



Online Financial Fraud in India: Legal Remedies and Challenges in Cybercrime Investigation

Dr. Vishva Nath Sharma

Associate Professor, Department of Law, Invertis University, Bareilly

Article Info: (Received- 20/05/2026, Accept- 14/06/2026, Published- 10/07/2026)

DOI- [10.70650/rvimj.2026v3i7006](https://doi.org/10.70650/rvimj.2026v3i7006)

Abstract

Online financial fraud has emerged as one of the most serious cybercrime challenges in India due to the rapid expansion of digital banking, online payments, mobile financial services, and internet-based transactions. This paper examines the legal framework, investigative mechanisms, institutional responsibilities, and victim-remedy systems governing online financial fraud in India. It analyses the role of the Information Technology Act, 2000, the Indian Penal Code, 1860, financial regulations, and other economic laws in addressing offences such as phishing, identity theft, payment fraud, data theft, malware attacks, and cyber-enabled money laundering. The study also highlights major procedural difficulties, including collection and preservation of electronic evidence, maintenance of chain of custody, tracing of digital money trails, jurisdictional conflicts, cross-border investigations, and limited forensic capacity. It evaluates the functions of police agencies, cybercrime cells, financial regulators, and digital forensic institutions in investigation and enforcement. In addition, the paper discusses civil, administrative, compensatory, and restitutionary remedies available to victims. Comparative perspectives are used to identify international best practices. The study concludes that stronger legal definitions, specialized investigation mechanisms, improved inter-agency coordination, enhanced digital forensic infrastructure, public awareness, and effective victim-recovery systems are essential for combating online financial fraud in India.

Keywords: Online Financial Fraud, Cybercrime, Cybercrime Investigation, Information Technology Act, Digital Evidence, Financial Cybercrime, Legal Remedies

1. Introduction

The term “online financial fraud” denotes a form of financial crime that has gained prominence in the wake of technological advancements and widespread digitalization. It encompasses a range of illegal, deceptive, and unethical acts perpetrated by individuals or groups to obtain money or other valuable assets from targeted individuals or entities through fraudulent online methods. Although applicable to all forms of financial crimes carried out online, the phrase is commonly associated with cyber-enabled financial offences, such as phishing, data theft, identity fraud, malware dissemination, online payment fraud, investment fraud, and money laundering through virtual-currency exchanges (Rana et al., 2017). As per the India Cyber Crime

Coordination Centre (IC4) Annual Report 2021-22, online financial fraud constituted 45.8% of total detected cybercrimes during the reporting period, involving amounts far exceeding the threshold for stringent enforcement under the Prevention of Money Laundering Act (Jerome Orji, 2019). Moreover, the same report ranked online financial fraud as the most significant financial crime in India, shedding light on its critical socio-economic impact.

The rise of online financial fraud in India has resulted from a combination of factors. Cybercriminals are incentivized to target the Indian populace due to its large population and perceived socio-economic vulnerabilities. Several risk factors further escalate the national vulnerability to online financial fraud. These include cashless payment mobility through smartphones and online banking, widespread adoption of unsecured digital transactions and merchant related services, personal details and transactional information shared on social-networking sites, rapid growth of consumer adoption of new financial products and services without comprehensive understanding, and a belief among mob-equivalent players that authorities may ignore fraud-related complaints or investigations.

