Development Economics of China
2025, VOL. 9, NO. 12, 10-13
DOI: 10.47297/wspdecWSP2515-797302.20250912

Challenges in Collecting Electronic Evidence for Online Fraud and Legal Application

Limin Chen[1,2], Батсайхан[2]

[1]Guangzhou Huashang University, Guangzhou, Guangdong, 511300, China

[2]Ikh Zasag University, Ulaanbaatar, 14010, Mongolia

ABSTRACT

As online fraud tactics evolve, electronic evidence has become a crucial component in convictions and sentencing. However, in judicial practice, the ephemeral nature of electronic evidence, its technical concealment, and the susceptibility of retrieval processes to third-party platform interference pose significant challenges in terms of timeliness and technical feasibility. At the level of legal application, ambiguities persist regarding the standards for admissibility of electronic evidence, technical criteria for authenticity verification, and procedural norms for evidence collection. This paper proposes improvement strategies, including establishing a technical support system, refining examination and recognition rules, and clarifying platform responsibility mechanisms, aiming to provide references for enhancing the collection of electronic evidence in online fraud cases.

KEYWORDS

Online fraud; Electronic evidence; Evidence collection challenges; Legal application

1 Introduction

In today's era, where information technology is deeply integrated into social life, cyber fraud crimes exhibit highly organized, covert, and technologically sophisticated characteristics, posing severe challenges to traditional criminal justice practices. As the core medium for reconstructing criminal facts, the probative value of electronic evidence directly impacts both prosecution and defense parties, as well as judicial fairness, in solving cyber fraud cases. However, since cyber fraud often operates within virtual spaces, electronic data possesses characteristics such as susceptibility to tampering, dynamic circulation, and high dependence on specific software and hardware. This creates practical bottlenecks for investigative agencies, including short evidence collection windows, technological methods lagging behind criminal techniques, and obstacles in obtaining third-party data [1]. The lag in legal application has also become increasingly apparent. How to precisely define the admissibility of evidence within vast digital information has become an urgent theoretical and practical challenge for the legal community. Therefore, researching the difficulties in collecting electronic evidence for online fraud and the underlying legal application disputes is a practical necessity to counter the escalation of criminal methods. It is also an inevitable choice for improving the criminal evidence system in the digital age and maintaining society's overall sense of legal security. This paper examines the challenges in collecting electronic evidence for online fraud cases and the associated legal application issues, proposing corresponding solutions to provide valuable insights for fair adjudication of such cases.

2 Challenges in Collecting Electronic Evidence for Online Fraud

2.1 Perishability of Electronic Evidence and the Timeliness Dilemma

Electronic evidence refers to information stored in digital form on storage media or within network environments. Its physical dependency and logical instability make it susceptible to damage or alteration. In cyber fraud cases, electronic evidence faces two primary risks of destruction: intentional human actions and automatic system overrides. First, suspects may use instant messaging "read-and-delete" features, remote control tools, or scripts to instantly wipe server data or local storage upon detecting investigations, creating a physical break in the crime chain. Second, network environments involve frequent underlying data flows where system logs, temporary files, and cached data disappear over time or get overwritten by new data. This imposes nearly exacting demands on the timeliness of evidence collection [2]. Frequent underlying data flows in network environments cause system logs, temporary files, and cached data to vanish over time or through overwriting by new data. This imposes nearly impossible demands on the timeliness of evidence collection. Investigative agencies often obtain leads after criminal acts have been committed, while electronic evidence has an extremely short lifespan. Consequently, by the time investigators access systems, critical traffic data, login logs, and transaction traces may already be overwritten or erased.

2.2 Technical Concealment vs. Forensic Capabilities Gap

The increasing sophistication of cyber fraud tactics poses severe technical concealment challenges for evidence collection. Suspects commonly employ proxy servers, virtual private networks (VPNs), and multi-layered relay hops to mask their actual IP addresses, making it difficult for investigators to locate physical devices within the vast cyberspace precisely. Furthermore, the widespread use of encryption technologies significantly complicates evidence gathering. End-to-end encryption protocols render intercepted communication packets unreadable to investigative agencies without the private key, effectively rendering evidence inaccessible due to technical barriers [3]. Furthermore, an objective gap exists between the pace of forensic capability development and the evolution of criminal techniques. The emergence of distributed storage, dark web technologies, and anonymous communication tools renders traditional physical seizure and online extraction methods ineffective against decentralized architectures. Updates to forensic devices and analysis software often lag behind technological advancements in the black and gray markets, preventing investigators from establishing complete evidence chains when confronted with new obfuscation algorithms or dynamic domain names. This asymmetry in the technological standoff directly undermines the probative value of electronic evidence in uncovering criminal facts.

