets, payment cards and other electronic systems have contributed to financial inclusion, commercial efficiency and the development of a less-cash economy. During 2024–25, digital transactions accounted for 99.9 per cent of the total volume of non-cash retail payments in India, demonstrating the central position occupied by electronic payments in the contemporary financial system.[1]

B. Meaning and Concept of Online Financial Fraud

Fraud generally involves intentional deception employed to obtain an unlawful financial benefit or cause wrongful loss to another person. Online financial fraud may be understood as the dishonest use of the internet, a computer resource, communication device, digital-payment system or electronic platform to deceive a person or institution and unlawfully obtain money, financial information, banking credentials or another economic advantage.

C. Background and Evolution of the Problem

The early forms of internet-enabled financial fraud in India were largely associated with deceptive emails, lottery messages, advance-fee scams and misuse of payment cards. The growth of internet banking subsequently led to credential theft, phishing websites, malware attacks and unauthorised fund transfers. The widespread adoption of smartphones and instant-payment applications further changed the nature and scale of the problem. Fraudsters began exploiting QR codes, remote-access applications, screen-sharing software, fraudulent customer-care numbers and deceptive UPI payment requests.

D. Statement of the Problem

India has developed one of the largest digital-payment ecosystems in the world, but the legal and enforcement response to online financial fraud remains divided among multiple statutes, regulators and institutions. The Information Technology Act addresses identity theft and computer-related personation, while the Bharatiya Nyaya Sanhita governs cheating, forgery, organised crime and related conduct. Procedural questions are governed by the Bharatiya Nagarik Suraksha Sanhita, 2023, and the proof of digital material is governed by the Bharatiya Sakshya Adhiniyam, 2023. Banking liability, payment-system supervision and fraud reporting are additionally shaped by RBI directions.

[1] RESERVE BANK OF INDIA, *Annual Report 2024–25*, ¶ IX.5 (2025), https://rbidocs.rbi.org.in/rdocs/AnnualReport/PDFs/09PAYMENT29052025564CFE8E29164796AC1B2016508B51A6.PDF.

 [ISSN 2581-5369]

E. Literature Review

David S. Wall explains that the internet changes the nature of crime by permitting offending to occur across physical boundaries and at a scale not ordinarily possible in conventional environments. His classification of cybercrime demonstrates that technology may transform established offences rather than merely create entirely new ones.[2] This approach is relevant to online financial fraud because deception and cheating are traditional offences whose reach, speed and anonymity have been substantially altered by digital networks.

F. Research Gap

Much of the available Indian literature either provides a general discussion of cybercrime or focuses upon particular techniques such as phishing, card fraud or UPI scams. Several studies were also completed before the Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita and Bharatiya Sakshya Adhiniyam came into operation on 1 July 2024.[3] Consequently, they do not adequately examine the interaction between the new criminal-law framework and the continuing provisions of the Information Technology Act.

G. Research Questions

What are the principal forms and methods of online financial fraud prevalent in India?

H. Hypothesis

The existing Indian legal framework contains several substantive, procedural and regulatory provisions for addressing online financial fraud. Its practical effectiveness is nevertheless reduced by fragmented regulation, delayed reporting, jurisdictional difficulties, deficiencies in digital investigation, inadequate coordination among institutions, low public awareness and the rapidly changing methods adopted by offenders. A coordinated legal, criminological, technological and victim-oriented response is therefore necessary to effectively prevent and control online financial fraud in India.

I. Research Objectives

The study seeks to examine the nature, evolution and principal forms of online financial fraud in India; analyse the criminological causes, offender motivations and opportunity structures associated with such fraud; identify the psychological, social and technological factors that

[2] DAVID S. WALL, CYBERCRIME: THE TRANSFORMATION OF CRIME IN THE INFORMATION AGE 45–48 (Polity Press 2007).

[3] MINISTRY OF HOME AFFAIRS, Notification Nos. S.O. 848(E), S.O. 849(E) and S.O. 850(E) (Feb. 23, 2024), *Gazette of India*, Extraordinary, pt. II, sec. 3(ii) (appointing 1 July 2024 as the date of commencement of the Bharatiya Nagarik Suraksha Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023 and the Bharatiya Nyaya Sanhita, 2023 respectively, the last excepting section 106(2)).