2. Conceptual Framework of Online Financial Fraud

The rapidly expanding array of digital finance offerings, the increasing complexity of financial products, and the multiplied transaction choices have created greater opportunities for exploitation by cybercriminals. Phishing, information-stealing malware, email-based identity theft, and other internet-based financial fraud have become widespread (Dzomira, 2016). Such crimes are conceptualized as online financial fraud, comprising cyber-enabled financial crime where electronic devices and the internet form an integral part of offence commission. Cyber-enabled financial crimes exploit existing criminal offence typologies while adopting creative methods and technologies. Criminals leverage offline opportunities instead of cyber methods, and there is considerable overlap between cyberspace and conventional modes when the objective is analogous. Any crime at the nexus of financial malfeasance and cyber capability fits into this conceptualization. The eco-system for digital finance also shapes the convenience and security of online transactions, potentially creating exposure to abuse. The theory of routine activity suggests three prerequisite conditions for crime: suitable targets, a motivated offender, and lack of capable guardians. The availability of instant digital payment systems, wealth accumulation options, and investment channels at the hands of consumers has increased target attractiveness for cybercriminals. The accessibility of the dark web for criminal networking materials and client recruitment facilitates the emergence of motivated offenders. The absence of adequate cybersecurity measures and unqualified online financial literacy leaves consumers vulnerable to intrusion, providing a tremendous opportunity for cybercriminals to operate.

3. Legal Regime for Online Financial Fraud in India

India is signatory to the 2001 Budapest Convention on Cybercrime, yet legally actionable cyber dependent offences remain largely unsecured. Penalty provisions for online financial fraud vis-à-vis statutes, applicable sections, nature, and degree of evidentiary and interpretive complications therewith.

The cyber-financial crime precursors (aggravated and simple imprisonment) foreseen by sections 3, 4, and 5 of the Indian Penal Code were partially declared unconstitutional in 2010, prompting amendment of those provisions. At present, online payment frauds—and consequently cyber-financial frauds generally situate themselves at the statutory control nexus of the Information Technology Act (sections 66C, 66D, and 67B), the Indian Penal Code (sections 420 and 419), and the Special Economic Offences Act

(section 3).

Data theft (theft, receiving stolen property) and several identity-related crimes (either subject to remaining statutory regimes or their aftermath) likewise occupy the lower functional precincts. Identity misuse forms part of the payment fraud ambit. The remaining Indian Penal Code statutory constructions (sections 378 and 392) subsume corresponding unenumerated concepts. Furthermore, though equipment possession bears pertinence to midway operation, it continues outside extant Indian discussion.

3.1. Penal Provisions

Digital India is governed by legislation created to safeguard electronic data and closely watch various kinds of crimes that occur through the use of electronic information. Presently, the Information Technology (IT) Act, 2000 governs online, internet-enabled financial frauds as the Country's primary and all-embracing statute. Financial frauds carried out internationally follow a different process and may often have multiple jurisdictional overlaps. In such cases, apart from the IT Act, the criminal provisions of the Indian Penal Code (IPC), 1860 and other specific economic offences legislation are invoked. Online fraud continues to proliferate globally, and India is no exception. As a plethora of convenience accompanies financial transactions conducted over the internet, the new model of financial fraud has taken service provider-protected netizens hostage, thus indicating a very few apprehensions of the criminals involved in these frauds. Have a look at the enormous online fraud statistics across the country, which depicts a grim picture of crimes committed using new technology under the able umbrella of financial services. As per the National Crime Records Bureau (NCRB), out of 29,099 Indian Penal Code (IPC) Financial fraud cases, the 2019 percentage share of (Sabrina Mohd Sabri, 2018) amid Crime Against Property juggled the utmost number of cases across the Country. Out of an enormous amount of 729 Cr. reported of online money fraud, 619 Crores were lost via phishing attempts. An analysis further exposed that the Crime in India Report of 2019 shows that people became potential victims of an alarming 77%, situated mostly in metropolitan cities, focusing on a segment that belonged primarily to the working judiciary and class among rural folks with a concentration of other rural sectors. Amount of instance generated during the financial year vis-a-vis public and private, and real banking shows the challenging step ahead to outsmart the hyenas of new-age fraud that generated attention across the mapping of the economy to sustain corruption ratio within a threshold limit.

The crucial criteria that govern a fraud case fall under the perview of the IT Act, and the standards for punishment and prosecution vary from one section to another. Uncovering the exact statute a fraudulent activity, a crucial task, is the first milestone in trailing the right statutory mechanism. Different typologies of online fraud motivate criminals differently. These prerequisites remained deterrent under the general Court of Criminal Procedure unless a fresh tool of law uprooted from British Statute adopted to bast it forth. Banking assets strategized remained in a limbo after going distinct from the portion.