2.3 Practical Obstacles in Retrieving Data from Third-party Platforms

Online fraud relies on various internet service providers, including social platforms, payment institutions, and cloud service providers. Most electronic evidence resides on these third-party servers rather than directly on the victim's or suspect's terminal devices. During investigations, law enforcement must obtain data through formal requests, but this process faces numerous obstacles. First, conflicts arise over the scope of data retrieval. Platforms typically restrict the type, timeframe, and granularity of data provided to protect user privacy and commercial secrets, resulting in incomplete or irrelevant evidence. Second, collaboration efficiency conflicts with compliance reviews. Platforms' internal management structures and compliance standards vary, and retrieval processes often involve multiple layers of administrative approvals. This lag proves inadequate when confronting the rapid flow of fraud funds and information. Additionally, smaller platforms or online service providers often lack specialized forensic capabilities, employ non-standard data storage formats, and lack effective hash verification mechanisms. Consequently, retrieved data may face legal validity crises during court cross-examination due to questions surrounding its authenticity and integrity.

3 Legal Application of Electronic Evidence in Cyber Fraud Cases

3.1 Admissibility and Classification of Electronic Evidence

In judicial practice, establishing the admissibility of electronic evidence is fundamental to its inclusion in litigation proceedings. Although the law recognizes electronic data as an independent category of proof, its diverse presentation forms often lead to classification disputes in cyber fraud cases. Specific evidence, such as chat records containing victim statements or electronic ledgers reflecting fund transfers, generally possesses multiple characteristics of documentary evidence, physical evidence, and audiovisual materials. Mechanically categorizing such evidence under traditional classifications overlooks the dependence of electronic data on storage environments and technical parameters, thereby affecting the standards for authenticity review. Furthermore, establishing evidentiary admissibility hinges on the legality of acquisition methods. During cyber fraud investigations, electronic data obtained through remote inspection or technical surveillance must satisfy conditions, including authorized collection entities, procedural compliance, and carrier integrity. If evidence collection violates procedural justice, even if the content truthfully reflects fraudulent facts, the risk of exclusion due to evidentiary defects remains. Therefore, clarifying the typological classification of electronic evidence in specific cases and establishing admissibility standards aligned with its technical characteristics form the logical starting point for ascertaining facts in cyber fraud cases.

3.2 Technical Standards for Authenticity Review of Electronic Evidence

Authenticity review lies at the core of electronic evidence's legal application. Given electronic data's susceptibility to tampering and lack of traceability, courts must establish rigorous technical review standards when adjudicating cyber fraud cases. First is carrier authenticity: whether the physical medium storing electronic data maintained its original state during extraction, sealing, and transfer, and whether it suffered physical damage or logical interference. Second is content authenticity: whether the electronic data was maliciously altered during its generation, storage, or transmission. To establish technical standards, judicial practice widely adopts hash value verification as the basis for identity comparison. This involves comparing algorithmic summaries of the original data and the evidence presented in court to determine if

the data has been altered.

Additionally, the entire lifecycle of electronic data must be traceable, encompassing system log analysis, timestamp verification, and digital signature validation. Only when electronic evidence can demonstrate reliable origins, clear transmission routes, and unmodified critical nodes can it be deemed admissible. This shift from technical to legal perspectives means judges cannot rely solely on written materials when assessing authenticity but must also depend on technical expert conclusions.

3.3 Regulatory Gaps in Electronic Evidence Collection Procedures

The current lack of procedural norms for collecting evidence in cyber fraud cases has become a bottleneck affecting evidence validity. The existing legal framework provides only general principles for electronic evidence extraction procedures, lacking operational details for complex network environments. In scenarios involving distributed cloud storage and cross-border data flows, there are no clear procedural guidelines on defining the geographical scope of search authority or conducting compliant online extraction without seizing physical originals. This leaves investigators frequently entangled in procedural uncertainties during practical operations. Additionally, legal regulations governing the evidence custody chain are inadequate. When electronic evidence is transferred from investigative agencies to procuratorates or courts, there are no unified digital transfer standards or tamper-proof oversight mechanisms. Inadequate operational protocols, equipment environment requirements, or handover documentation during custody can all raise questions about evidence integrity. This lack of procedural regulation increases the risk of evidence exclusion and undermines the effectiveness of cross-examination by defendants and their counsel.