 [ISSN 2581-5369]

increase victim vulnerability; critically evaluate the substantive, procedural, evidentiary and regulatory framework; study the institutional response of law-enforcement agencies, banks, payment intermediaries, RBI and I4C; examine difficulties relating to jurisdiction, attribution, electronic evidence and recovery of money; and propose reforms for prevention, prosecution, financial recovery and victim protection.

J. Research Methodology

The research adopts a doctrinal, analytical and qualitative methodology. Primary sources include the Constitution of India, Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023, Bharatiya Sakshya Adhiniyam, 2023, Information Technology Act, 2000, Prevention of Money Laundering Act, 2002, Payment and Settlement Systems Act, 2007, Consumer Protection Act, 2019, judicial decisions and regulatory directions issued by the RBI.

K. Scope and Limitations

The study primarily covers online financial fraud affecting individual users, banking customers, consumers and digital-payment participants in India. It includes phishing, smishing, vishing, identity theft, UPI fraud, payment-card fraud, account takeover, digital-arrest scams, online investment fraud, loan-app fraud, e-commerce deception, impersonation and mule-account operations.

II. Nature, Forms and Criminological Dimensions of Online Financial Fraud

A. Introduction

Online financial fraud is a rapidly evolving form of economic crime in which digital communication, electronic payment systems and human deception converge. Unlike conventional financial offences, it can be committed remotely, at great speed and against a large number of persons without physical contact between the offender and victim. The offence may involve unauthorised access to financial information, but many contemporary frauds depend primarily upon manipulating the victim into disclosing confidential information or authorising a transaction.

B. Evolution of Online Financial Fraud in India

The earliest internet-enabled financial frauds in India largely involved lottery emails, false inheritance claims, advance-fee schemes and deceptive offers from persons pretending to be foreign officials or business representatives. As internet banking expanded, offenders began creating imitation banking websites and fraudulent emails to obtain usernames, passwords and

 [ISSN 2581-5369]

card information. The increased use of mobile phones subsequently produced vishing, smishing, SIM-related fraud and malicious applications.

C. Phishing, Smishing and Vishing

Phishing involves the use of fraudulent electronic communications designed to obtain passwords, card details, one-time passwords or other confidential information. A phishing message commonly imitates a bank, government department, online marketplace or service provider and directs the recipient to a false website. The imitation page records the information entered by the victim and transmits it to the offender.

D. UPI and Digital-Payment Fraud

UPI fraud has become especially significant because payments are executed almost instantaneously. Fraudsters may send a deceptive collect request while falsely claiming that the victim must enter a UPI PIN to receive money. In other cases, they persuade the victim to scan a QR code, approve a mandate or share a screen while accessing a payment application. The victim may believe that these steps will produce a refund or credit, although they actually authorise a debit.

E. Identity Theft and Account Takeover

Identity theft involves the fraudulent use of another person's password, electronic signature, identification number or other unique identifying information. Such information may be obtained through phishing, data breaches, malware, stolen devices or deceptive KYC procedures. The offender may then open or operate bank accounts, access digital wallets, obtain credit or impersonate the victim before financial institutions.

F. Digital-Arrest and Impersonation Scams

Digital-arrest fraud is based upon fear and abuse of perceived governmental authority. Fraudsters impersonate police officers, investigative agencies, customs authorities, courts or telecommunications officials. The victim is falsely informed that a mobile number, bank account, parcel or identity document is connected with money laundering, narcotics or another serious offence. The victim may be ordered to remain continuously visible on a video call, avoid communication with family members and transfer money for supposed verification.

G. Mule Accounts and Organised Fraud Networks

A mule account is a bank or payment account used to receive, transfer or withdraw proceeds of crime. Some account holders knowingly assist offenders for commission, while others are recruited through false employment, loan or investment schemes. The proceeds may be divided

 [ISSN 2581-5369]

among several accounts and transferred repeatedly to obscure the financial trail. Funds may ultimately be withdrawn in cash, converted into digital assets or remitted beyond India.

H. Social Engineering and Psychological Manipulation

Social engineering is the deliberate manipulation of human emotion and decision-making to obtain information, access or money. Fraudsters exploit authority, urgency, fear, greed, sympathy, curiosity and scarcity. A victim threatened with arrest may comply because fear prevents calm reflection. A victim offered unusually high investment returns may respond to optimism and fear of missing an opportunity. A person contacted by someone appearing to be a relative may act out of concern and trust.