3.2. Procedural Mechanisms

The investigation of online financial fraud is plagued by various procedural challenges (Rana et al., 2017). Several important processes must be completed following the registration of a complaint under the IT Act or IPC: the collection of electronic evidence, analysis of the data to identify the modus operandi of the fraudster, and tracing of the money trail after the relevant bank accounts have been identified. In many cases, the fraud may be of a cross-border nature involving international money transfers. In India, the number of companies engaged in cross-border digital fraud is

on the rise, which illustrates the need for cooperation between enforcement agencies. The collection of electronic evidence from the servers of intermediary companies (e.g., social networking sites, email service providers, internet service providers) is facilitated if the necessary data can be obtained in under 72 hours, which is crucial to ensuring the admissibility of the evidence before a court of law (Nouh et al., 2019). Such procedural mechanisms are critical to enforcement in India and are described further below.

In order to preserve a proper chain of custody for electronic evidence, it is essential to prepare a statement of facts for the magistrate detailing the circumstances under which the electronic evidence was obtained and packed, as well as the whereabouts of the material at all times. These details should accompany the forwarding letter for the materials, which should indicate the specific evidential issue that the forensic examination would address (Sabrina Mohd Sabri, 2018). While the chain of custody is important for any piece of evidence, it is a prerequisite for the admissibility of digital evidence and an essential consideration for the investigating officer. For this reason, it is advisable to contact the court even before the registration of an FIR in order to avoid time-consuming delays that may compromise the evidence and complicate the matter still further.

3.3. Financial and Economic Offences

Cross-border transactions or online purchases invariably involve the movement of money or information across national borders. These transfers fall within the ambit of the ambit of financial and economic offences, requiring coordination with the Reserve Bank of India (RBI) and Financial Intelligence Unit (FIU) for the preservation, and possible forfeiture and confiscation of proceeds. The Foreign Exchange Management Act prohibits the remittance of money for certain types of online payment fraud (Rana et al., 2017). Entities involved in these transactions are subject to Know Your Customer (KYC) and Customer Due Diligence (CDD) compliance obligations (Sabrina Mohd Sabri, 2018).

4. Cybercrime Investigation: Institutions, Powers, and Jurisdiction

Following the 2008 financial crisis, an unprecedented upswing in the volume and complexity of online financial fraud has been observed in India, accompanying the accelerated digitalization of finance and the adoption of digital payment methods. Online financial fraud occurs when perpetrators obtain sensitive financial information through illegitimate means—primarily phishing scams, malware, and identity theft—and use this information to execute unauthorised financial transactions on digital platforms or telephonically through unsolicited calls ostensibly from legitimate financial institutions. Types of online financial fraud include fraudulent bank account opening; illegal money transfers from bank accounts; payment using stolen credit or debit card details; unauthorized automatic payment debits against credit card accounts; fraudulent fund transfer requests impersonating company management; and unauthorised sale of e-wallets, pre-paid cards, and debit or credit card details (Rana et al., 2017).

4.1. Enforcement Agencies and Their Roles

The investigation of online financial fraud in India is complicated by the multifaceted nature of the phenomenon, its evolving contours, and a fast-changing technological landscape. Yet, at the operational level, the task is primarily about the identification of offenders and the recovery of stolen funds. Enforcement agencies, therefore, are under considerable pressure to employ sound investigative techniques supported by

solid operational frameworks. Specific institutional arrangements can play a pivotal role in facilitating cybercrime investigation, and inter-agency coordination across law enforcement, financial investigation, and digital forensics is crucial. India's existing procedures are shaped by several factors, including legislative and policy frameworks, judgements, anti-money-laundering requirements, international obligations, and technical capacity and competence. Parallel processes are followed under civil and criminal statutes.

