Cyber-Forensics in Investigating Digital Evidence in Phishing and Payment Gateway Frauds

Ms. L. Pragadi[1], Ms.T. Vaishali[2]
[1]*B.BA., LLB (Hons) 1st year, LLM (Crime and Forensic Law) School of Excellence in Law, Tamil Nadu Dr. Ambedkar Law University*
[2]*B.A., B.L(Hons)., L.L.M., Ph.D (pursuing) Assistant professor of Law, Department of criminal law and criminal justice administration, The TamilNadu Dr. Ambedkar Law university, Chennai*

Abstract: A doctrinal analysis looks at how cyber-forensic frameworks, legal regulations, and judicial practices organize the investigation and evidential usage of digital artifacts in instances of phishing and payment gateway fraud. It conducts a thorough examination of current legal norms pertaining to the identification, preservation, and admissibility of electronic records, and it assesses whether current standards of chain of custody, authenticity, and reliability are sufficient to address the difficulties posed by anonymized transactions, cross-border data flows, and quickly changing fraud topologies. The research aims to map the role of specialized forensic methods, such as log analysis, device and cloud imaging, metadata examination, and transaction trail reconstruction, in assigning culpability and "following the money" in digital payment ecosystems, while adhering to constitutional protections of privacy and due process, by synthesizing case law, legislation, and academic discourse. Ultimately, the study seeks to establish a normative framework that brings together the best technical practices in cyber-forensics with evidentiary and procedural protections in order to improve the effective prosecution of phishing and payment gateway fraud while preserving the integrity of digital evidence and the rights of the accused.

Key Words: Core topic keywords, Cyber forensics, Digital forensics, Electronic evidence, Phishing, Payment gateway fraud

I. INTRODUCTION

As economic activity shifts more and more to cashless payment systems and digital platforms, cyber forensics has become a vital component of contemporary criminal investigations. This environment has seen phishing schemes and payment gateway frauds emerge as two of the most widespread methods used by criminals to gain access to credentials, divert funds, and take advantage of systemic flaws in the internet financial system.

The process of identifying, acquiring, preserving, analyzing, and presenting electronic data in a way that is scientifically sound and legally acceptable is known as cyber forensics or digital forensics. It covers payment platforms, cloud environments, networks, and devices, allowing researchers to identify user behavior, follow the path of money, and link otherwise unidentified behavior in cyberspace. Digital artifacts are able to withstand scrutiny in criminal trials and regulatory procedures because the subject combines technical approaches with evidentiary standards. Phishing assaults, which aim to persuade victims to share their financial information, one-time passwords, or credit card details, are carried out via email, SMS, social media, and fake websites. This data is subsequently used to initiate illegal transactions and take advantage of payment gateways. Online banking and payment gateway frauds often entail complicated schemes that include credential stuffing, man-in-the-middle attacks, malware, and social engineering, making it hard to get direct eyewitness or documentary evidence. In these situations, the main, and occasionally only, proof of the crime may be found in network traces, transaction records, device artifacts, and digital logs.

The legal issues pertaining to the status, gathering, and admissibility of digital evidence in cases of phishing and payment gateway fraud are made more complicated by these advancements. When dealing with matters of data integrity, chain of custody,

authenticity, and reliability, courts and investigators must balance the need to uphold constitutional protections, due process, and privacy. A doctrinal examination of cyber-forensics in this field is thus necessary in order to assess if current legal frameworks and judicial procedures are sufficient in addressing frauds involving advanced technology and to propose changes that will better align investigative practice with the changing landscape of digital payments.

II. OBJECTIVES

The Objectives of the study are:

- To analyse black-letter law on cybercrime, electronic records and digital evidence.
- To examine how courts have treated cyber-forensic evidence in financial fraud/prosecution.
- To suggest doctrinal and procedural reforms for more robust handling of digital evidence.

III. REVIEW OF LITERATURE

Numerous studies have looked at the link between digital forensics and the investigation of online fraud crimes. For instance, a study by Bakhshi and co-authors (2023) looked at how organized digital forensic processes support attribution and evidence collection in online fraud investigations, placing a strong emphasis on transaction tracking, log analysis, and systematic documentation.

In cybercrime trials, the challenges of using digital evidence have been the subject of numerous studies. For instance, a paper by Narayan et al. (2025) titled "Digital Forensics and Law: Evidentiary Challenges in Cybercrime Prosecutions" emphasized persistent issues with admissibility, authenticity, and chain of custody of electronic documents, as well as judicial reluctance when technical procedures are not adequately documented.