I. Routine Activity Theory

Routine activity theory explains crime through the convergence of a motivated offender, a suitable target and the absence of capable guardianship.[4] In the online environment, physical proximity is unnecessary. Routine activities such as online shopping, digital banking, social-media use and responding to messages expose individuals to remote offenders.

J. Rational Choice and Opportunity Perspectives

Rational choice theory views offending as a decision influenced by perceived reward, effort and risk. Online financial fraud can offer high returns with limited physical danger. False identities, disposable telephone numbers, remote communication and mule accounts reduce the offender's perceived probability of detection. Offenders may consequently regard online fraud as more profitable and less risky than conventional property crime.

K. Differential Association, Neutralisation and Organisational Learning

Differential association theory proposes that criminal conduct is learned through interaction with others, including techniques of offending and attitudes that justify law-breaking.[5] Online fraud networks provide environments in which participants learn scripts, impersonation methods, fund-transfer techniques and ways of avoiding detection. Digital groups may distribute stolen information, malicious software and operational instructions.

L. Victimology and Patterns of Vulnerability

Online financial fraud can affect persons of every age, educational background and economic position. Vulnerability is situational rather than inherent. Elderly persons may face difficulty

[4] Lawrence E. Cohen & Marcus Felson, *Social Change and Crime Rate Trends: A Routine Activity Approach*, 44 AM. SOC. REV. 588, 589 (1979), https://doi.org/10.2307/2094589.
[5] EDWIN H. SUTHERLAND & DONALD R. CRESSEY, CRIMINOLOGY 75–77 (10th ed., J.B. Lippincott Co. 1978).

 [ISSN 2581-5369]

recognising new technological methods, while younger users may be exposed through frequent engagement with online shopping, gaming, investment and social media. Persons seeking employment, credit or high returns may be targeted through offers tailored to their immediate needs.

III. Legal Framework Governing Online Financial Fraud in India

A. Introduction

India does not possess a single consolidated statute exclusively governing online financial fraud. The applicable framework is distributed across general criminal law, information-technology law, criminal procedure, electronic-evidence law, banking regulation, anti-money-laundering legislation, consumer protection and data-protection law. The nature of the transaction, method of deception, identity of the offender, manner in which the proceeds are transferred and the involvement of intermediaries determine which provisions apply.

B. Constitutional Dimensions

The Constitution does not expressly create a fundamental right to cybersecurity or protection from online financial fraud. Nevertheless, Articles 14 and 21 provide an important normative foundation for fair administration, protection of personal liberty and informational privacy. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court recognised privacy as a fundamental right and acknowledged informational privacy as an essential component of individual liberty.[6] Financial information, banking credentials and transaction histories are closely connected with personal autonomy and privacy.

C. Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023 replaced the Indian Penal Code and came into force on 1 July 2024. Section 318 defines cheating as deception that fraudulently or dishonestly induces a person to deliver property, consent to the retention of property, or do or omit an act likely to cause harm. Where cheating dishonestly induces delivery of property or the making, alteration or destruction of a valuable security, the punishment may extend to seven years and fine.[7] This provision applies to fraudulent investment schemes, fake shopping platforms, digital-arrest scams and other cases in which deception causes transfer of money.

[6] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1, 264–65 (India).
[7] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 318, India Code (2023).

 [ISSN 2581-5369]

D. Information Technology Act, 2000

The Information Technology Act remains the principal special legislation governing computer-related offences. Section 43 creates civil liability for unauthorised access, downloading or extraction of data, introduction of a contaminant, disruption of a computer resource and related conduct. When acts described in section 43 are committed dishonestly or fraudulently, section 66 imposes criminal punishment. These provisions may apply to account compromise, malware deployment and unauthorised extraction of banking data.

E. Intermediary Liability and Due Diligence

Banks, social-media platforms, search engines, communication services and online marketplaces may possess information necessary to identify offenders or remove fraudulent content. Section 79 of the Information Technology Act grants conditional protection to intermediaries for third-party information where their role is limited and they observe statutory due diligence.