At the apex of the enforcement ecosystem, the police have overall jurisdiction to investigate financial fraud offences and are the first point of contact for victims reporting cybercrime to law enforcement. The police are further supported by a range of specialized cybercells, financial investigation units, and Computer Emergency Response Teams (CERT) operating at both the national and state levels. A national Financial Fraud Investigation Agency has also been constituted on the lines of the Federal Bureau of Investigation to investigate large-scale and multi-jurisdictional financial fraud and cybercrime.

4.2. Investigative Techniques and Digital Forensics

Establishing a legally valid connection between a suspect and a cybercrime requires specific information, and the adage "Everything is stored as data" is highly relevant (Rana et al., 2017). Cyber forensics helps identify the type of fraud involved using data from systems to track a suspect's device, applications, mode of operation, and communication lines with victims. Data collection, preservation, and analysis techniques include studying the metadata of transactions and files created or modified by suspects, log analysis, backdoor discovery, and malware source tracking.

During investigations, covert surveillance at suspicious places after receiving complaints helps identify fraudsters with similar backgrounds. Surveillance warrants determine legal validity. Intercept procedures safeguard the accused's right to privacy; internet service provider details assist in locating the suspect's machine, while the judicial third-party clause prevents unauthorized access. Encrypted data is paramount in today's society; investigators use field applications for preservation, while a forensic investigator addresses decryption. Unfortunately, some vendors don't disclose flaws in their products, hindering effective enforcement.

Intelligence-led investigations draw on an intelligence database maintained by CERT-In for prior incidents. Cyber threat intelligence highlights the attack type, tools used, targeted sectors, and the attacker's country, skill level, and motivation, assisting investigation prioritization. Vulnerability assessment identifies weaknesses in systems, applications, and network links and leads to the identification of likely criminals. Private-sector cooperation is essential; service providers usually have incident response protocols detailing data retention policy and cyber forensic examination assistance.

4.3. Jurisdictional Challenges in Cross-Border Fraud

Cross-border fraud is a major hindrance to effective online financial fraud prosecution (Rana et al., 2017). Financial transactions are transcending borders with the advent of new payment systems and internationalisation of the internet (AZZAM SAQF AL HAIT, 2014). Jurisdictional rules assist the determination of the applicable law to the case. Consequently jurisdiction consumption creates significant inconvenience to fair trial rights, prolonging the travel and documentation time of enforced return (Casino et al., 2022).

The forces opposing an investigation or prosecution largely controls forum and choice of law. Possession of the exculpatory evidence on the suspect devices, necessary for pursuing legally competing fraud cases constitutes a significant incentive to oppose the investigation. Extradition and mutual legal assistance processes involving the

cross-border cooperation often frustrates the timely access to the evidence.

5. Remedies for Victims and Redress Mechanisms

Online financial fraud continues to be a major concern for the Indian populace due to the surge in transactions through online banking. This has, in turn, ignited a rise in fraud cases by various actors on the dark web. For the protection of citizens, the Indian courts and legislatures have enacted various legal remedies that hinder the occurrence of such frauds. In particular, the second bank of India, a government-regulated banking institution, enables online users to check the authenticity of messages received through SMS, e-mails, and pop-ups. Users are able to visit the bank's website to check whether the message is genuine or if it is a hoax. More recently, the Reserve Bank of India, on its recently released website, has published information about various malware that targets banking users and enables them to check on their behalf whether their devices are infected.

5.1. Civil and Administrative Remedies

Online financial fraud can trigger both civil and administrative remedies. A formal civil suit may be filed to recover damages or seek equitable relief, such as an injunction. Victims of online financial fraud can also lodge complaints with various regulatory agencies, including the Securities and Exchange Board of India (SEBI) and the Reserve Bank of India (RBI). Many such complaints may be channeled through consumer-protection forums, whose jurisdiction extends to broader misconduct (Rana et al., 2017).