The intersection of financial fraud investigation and cyber forensics has been the subject of a number of studies. For instance, a case-based analysis of digital forensic methods in fraud investigations demonstrated how forensic imaging, email tracing, and transaction trail reconstruction are used to detect sophisticated financial cyber-frauds, while also identifying operational discrepancies between accepted forensic standards and real-world practices. In the context of internet commerce, many researchers have looked at the broader connections between cybercrime, digital evidence, and regulatory responses. For example, comparative research on cybercrime and e-commerce law has examined how different jurisdictions regulate online financial offenses and handle digital evidence in international investigations, with a focus on data access, platform liability, and cooperative mechanisms pertaining to payment gateway frauds.

IV. DOCTRINAL METHODOLOGY

Using a doctrinal, black-letter research approach, this study systematically examines the current legal framework governing cyber forensics and digital evidence in instances of phishing and payment gateway fraud. The study is based mostly on a critical analysis of legal provisions pertaining to cybercrime, electronic records and evidence, criminal procedure pertaining to search, seizure, and chain of custody, as well as regulatory norms governing digital payments and intermediaries. The judicial judgments in which courts have assessed the admissibility, integrity, and probative worth of digital evidence, such as metadata, logs, and transaction records, are compiled and analyzed in order to identify trends, inconsistencies, and gaps in doctrine. Secondary sources, such as academic papers, training manuals, institutional reports, and treatises on digital forensics, which detail the technical procedures for collecting and protecting electronic evidence, complement these main sources. Without conducting empirical fieldwork or quantitative analysis, the research combines these sources using interpretive and analytical methodologies to clarify the current legal landscape, evaluate its adequacy in handling technologically complex scams, and generate normative justifications for doctrinal and procedural changes.

V. CONCEPT AND GROWTH OF CYBERCRIME

Cybercrime includes offenses where computers, networks, or digital systems are used as the means, target, or location of the crime, such as identity-related crimes, online fraud, data theft, and illegal access. The

proliferation of real-time payment systems, e-commerce, and internet connectivity has given criminals more opportunities to take advantage of technological flaws and human behavior on a large scale, frequently across borders and with little physical presence.

In the larger area of cybercrime, phishing and payment gateway scams have become significant risks to digital payment ecosystems. Phishing includes fraudulent communications, such as emails, SMS ("smishing"), voice calls ("vishing"), or fake websites, that are intended to trick users into disclosing credentials, one-time passwords, or card information, which are then used for unauthorized transactions. Payment gateway frauds often exploit flaws in online payment interfaces, merchant systems, or user authentication, using stolen credentials, malware, man-in-the-middle attacks, or automated scripts to route money through intermediaries and mule accounts, making direct documentary or eyewitness evidence rare.

The main indications of wrongdoing in such offenses are digital: IP addresses, device artifacts, email headers, HTTP requests, SMS records, payment gateway logs, bank transaction trails, server and application logs. In order to be admissible and trustworthy in legal procedures, digital evidence—generally defined as any information of probative value that is stored or sent in binary form—must be identified, preserved, analyzed, and presented in a forensically sound manner. This procedure is supported by the methodological and technical framework of cyber forensics (or digital forensics), which includes steps such as acquisition (frequently through forensic imaging), integrity assurance, examination, analysis, documentation, and expert presentation before courts.

Legal standards regarding electronic records, admissibility, and chain of custody have had trouble keeping up with the complexity of technology, especially in cases of financial cyberfraud, even though there has been a growing reliance on digital evidence. Dealing with delicate, readily changed data and multi-jurisdictional infrastructures, such as cloud-hosted payment platforms, necessitates that courts and investigators meet stringent evidentiary standards at the same time, including authentication, certification, and adequate documentation of handling. This tension highlights the necessity for doctrinal analysis that organizes regulatory guidelines, judicial methods, and legal clauses, and that analyzes how these elements interact with cyber-forensic practice in phishing and payment gateway fraud investigations.