F. Bharatiya Nagarik Suraksha Sanhita, 2023

The Bharatiya Nagarik Suraksha Sanhita governs registration, investigation, search, seizure, arrest and prosecution. Section 173 permits information relating to a cognizable offence to be given orally or through electronic communication, irrespective of the area where the offence was committed. Information submitted electronically must be signed within three days.[8] This provision strengthens the legal basis for a Zero FIR and is important in online fraud cases where the victim, bank account, communication device and offender may be located in different jurisdictions.

G. Bharatiya Sakshya Adhiniyam, 2023

Online financial-fraud prosecutions depend substantially upon electronic evidence. Relevant material may include bank statements, transaction logs, call records, emails, messages, IP information, CCTV recordings, device contents and platform data. Section 61 of the Bharatiya Sakshya Adhiniyam provides that an electronic or digital record shall not be denied admissibility merely because it is electronic, subject to the requirements of section 63.[9]

H. Prevention of Money Laundering Act, 2002

Online fraud rarely concludes with the first transfer of money. The proceeds may pass through mule accounts, shell entities, prepaid instruments or virtual assets before withdrawal or

[8] Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, § 173, INDIA CODE (2023).
[9] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 61, 63, INDIA CODE (2023).

 [ISSN 2581-5369]

conversion. The Prevention of Money Laundering Act, 2002 applies where property constitutes the proceeds of a scheduled offence and a person becomes involved in its concealment, possession, acquisition, use or projection as untainted property.[10]

I. Payment and Settlement Systems Act, 2007

The Payment and Settlement Systems Act, 2007 authorises the RBI to regulate and supervise payment systems in India. No person may operate a payment system without authorisation from the RBI, subject to statutory exceptions. The RBI may prescribe standards, call for information, inspect systems and issue directions in the public interest.[11]

J. Consumer Protection Act, 2019

Banking and financial services fall within the broad definition of "service" under the Consumer Protection Act, 2019. A customer may seek relief where loss results from deficiency in service, failure to maintain reasonable security, unjustified refusal to address a complaint or breach of a legally enforceable obligation.[12] Consumer liability should nevertheless be determined according to the evidence and applicable RBI directions rather than on the mere occurrence of fraud.

K. Digital Personal Data Protection Act, 2023

Online financial fraud is frequently facilitated by misuse of names, telephone numbers, identity documents and financial information. The Digital Personal Data Protection Act, 2023 establishes duties concerning lawful processing, security safeguards and personal-data-breach notification.[13] The Digital Personal Data Protection Rules, 2025 provide for phased commencement, meaning that significant substantive obligations become operational according to the timelines specified in the notification.[14]

L. RBI Framework on Customer Liability

The RBI's 2017 circular on unauthorised electronic banking transactions is central to customer protection. A customer has zero liability where the unauthorised transaction results from contributory fraud, negligence or deficiency on the part of the bank. Zero liability may also arise in a third-party breach where the deficiency lies neither with the bank nor customer

[10] Prevention of Money Laundering Act, No. 15 of 2003, §§ 2(1)(u), 3–5, INDIA CODE (2002).
[11] Payment and Settlement Systems Act, No. 51 of 2007, §§ 4, 10, 12–18, INDIA CODE (2007).
[12] Consumer Protection Act, No. 35 of 2019, §§ 2(11), 2(42), 35, INDIA CODE (2019).
[13] Digital Personal Data Protection Act, No. 22 of 2023, §§ 4–8, INDIA CODE (2023).
[14] Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), r. 1(2)–(4), *Gazette of India*, Extraordinary, pt. II, sec. 3(i) (Nov. 13, 2025).

 [ISSN 2581-5369]

and the customer reports the transaction within three working days of receiving communication from the bank.[15]

M. Fraud Risk Management and KYC Requirements

The RBI's Fraud Risk Management Directions require regulated entities to establish board-approved policies for prevention, early detection, reporting, investigation and recovery. Banks must report relevant fraud incidents to the Central Fraud Registry and payment-related suspected or attempted fraudulent transactions to the Central Payments Fraud Information Registry.[16]

N. Deficiencies in the Existing Framework

The legal framework criminalises most major forms of online financial fraud, but fragmentation creates uncertainty and inconsistent application. Overlap between the BNS and Information Technology Act may produce incorrect charging, while the distinction between unauthorised transactions and fraudulently authorised payments affects reimbursement. Extraterritorial provisions are difficult to enforce without timely international cooperation.