Administrative avenues are not limited to complaints. In some situations—such as those implicating stock-market regulations or failure to honour payment instruments—statutory compensation may also apply. If a bank is involved and online banking or electronic funds transfer had been used, the victim may be eligible for a recovery-of-funds scheme specified in the relevant RBI circular, provided that the complaint is lodged with the bank within a stipulated time (Sabrina Mohd Sabri, 2018).

5.2. Compensation and Restitution Schemes

Although compensation and restitution schemes are available, victims of online financial fraud in India often face lengthy and complex processes that delay relief. By the time relief is awarded, it is not uncommon for substantial portions of the embezzled funds to be transferred out of the jurisdiction even when recovery processes are promptly initiated (Hendrik Samudra, 2019). Payments are routinely routed through multiple bank accounts, e-wallets, shell companies, and crypto wallets. As these schemes become more elaborate and harder to track, the chances of recovery fall dramatically.

6. Challenges in Enforcement and Prosecution

Enforcement and prosecution face hurdles arising from legal definitions, policy gaps, and lack of training. Unlike traditional crimes, online financial fraud remains ill-defined in Indian legislation. Existing statutes regulate only certain aspects of financial fraud without specifying crime types or consolidated provisions; their definitions do not encompass all cybercrime forms or modern technology (Rana et al., 2017). Attempts to formulate a comprehensive legal framework have stalled, impeding effective deterrence and contributing to widespread impunity.

Consequently, offenders circumvent regulatory frameworks, operating under the erroneous assumption that only non-technology-based fraud constitutes an offence. Online fraud such as phishing, vishing, card-not-present transactions, and cyber-money laundering therefore proliferate without targeted regulatory control (Nouh et al., 2019). Even when conventional definitions match the fraud type deployed, ambiguities arise; for instance, “cyber” elements in cyber-financial schemes complicate compliance demand. Moreover, the absence of technology-mandated legislative specifications

permits offenders to breach the law confidently, insisting on prior physical dependence on the victim (Naqvi, 2018). Policy gaps compound the challenges of investigating online financial fraud. Inter-agency coordination remains often lax, despite accountability links among judicial, law enforcement, and financial sector stakeholders. Investment in forensic expertise—an essential component of the financial investigative model—adds to the commitment required to conclusively establish inter-agency synergies. The introduction of specialized frameworks for investigating other types of online fraud, such as child pornography, poses further complications; compliance with such measures without a corresponding regime for financial fraud supervisors precludes a targeted investigations approach.

6.1. Technical and Evidentiary Hurdles

Cyber-attacks have evolved to a great extent in recent years. Malicious software, commonly referred to as malware, is one of the most quoted methods for such attacks. Although its use in the investigation of cybercrimes is limited, it plays an indispensable role in crimes such as account take-over fraud, phishing, identity fraud, corporate espionage, data theft, and many more (Rana et al., 2017). The sophistication of cyber-attacks threatens not only an individual's privacy but the safeguarding of the country's secrets and vital information. These threats range from spam to full-scale industrial espionage or the theft of private information. With cybercrime growing 3 percent globally per year, and an average cost of \$11 million per year per organization, stricter laws have been made to reduce cyber-attacks. This includes tampering with the mails, threatening an individual online or any use of the internet which results in privacy invasion such as spam, hacking, cyber stalking and impersonation. The enhancing of case studies and policies, and their replicability to other jurisdictions are needed (Nouh et al., 2019).

6.2. Legal Gaps and Policy Gaps

Before extensive legislative and policy measures are adopted by regulating and investigating authorities, India has evolved considerable legislation and institutional structure to prevent a growing online financial fraud. Educating the public about the financial sector and financial technology should be the priority—this would improve the effectiveness of preventive measures and the entire regime. Despite the existence of many regulations to prevent online financial fraud, awareness and need of legal action remains poor. Financial sector regulators such as Reserve Bank for India and Securities Exchange Board of India (Hazarika, 2021) thus must harmonise and propagate various laws with citizen-level knowledge on omnipresent financial frauds concerning distinct media.