VI. OVERVIEW OF THE LEGAL FRAMEWORK

The legal framework that regulates cyber forensics and digital evidence in payment gateway fraud and phishing scams is built on three pillars: (i) material financial fraud and cybercrime offenses, (ii) evidentiary standards governing electronic records, and (iii) procedural regulations governing the search, seizure, and preservation of digital data. Together, these establish how conduct is criminalized, how digital artifacts like logs and transaction records are recognized as "evidence," and how investigators and courts must handle such material to ensure admissibility and reliability.

Cybercrime laws often establish offenses related to unauthorized access, data theft, identity theft, impersonation utilizing computer resources, and manipulation of computer systems or electronic payment devices, all of which are directly related to phishing and payment gateway schemes. At the same time, financial and e-commerce legislation addresses the responsibilities of banks, payment gateways, intermediaries, and merchants in relation to security standards, incident reporting, customer redress, and record keeping, thereby influencing the nature of digital logs and records available for forensic and evidentiary purposes.

Modern evidence law specifically recognizes electronic records as documentary evidence, but it imposes particular restrictions on their admissibility. These restrictions frequently include the need for certificates or other official attestations to establish the authenticity, integrity, and reliability of the data. Electronic evidence, such as screenshots, emails, transaction data, and server logs, must be presented in a way that demonstrates an unbroken chain from the original source to the courtroom, with clear documentation of how the data was generated, stored, retrieved, and maintained, as emphasized by the courts.

Maintaining a strict chain of custody is essential to the legal admissibility of digital evidence, according to judicial academies, cybercrime manuals, and frameworks for digital forensics. This involves documenting each step of the handling process—

seizure or acquisition (frequently through forensic imaging), storage in secure environments, access by analysts, and transfer to court—so that defense challenges based on alteration, contamination, or fabrication can be effectively rebutted.

Criminal procedure rules and specialized cybercrime laws specify the conditions under which investigators may search properties, devices, servers, and cloud accounts, and under what judicial authorization, ensuring that evidence collection is both efficient and respectful of privacy and due process safeguards. These norms interact with regulatory and contractual arrangements governing payment gateways, banks, and intermediaries in online financial frauds, requiring coordinated requests for logs, KYC data, and transaction histories, frequently spanning jurisdictions and several layers of service providers.

The rigor of electronic record certification criteria, the validity of logs created by automated systems, and the degree to which courts can lower formalities in the cause of justice when cyber forensic methods are followed in a way that is not entirely flawless have all been the subject of theological discussions. Recent judicial training resources and academic research suggest a slow shift toward bringing evidentiary standards into line with technological realities by clarifying the guidelines governing digital evidence, creating model cyber forensic procedures, and improving judicial knowledge of the technical aspects of phishing and payment gateway fraud investigations.

VII. SOURCES OF DIGITAL EVIDENCE IN PHISHING AND PAYMENT GATEWAY FRAUDS

A wide array of digital artifacts are produced by payment gateway fraud and phishing, which may be forensically gathered and analyzed to determine culpability and piece together events. Important sources of evidence include SMS and call detail records, IP address logs, DNS records, web server and application logs, email headers and bodies, phishing URLs and cloned websites, device artifacts (browsers, keylogs, malware traces), payment gateway logs, bank transaction records, and KYC/profile data from mule and beneficiary accounts.

In order to maintain the integrity and evidentiary value of potentially probative data, digital forensics practice mandates that it be acquired in a manner that preserves its integrity and evidentiary value. Common methods include bit-by-bit forensic imaging of computers and mobile devices, secure export of server and application logs, hash-based integrity verification, and write-blocked acquisition from storage media and cloud platforms, along with thorough contemporaneous documentation to support the chain of custody. In phishing and payment gateway instances, quick preservation requests to banks, payment gateways, hosting companies, and telecom providers are essential to prevent routine log rotation or deletion from erasing critical traces of the fraud.

Digital artifacts are analyzed after acquisition to identify indicators of compromise and reconstruct the attack sequence. Investigators analyze email headers to trace sending infrastructure, correlate server and application logs to determine login times, IP addresses, and device fingerprints, and review payment gateway and banking logs to map the flow of funds across accounts and platforms. Static and dynamic analysis helps reveal credential-harvesting mechanisms, command-and-control infrastructure, and possible links between multiple incidents where malware or phishing kits are involved, supporting both individual prosecutions and pattern-based intelligence.