IV. Investigation, Evidence and Institutional Response

A. Introduction

The effectiveness of laws governing online financial fraud depends upon the ability of institutions to receive complaints, preserve electronic evidence, trace financial transactions, identify offenders and recover proceeds before they are dissipated. These offences create distinctive investigative difficulties because communication may originate from one State, the victim may reside in another, the recipient bank account may be maintained elsewhere and the principal offender may operate outside India.

B. Reporting and Registration of Complaints

A victim of online financial fraud may report the incident to the local police, cybercrime police station, National Cyber Crime Reporting Portal or helpline number 1930. The most effective response requires simultaneous reporting to the bank or payment service provider because the institution may be able to block the relevant payment instrument or alert the beneficiary bank.

---

[15] Reserve Bank of India, *Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions*, RBI/2017–18/15, DBR.No.Leg.BC.78/09.07.005/2017–18, ¶¶ 6–10 (July 6, 2017), https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11040.

[16] Reserve Bank of India, *Master Directions on Fraud Risk Management in Commercial Banks (Including Regional Rural Banks) and All India Financial Institutions*, RBI/DOS/2024–25/118, DOS.CO.FMG.SEC.No.5/23.04.001/2024–25, ¶¶ 6.2–6.3 (July 15, 2024), https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12702.

 [ISSN 2581-5369]

C. The Golden-Hour Principle and Fund Interception

The initial period following a fraudulent transaction is commonly described as the "golden hour." Although it is not a rigid statutory duration, it signifies the limited period during which the proceeds may remain traceable within the formal banking system. The victim should immediately contact the bank and 1930, preserve the transaction reference number and provide details of the fraudulent communication.

D. Territorial Jurisdiction and Interstate Investigation

Online financial fraud rarely conforms to traditional territorial boundaries. A fraudulent call may originate abroad, use an Indian telephone number, direct payment to an account opened in another State and transfer the proceeds through several additional jurisdictions. Section 202 of the BNSS recognises jurisdiction where cheating is committed through electronic communication and permits inquiry or trial where the communication was sent or received or where the property was delivered or received.[17]

E. Identification of the Offender

The apparent identity displayed during an online fraud may have little connection with the actual offender. Fraudsters use spoofed telephone numbers, false subscriber records, compromised accounts, virtual private networks, remote devices and fabricated identity documents. Identification must therefore be based upon the combined examination of subscriber information, IP logs, device identifiers, account-opening records, transaction data, CCTV footage and withdrawal patterns.

F. Search, Seizure and Digital Forensics

Investigators may need to search premises, seize mobile phones and computers, collect storage media and obtain relevant electronic records. The BNSS requires prescribed search-and-seizure procedures and promotes audio-video recording of such operations. A lawful and transparent seizure protects both evidentiary integrity and the rights of the person from whom the device is obtained.

G. Production and Preservation of Electronic Records

Banks, telecom operators, social-media companies, email providers and payment intermediaries commonly hold records essential to the investigation. Section 94 of the BNSS authorises a court or police officer to require production of documents, electronic communications and

[17] Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, § 202, INDIA CODE (2023).

 [ISSN 2581-5369]

communication devices likely to contain digital evidence.[18] Investigators may also issue preservation requests so that volatile logs are not deleted under ordinary retention policies.

H. Admissibility and Proof of Electronic Evidence

Electronic evidence is central to online financial-fraud trials, but its usefulness depends upon admissibility and authenticity. The Bharatiya Sakshya Adhiniyam, 2023 places electronic and digital records on a legally recognised footing. Section 63 prescribes conditions for admitting computer output and requires the statutory certificate where applicable.

I. Seizure and Freezing of Bank Accounts

Freezing a recipient or mule account is one of the most important measures in financial-fraud investigation. In *State of Maharashtra v. Tapas D. Neogy*, the Supreme Court held that a bank account falls within the meaning of "property" capable of seizure under section 102 of the Code of Criminal Procedure where it has a direct link with the alleged offence.[19] The principle continues to influence account-freezing powers under the corresponding BNSS framework.