4 Improving Strategies for Cyber Fraud Evidence Collection and Legal Application

4.1 Strengthening the Technical Support System for Electronic Forensics

To enhance the effectiveness of combating cyber fraud, a modernized technical evidence collection support system must be established. On one hand, the research and application of underlying technologies should be advanced, vigorously developing decryption software for data extraction—such as encrypted communication tools, virtual dialing utilities, and decentralized applications—to narrow the time gap between investigative methods and criminal techniques. Establishing specialized electronic data forensics laboratories equipped with high-performance memory imaging extraction devices and network traffic analysis platforms facilitates the immediate preservation of digital traces at crime scenes and enables in-depth investigation [4]. Simultaneously, standardizing the evidence collection process is crucial. This involves promoting electronic forensics for digital evidence such as electronic data, audiovisual materials, and voiceprint images, thereby establishing standardized investigative procedures. Creating a full-process online forensics platform that integrates hash verification, timestamp reinforcement, and blockchain evidence storage technologies into forensics terminals ensures that every step in the generation, extraction, and transfer of electronic evidence is backed by tamper-proof technical proof. Through the upgrading of technical equipment and the standardization of operational procedures, tangible support can be provided to address the issue of easily perishable evidence.

4.2 Refining Rules for Reviewing and Admitting Electronic Evidence

Refining legal application requires establishing clearer, actionable standards for reviewing and admitting electronic evidence. Uniform criteria for assessing authenticity should be adopted, mandating that electronic evidence submissions include complete evidence collection records, mirror images of original storage media, and verification checksum comparison logs for critical nodes. For fragmented data resulting from conversion, cleansing, or restructuring, the conversion logic and technical principles must be explained to ensure evidence withstands authenticity scrutiny during court cross-examination. Additionally, establish presumption and proof rules for "human-machine consistency." Addressing the issue of identity concealment in cyber fraud, integrate elements such as login IP addresses, device identifiers, behavioral biometric features, and payment association information to construct multi-faceted logical chains. This approach reconstructs the connection between virtual identities and real-world suspects. Simultaneously, enhance the expert witness system by permitting computer forensic specialists to participate in court proceedings, assisting judges in conducting in-depth, penetrative reviews of technical issues involving algorithmic principles and data recovery.

4.3 Streamlining Platform Assistance Mechanisms for Evidence Collection

To overcome obstacles in accessing third-party platform data, establish a cooperative framework with clear responsibilities and transparent procedures. First, define the statutory obligation of internet service providers to

cooperate with criminal investigations, establishing tiered standards for data retrieval. For critical traffic data and account transaction information containing criminal leads, platforms should establish rapid response channels and reserve standardized retrieval interfaces to meet the timeliness requirements of investigative work [5]. Secondly, a compliance review and accountability mechanism for platform-assisted evidence collection should be established. When providing data, platforms must ensure its originality and integrity, attaching technical descriptions of the data generation environment and authenticity commitments. Platforms that lose or leak critical evidence due to internal mismanagement or non-compliant data storage should bear legal liability for negligence. Standardized police-enterprise cooperation agreements should unify data exchange formats and encrypted transmission protocols to accelerate evidence retrieval and ensure judicial authentication standards during data transfer.

5 Conclusion

The collection and authentication of electronic evidence in online fraud cases involve a technical tug-of-war and precise alignment with legal procedures. Addressing challenges such as the perishable nature of electronic evidence, its high technical concealment, and difficulties in third-party platform collaboration requires coordinated governance through both legal frameworks and technological solutions. Establishing a modernized evidence collection support system, refining rules for authenticity review, and implementing platform collaboration mechanisms with clear delineation of rights and responsibilities will facilitate the deep integration of technical standards for evidence collection with legal application criteria. This approach will effectively counter the iterative evolution of online fraud crimes.

About the Author

Limin Chen, Lecturer, Ph.D. candidate, Research Focus: Ideological and Political Education.;Батсайхан,Ph.D.Professor,Research Focus:Law.

References

[1] Han P. AI-powered digital arbitration framework leveraging smart contracts and electronic evidence authentication[J].Scientific Reports,2025,15(1):37327-37327.

[2] Guan C. Cross-Border Cybercrime Digital Evidence: Current Research and Fundamental Categories[J].Modern Law Research,2025,6(4).

[3] Shurson J. The balance of efficiency and fundamental rights in the EU e-Evidence Regulation[J].New Journal of European Criminal Law,2025,16(3):278-299.

[4] Xiao Y, Chen L. Efficient and secure electronic evidence exchange scheme for Internet of Things [J]. Frontiers in Physics, 2025, 131522170-1522170.

[5] Lin T. Analysis on Challenges and Improvements of Electronic Evidence Preservation on Blockchain in China[J]. Modern Law Research, 2024,5(2).