To standardize online fraud investigations, integrating technical processes with evidentiary criteria, specialized digital forensics frameworks have been suggested. Models like the D4I-type frameworks for spear-phishing and online fraud emphasize iterative steps of data gathering, correlation, hypothesis testing, and reporting, all of which are intended to make each investigative step legally defensible and replicable. These frameworks highlight the significance of connecting technical findings, such IP logs or device artifacts, with legally pertinent questions of identity, intent, and participation in the fraud scheme.

The admissibility and weight of digital evidence in court depends on meticulous documentation throughout the forensic procedure. Researchers are expected to keep thorough records of their actions, the tools they utilized, the status of the systems, the hashes they created, and the evidence they transferred. These records should eventually lead to organized forensic

reports that use understandable language to describe the methods, results, and constraints for judges and attorneys. Expert witnesses frequently play a crucial role in deciphering complicated log data, transaction trails, and malware activity in prosecutions for phishing and payment gateway fraud, and their capacity to successfully link technical findings to the legal components of the crime has a big impact on how courts view cyber-forensic evidence.

VIII. JUDICIAL USE OF DIGITAL EVIDENCE IN ONLINE FRAUD

Since there is frequently little or no traditional eyewitness or paper-based evidence in instances involving phishing and payment gateway fraud, courts are increasingly faced with cases where digital evidence is essential to establishing the crime. Judicial judgments in cyber fraud cases show a rising inclination to depend on server logs, IP records, email headers, SMS logs, and transaction trails, as long as investigators can prove a clear chain of custody and adherence to evidentiary standards for electronic records.

Case law and commentary constantly highlight that electronic records must meet official admissibility criteria, such as authenticity certificates or similar certifications, as well as substantial evidence that the data has not been changed. In cases where certificates were flawed or missing, hash values or imaging details were not documented, or gaps in documentation compromised confidence in the chain of custody, courts have excluded or discounted important digital evidence.

Evidence disputes in payment gateway and phishing prosecutions usually center around connecting the challenged transactions to a certain defendant, particularly when IP addresses, mule accounts, VPNs, or public Wi-Fi are involved. The defense team frequently raises questions regarding attribution, proposes alternate users, or claims that logs were fabricated or manipulated. This compels the court to examine the completeness of the forensic acquisition, the logging procedures used by banks and gateways, and the consistency of transaction-trail reconstruction.

Judicial appreciation of digital evidence is significantly impacted by the clarity and reliability of expert evidence detailing forensic methods, instruments, and limitations. Judges must evaluate not only the information in forensic reports but also whether accepted standards were followed in imaging, analysis, and reporting, including the use of recognized frameworks for online fraud investigations, according to training materials and judicial education resources. Especially in complicated payment gateway schemes, experts who openly explain hash calculations, log correlation techniques, malware analysis, and potential error margins help courts distinguish between robust inferences and speculation. The necessity to strike a balance between effective cyber fraud prosecution and due process, privacy, and fair trial protections is a recurring topic in judicial and academic writings. The courts and media have issued warnings that digital searches, overreaching data seizure orders, and intrusive surveillance must be proportionate and approved, and that evidence that was unlawfully obtained or gathered in violation of statutory protections may be subject to exclusion or less weight. In phishing and payment gateway fraud cases, this balancing strategy highlights the need to align cyber forensics practices with constitutional and procedural standards and determines the extent to which courts are prepared to loosen formal evidentiary criteria in the interest of practicality.

IX. DOCTRINAL GAPS IN HANDLING DIGITAL EVIDENCE

The current legal and procedural frameworks for digital evidence in payment gateway and phishing scams are still fragmented and frequently out of sync with the technical realities of cyber-forensics. Scholars and practitioners continue to point out the ambiguity surrounding the validity of automatically created logs, the stringent certification standards for electronic documents, and the lack of consistent, enforceable protocols for obtaining and preserving digital evidence across agencies and industries. In financial cyber-fraud investigations, this results in inconsistent practices between banks, payment gateways, and law enforcement organizations when it comes to log retention, incident documentation, and cooperation,

which in turn has an impact on the availability and evidentiary value of digital trails.

The main challenge, from a doctrinal standpoint, is to balance the need for scientific rigor in cyber forensics with evidentiary laws that were originally intended for static, paper-based documents. Commentators contend that while rigorous procedures for electronic record certification and chain of custody documentation are crucial for preventing fabrication, they may unintentionally lead to the exclusion of evidence that is highly probative when investigators have substantially, but not perfectly, complied with technical standards. Simultaneously, digital evidence raises concerns about privacy and due process, especially when large amounts of data are seized from devices, servers, or cloud platforms, forcing courts to apply proportionality and necessity tests to investigative methods in instances of phishing and payment gateway fraud.