J. Role of Banks and Payment Intermediaries

Banks and payment intermediaries occupy a dual position. They possess customer and transaction information essential to investigation, and they are also expected to maintain preventive systems. Their responsibilities include KYC verification, transaction monitoring, reporting of suspicious activity, preservation of records, maintenance of grievance channels and cooperation with lawful requests.

K. Intermediary Cooperation and Safe Harbour

Online platforms may host fraudulent advertisements, false investment groups, impersonating accounts and fake customer-care details. Section 79 of the Information Technology Act grants intermediaries conditional safe-harbour protection for third-party information where they comply with statutory requirements and do not actively participate in the illegality.

L. Special Law and Overlapping Offences

An online act may appear to constitute both cheating under the BNS and an offence under the Information Technology Act. In *Sharat Babu Digumarti v. Government of NCT of Delhi*, the Supreme Court emphasised the special character of the Information Technology Act in relation to offences specifically governed by it.[20] The case concerned electronic publication rather than

[18] Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, § 94, INDIA CODE (2023).
[19] *State of Maharashtra v. Tapas D. Neogy*, (1999) 7 S.C.C. 685, 694 (India).
[20] *Sharat Babu Digumarti v. Government of NCT of Delhi*, (2017) 2 S.C.C. 18, 27–31 (India).

 [ISSN 2581-5369]

financial fraud, but its reasoning is relevant when selecting charges under overlapping general and special laws.

M. International and Cross-Border Cooperation

Where offenders, platforms or servers are located abroad, domestic investigative powers may be insufficient. Investigators may seek information through mutual legal assistance treaties, letters rogatory, international police cooperation and requests made under applicable bilateral arrangements. Section 75 of the Information Technology Act provides extraterritorial application where the conduct involves a computer resource located in India, but statutory jurisdiction does not guarantee practical access to foreign evidence.

N. Judicial Approach to Technology and Investigation

In *Tomaso Bruno v. State of Uttar Pradesh*, the Supreme Court recognised the significance of scientific and electronic evidence and observed that adverse inference may arise where material evidence such as CCTV footage under the control of a party is unjustifiably withheld.[21] The decision underscores the need to collect the best available digital evidence rather than rely exclusively upon oral testimony.

O. Enforcement Gaps and Institutional Constraints

The principal enforcement problems include delayed reporting, shortage of trained personnel, fragmented jurisdiction, incomplete electronic-evidence certification and slow cooperation from institutions. Local police stations may possess limited capacity to trace layered digital transactions or examine complex devices. Rapid changes in fraud methods require continuous training rather than occasional instruction.

V. Prevention, Victim Protection and Institutional Response

A. Introduction

Online financial fraud cannot be controlled through prosecution alone. By the time an offender is identified and brought before a court, the victim's money may have passed through several accounts or left the formal financial system. Prevention must therefore operate before, during and immediately after a fraudulent transaction. It requires secure payment architecture, effective customer verification, real-time transaction monitoring, rapid reporting, institutional coordination and informed users.

[21] *Tomaso Bruno v. State of Uttar Pradesh*, (2015) 7 S.C.C. 178, 193–95 (India).

 [ISSN 2581-5369]

B. Preventive and Supervisory Role of the RBI

The Reserve Bank of India occupies a central position in the prevention of online financial fraud because it regulates banks and payment systems. Its Fraud Risk Management Directions require regulated entities to establish board-approved policies covering prevention, early detection, investigation, staff accountability, reporting and recovery.[22] Fraud management should not be confined to a department responding after loss; it must be integrated into institutional governance, product design and customer protection.

C. Customer Liability and Unauthorised Transactions

The RBI's customer-protection framework allocates liability according to the source of the failure and the speed of reporting. A customer ordinarily bears no loss where an unauthorised transaction results from fraud, negligence or deficiency on the part of the bank. Zero or limited liability may also arise in a third-party breach where the customer reports within the prescribed period. Banks must provide twenty-four-hour reporting channels and communicate transaction alerts.[23]

D. Need for an Authorised Push-Payment Fraud Framework

India should consider a separate regulatory framework for fraudulently induced authorised payments. The framework should not impose automatic liability upon banks in every case, because institutions cannot prevent all deceptive communications occurring outside their systems. It should instead allocate responsibility according to the conduct of the sending bank, receiving institution, customer and relevant platform.