Legislative and institutional mechanism for the country presently harmonise remarkably with other jurisdictions concerning coverage. Yet due to rural-urban disparity and below-world-average income group pockets, the public domain remains poorly informed on financial fraud incidents and preventive regulations. Conformed income details further show many citizens never apply for bank loans, do not have a bank account, or maintain bank balance-command frugally below thousand rupees; such restricts the legal knowledge reaching them via countrywide online portals or public grievance redress mechanism. Though legislative, institutional, and policy mechanism contend worldwide forefront, still gaps in formulation and implementation operate counterpart underprivileged sector, particularly education (Misra & Chacko, 2021).

6.3. Resource Constraints and Capacity Building

The investigation of online financial fraud in India is presently hampered by resource and capacity constraints. Police agencies tasked with investigating fraud lack essential

capabilities—such as training, funding, manpower, analytical tools, and infrastructure. Developing specialized institutions for cybercrime investigation could improve the overall quality and speed of investigations without losing a holistic approach; such institutions could remain generic in terms of crime type while developing deep knowledge of the cybercrime threat landscape (Rana et al., 2017).

The government should also leverage private-sector investment to bolster investigation, remediation, and clean-up capabilities. A recent report advocated for the establishment of specialized cybercrime courts and regional cybercrime labs within the law-enforcement framework. The report underscored the need to establish a National Cybercrime Centre for coordinating cybercrime investigation and infrastructure-sharing between agencies and the financial sector (Apau & N. Koranteng, 2020).

7. Comparative Perspectives: Lessons from Other Jurisdictions

Despite the rapid growth of online financial fraud targeting Indian consumers, legal and enforcement responses remain underdeveloped compared to international front-runners. Drawing on comparative analyses of national frameworks in the financial sector and broader cybercrime, the present section distils best practices and identifies potentially transferable approaches to redress systemic weaknesses (Rana et al., 2017).

Internationally, jurisdictions with relatively stringent cybercrime laws have responded to identical challenges by broadening their existing legal apparatus and operational capacities. Civil remedies such as consumer protection and compensation legislation have been emphasised, alongside the implementation of victim-recovery frameworks and statutory reimbursement pools. The Indian consumer-protection regime lacks a separate legal framework for digital payment, severely hampering tackling online financial fraud despite there are ex-ante and ex-post remedial schemes in place. Without a specific right to compensation, there is no statutory expectation of expediency within existing recovery systems, and inadequate coordination and pooling of restitution measures impede potentially swift victim-recovery options.

8. Policy Implications and Recommendations

Online financial fraud is an ongoing challenge that affects individuals and the nation as a whole. The study aims to provide the necessary basis to address the fraud issue and identify the improvements needed within Indian jurisdictions. Formal recommendations are provided. The penetration of online financial fraud systems is a genuine area of concern for the individual and the Indian economy. There has been a noticeable rise in various kinds of online financial frauds perpetrated by known and unknown players throughout the nation. Specific typologies concerning online fraud include payment frauds, phishing, data thefts, and identity frauds. As observed, the perpetrators of the mentioned frauds usually get offers from outside the country. Another noticeable aspect is that various types of commodity frauds (gold, silver, and forex) are predominantly contacted and offered through social media platforms such as WhatsApp and Telegram.

9. Conclusion

The socio-economic upheaval triggered by the COVID-19 pandemic has intensified the scourge of online financial fraud in India, with 94.93 per cent of cybercrimes in 2020 targeting property and money, and the aggregate financial outlay for cybercrime mitigation during 2014–19 and 2020–21 standing at INR 60,113 crore. Various legal and institutional frameworks and mechanisms have been adopted to prevent and penalise online financial fraud. Statutory provisions contained in the Information Technology Act, 2000 and the Indian Penal Code, 1860 subject offenders to

imprisonment of up to ten years and fines of up to INR 1 crore. Procedural safeguards permit the police and other enforcement agencies to preserve forensic data and digital evidence, share information to prevent repetition of fraud, and freeze accounts suspected in the commission of online fraud. Several avenues exist for the redress of fraud victims through civil suits, administrative complaints, and compensation schemes regulated and supervised by the Reserve Bank of India.