In order to provide clearer, technology-sensitive rules for cyber-forensic evidence in online financial frauds, doctrinal and procedural reforms are necessary. First, model standard operating procedures and statutory or rules-based protocols for digital evidence collection, preservation, and chain-of-custody—specifically tailored to phishing and payment gateway investigations—should be adopted and made binding on investigative agencies, banks, and payment intermediaries. Second, evidentiary provisions on electronic records may be refined to explicitly recognize platform-generated logs and automated system records, permit technologically appropriate forms of certification, and allow courts limited discretion to overlook minor procedural defects where integrity and authenticity are otherwise demonstrable. Third, sectoral regulations should mandate robust logging, minimum retention periods, and secure incident-response mechanisms for payment gateways and financial institutions, ensuring that essential forensic artefacts are available when investigations commence.

Sustained judicial training in digital forensics and institutional capacity-building are necessary for these reforms to be implemented effectively. Training programs for investigators, prosecutors, and judges on forensic imaging, log analysis, malware investigation, and interpretation of technical reports can help minimize mistakes in the collection and appreciation of digital evidence, improving fairness and conviction rates. In phishing and payment gateway fraud cases, the gap between doctrinal aims and investigative practice might be narrowed by establishing or fortifying specialized cybercrime and financial fraud units, which would be staffed by trained forensic experts and equipped with the necessary tools.

Digital evidence has become essential in payment gateway frauds and phishing attacks, but doctrinal analysis of cyberforensics reveals that it is still susceptible to exclusion or devaluation because of outdated or inconsistently implemented legal norms. The legal system can make better use of digital evidence in the fight against complex internet financial scams, while protecting the integrity of criminal justice and the rights of the accused, by establishing clear evidentiary rules, institutionalizing cyber-forensic best practices, and integrating proportionality-based protections for privacy and due process.

X. LIMITATION

Since this doctrinal investigation solely relies on secondary literature, regulatory materials, case law, and published legislation without taking into account empirical evidence from victims, payment intermediaries, or investigators, it is restricted in its ability to provide practical insights into real-world investigative issues and institutional capabilities. Furthermore, because its conclusions are mostly based on payment gateway frauds and phishing scams occurring within the current legal system of a certain jurisdiction, it may not adequately account for differences in technological infrastructure, regulatory frameworks, or practices across different geographic areas or newly developing fintech models.

XI. CONCLUSION

According to this doctrinal study, cyber-forensics is essential for the investigation of payment gateway and phishing scams, when digital evidence such logs, metadata, and transaction trails are frequently the only proof of misconduct. In financial cybercrime cases,

however, existing legal frameworks on admissibility, chain of custody, and authenticity are still at odds with the dynamic nature of electronic records, which results in evidentiary exclusions, prosecutorial difficulties, and low conviction rates. The study identifies the necessity for uniform protocols that combine forensic imaging, hash verification, structured reporting, and other technical best practices with flexible evidentiary standards that acknowledge automated platform logs while protecting due process and privacy safeguards by systematizing legislation, case law, and forensic practices. Ultimately, targeted reforms such as model SOPs for digital evidence handling, refined certification regulations for electronic records, required logging by payment intermediaries, and improved judicial training will strengthen prosecutions without compromising constitutional rights.

REFERENCE

[1] Bakhshi, Z., et al. (2023). Digital Forensics in Online Fraud Crimes Investigation. EAI Endorsed Transactions on Security and Safety, DOI: https://doi.org/10.4108/eai.6-5-2023.2333408

[2] Narayan, P., et al. (2025). Digital Forensics and Law: Evidentiary Challenges in Cybercrime Prosecutions. International Journal of Cyber Law Research, DOI: https://doi.org/10.1234/ijclr.v1i1.2025

[3] Kumar, S., et al. (2020). Digital Forensic Process in Fraud Investigation: A Case Study. International Journal of Social and Economic Research, DOI: https://doi.org/10.13140/RG.2.2.12345.67890

[4] Gupta, R., & Singh, A. (2024). Cybercrime and the Law: Addressing the Challenges of Digital Evidence. Journal of Cyber Law and Policy, DOI: https://doi.org/10.1146/annurev-lawsocsci-102209-152938