E. Reporting through 1930 and NCRP

Victim protection begins with a simple and immediate reporting system. The 1930 helpline enables persons to report financial cyber fraud, while the National Cyber Crime Reporting Portal permits completion and tracking of the complaint. A person who reports through 1930 must subsequently complete the formal complaint on the portal within the prescribed period communicated through the system.[24]

F. Recommendations for Reform

India should adopt a comprehensive national framework distinguishing unauthorised transactions from fraudulently induced authorised payments. Banks and receiving institutions

[22] RESERVE BANK OF INDIA, *Master Directions on Fraud Risk Management*, *supra* note 16, ¶¶ 2–6.
[23] RESERVE BANK OF INDIA, *Customer Protection – Limiting Liability of Customers*, *supra* note 15, ¶¶ 5–10.
[24] INDIAN CYBER CRIME COORDINATION CENTRE, MINISTRY OF HOME AFFAIRS, *Frequently Asked Questions*, https://i4c.mha.gov.in/FAQ.aspx (last visited Sept. 17, 2026).

 [ISSN 2581-5369]

should share responsibility where preventable failures contribute to loss. Standardised risk warnings, confirmation-of-payee mechanisms and targeted cooling periods should be implemented for high-risk transactions.

VI. Findings and Recommendations

A. Findings

The study finds that online financial fraud in India is not a single or uniform offence. It includes phishing, vishing, smishing, UPI fraud, identity theft, account takeover, payment-card fraud, fake loan applications, online investment fraud, e-commerce deception, digital-arrest scams and business impersonation. Although their methods vary, these offences ordinarily involve deliberate deception, psychological manipulation and rapid transfer of money through digital-payment systems.

A significant finding is that contemporary offenders increasingly target human judgment rather than directly compromising banking infrastructure. Multi-factor authentication and secure payment systems may prevent unauthorised access, but they cannot always prevent a frightened or deceived customer from personally approving a transaction. Consequently, the distinction between an unauthorised transaction and an authorised push-payment fraud has become particularly important.

The study further finds that online financial fraud is frequently organised. Separate participants may procure identity documents, operate fraudulent calls, provide technical assistance, recruit mule-account holders, transfer funds and withdraw the proceeds. The use of layered mule accounts distances the principal offenders from victims and makes recovery difficult.

India possesses a broad legal framework for prosecuting such conduct. The Bharatiya Nyaya Sanhita, 2023 criminalises cheating, personation, forgery and related conduct, while the Information Technology Act, 2000 addresses identity theft, unauthorised computer access and cheating through computer resources. The BNSS and BSA govern investigation and electronic evidence. Nevertheless, the framework remains fragmented, creating uncertainty in the selection of charges, jurisdiction and institutional responsibility.

The study also finds that delayed reporting is a major reason for unsuccessful recovery. Digital funds may be transferred through several accounts within minutes. The 1930 helpline, National Cyber Crime Reporting Portal and Citizen Financial Cyber Fraud Reporting and Management System have improved immediate reporting and fund interception. However, victims may still be required to separately contact banks, payment intermediaries and police agencies.

 [ISSN 2581-5369]

Investigation is weakened by jurisdictional disputes, shortage of trained personnel, delayed preservation of electronic records and inadequate coordination among States. Improper collection or certification of digital evidence may render important transaction logs, messages and electronic records inadmissible. Indiscriminate freezing of entire bank accounts can also harm innocent account holders where only a limited amount is connected with the alleged fraud.

Finally, the present RBI customer-liability framework provides meaningful protection against unauthorised transactions but does not adequately address payments technically authenticated by victims under deception, impersonation or coercion.

B. Recommendations

India should establish a comprehensive regulatory framework for fraudulently induced authorised payments. Liability should be determined by examining the conduct of the customer, sending bank, receiving institution and relevant digital or telecom platform. A victim should not be denied protection merely because the payment was technically authenticated.

The 1930 helpline should be directly integrated into all banking and payment applications. A single verified complaint should automatically alert the sending bank, receiving institution, payment intermediary and competent police agency. The complaint should generate one reference number through which the victim can track fund interception, FIR registration and restoration.

Uniform procedures should be adopted for registration, preservation notices, interstate investigation, account freezing and release of recovered money. Ordinarily, only the amount connected with the suspected transaction should be frozen unless broader restriction is supported by evidence. Jurisdictional questions should be resolved after immediate protective action.