The legal regime for frauds encountered through the medium of electronic payment systems remains partially effective. The statutory definition of fraud enshrined in Indian Penal Code excludes deception aimed purely at exercising dominion over property without the consent of the owner. The framing of an online fraud offence is additionally impeded, because of the absence of an explicitly designated e-fraud statute and only limited and sometimes inconsistent judicial pronouncements on the subject. Current payment infrastructure leads to untraced direct transfers of money from victim to fraudster between different banking systems, while low transaction limits offered during the onboarding process hinder the applicability of existing laws to online payments by electronic means. The absence of a designated statutory authority for resolving customer complaints pertaining to online payment fraud compels many victims to retract their complaint with the police soon after lodging it. Other constraints include the ineffectiveness of many cybercrime cells and investigative units and the absence of an appropriate analysis tool for tracing digital funds transacted via Payment Gateway (Rana et al., 2017).

Author's Declaration

I/We, the author(s)/co-author(s), declare that the entire content, views, analysis, and conclusions of this article are solely my/our own. I/We take full responsibility, individually and collectively, for any errors, omissions, ethical misconduct, copyright violations, plagiarism, defamation, misrepresentation, or any legal consequences arising now or in the future. The publisher, editors, and reviewers shall not be held responsible or liable in any way for any legal, ethical, financial, or reputational claims related to this article. All responsibility rests solely with the author(s)/co-author(s), jointly and severally. I/We further affirm that there is no conflict of interest financial, personal, academic, or professional regarding the subject, findings, or publication of this article.

References:

1. Rana, N., Sansanwal, G., Khatter, K., & Singh, S. (2017). Taxonomy of Digital Forensics: Investigation Tools and Challenges.
2. Jerome Orji, U. (2019). Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria.
3. Dzomira, S. (2016). Financial consumer protection: internet banking fraud awareness by the banking sector.
4. Sabrina Mohd Sabri, N. (2018). A legal study of the Section 420 of the Penal Code in regulating internet cheating offences / Nurfitri Sabrina Mohd Sabri.
5. Nouh, M., R. C. Nurse, J., Webb, H., & Goldsmith, M. (2019). Cybercrime Investigators are Users Too! Understanding the Socio-Technical Challenges Faced by Law Enforcement.
6. Flory, T. (2015). Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana Agencies.
7. AZZAM SAQF AL HAIT, A. D. E. L. (2014). Jurisdiction in Cybercrimes: A Comparative Study.
8. Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: Cross-border Criminal Investigations and Digital Evidence.
9. Hendrik Samudra, A. (2019). MODUS OPERANDI DAN PROBLEMATIKA PENANGGULANGAN TINDAK PIDANA PENIPUAN DARING.
10. Naqvi, S. (2018). Challenges of Cryptocurrencies Forensics – A Case Study of Investigating, Evidencing and Prosecuting Organised Cybercriminals.
11. Hazarika, A. (2021). E-Commerce: Expectations and Shortfalls.
12. Misra, A. & Chacko, M. (2021). Square pegs, round holes, and Indian cybersecurity laws.

ncbi.nlm.nih.gov

13. Apau, R. & N. Koranteng, F. (2020). An overview of the digital forensic investigation infrastructure of Ghana. ncbi.nlm.nih.gov
14. Cassim, F. (2009). Formulating specialised Legislation to address the Growing Spectre of Cybercrime: A Comparative Study.

Cite this Article-

'Dr. Vishva Nath Sharma', "Online Financial Fraud in India: Legal Remedies and Challenges in Cybercrime Investigation", Research Vidyapith International Multidisciplinary Journal, ISSN: 3048-7331 (Online), Volume:3, Issue:7, July 2026.

“Copyright © 2026 The Author(s). This work is licensed under Creative Commons Attribution 4.0 (CC-BY), allowing others to use, share, modify, and distribute it with proper credit to the author.”