Banks should move beyond initial KYC verification and continuously monitor abnormal account behaviour. Newly opened accounts receiving multiple unrelated credits, rapid pass-through transactions and sudden changes in devices or transaction patterns should attract enhanced review. Artificial-intelligence tools may assist detection, but adverse decisions must remain explainable and subject to human review.

Payment applications should provide clear, transaction-specific warnings. Users must be informed that a UPI PIN is required to send money and never to receive it. Confirmation-of-payee mechanisms, targeted cooling periods and additional verification should be introduced for high-risk or unusually large first-time transfers.

 [ISSN 2581-5369]

Cybercrime units should receive specialised training in digital forensics, financial tracing, virtual assets and electronic-evidence certification. Prosecutors should participate during complex investigations so that legally admissible records are collected from the beginning.

Telecom providers and digital platforms should rapidly act against verified fraudulent numbers, advertisements and impersonating accounts while preserving information required for investigation. Enhanced verification should be mandatory for advertisements offering investment, lending and financial-recovery services.

Finally, public-awareness programmes should provide practical instructions in regional languages. Citizens must be informed that digital arrest has no legal existence, official agencies do not require transfer of money to a "safe account," and immediate reporting is essential. Awareness campaigns must avoid victim-blaming and encourage prompt disclosure of fraud.

VII. Conclusion

Online financial fraud has emerged as a serious challenge to India's rapidly expanding digital economy. The growing use of UPI, internet banking, payment cards, mobile wallets and online commercial platforms has improved financial inclusion and transactional convenience, but it has also created opportunities for offenders to deceive victims remotely, conceal their identities and transfer criminal proceeds within seconds. The study establishes that online financial fraud is not merely a technological offence; it is a complex economic crime involving social engineering, psychological manipulation, digital infrastructure and organised financial networks.

Phishing, vishing, identity theft, account takeover, investment scams, fraudulent loan applications, digital-arrest scams and UPI fraud demonstrate that offenders increasingly exploit human judgment rather than directly compromise banking systems. Routine activity theory, rational choice theory, differential association and neutralisation theory explain how suitable targets, inadequate guardianship, perceived rewards, learned criminal techniques and moral rationalisations contribute to such offending. Victim vulnerability is situational and may affect persons of any age, education or economic position. Accordingly, victims should not be blamed for conduct produced through calculated fear, urgency, impersonation or deception.

India possesses a broad legal framework through the Bharatiya Nyaya Sanhita, 2023, Information Technology Act, 2000, Bharatiya Nagarik Suraksha Sanhita, 2023, Bharatiya Sakshya Adhiniyam, 2023 and relevant financial and regulatory enactments. Nevertheless, fragmentation, overlapping offences, territorial disputes, deficiencies in electronic-evidence collection and delayed institutional cooperation reduce its practical effectiveness. The

 [ISSN 2581-5369]

distinction between unauthorised transactions and fraudulently induced authorised payments also leaves an important gap in customer protection.

Initiatives such as the 1930 helpline, National Cyber Crime Reporting Portal, Citizen Financial Cyber Fraud Reporting and Management System, Cyber Fraud Mitigation Centre, Suspect Registry and artificial-intelligence-based mule-account detection represent significant progress. Their success, however, depends upon immediate reporting, accurate information sharing and coordinated action among police, banks, payment intermediaries, telecom providers and digital platforms.

India must therefore adopt a preventive and victim-centred strategy. A unified framework should govern authorised push-payment fraud, account freezing, restoration of recovered money and allocation of responsibility across the payment chain. Banks must undertake continuous transaction monitoring, while cybercrime units require specialised forensic training and prosecutorial assistance. Payment applications should provide transaction-specific warnings, confirmation-of-payee safeguards and additional verification for high-risk transfers. Public awareness must be practical, multilingual and free from victim-blaming.

Ultimately, online financial fraud cannot be controlled through punishment alone. Effective regulation must combine secure technology, informed users, real-time fraud detection, prompt financial intervention, admissible electronic evidence and meaningful victim redress. Such coordinated guardianship is essential to preserve public confidence in India's digital-payment ecosystem while ensuring accountability for those who exploit it.

*****

 [ISSN 2581-5369]