Journal of Commercial Law Review
2025, VOL. 9, NO. 3, 7-13
DOI: 10.47297/wspjclrWSP2516-249701.20250903

Research on Electronic Data Forensics Issues and Rule Reconstruction in Fourth-Party Payment-Based Cyber Money Laundering Crimes

Liyana Mi

China University of Political Science and Law, Beijing, 100091, China

ABSTRACT
This study investigates the critical challenges and corresponding solutions in electronic data forensics within the context of fourth-party payment-based cyber money laundering crimes. As digital finance evolves, the abuse of fourth-party payment platforms for money laundering has become increasingly rampant, making electronic data the cornerstone of conviction and sentencing. However, current practices are hindered by outdated legal frameworks, ambiguous procedural norms, and inadequate mechanisms for ensuring the defendant's right to cross-examination.To address these systemic gaps, this paper first identifies the key application dilemmas of electronic data evidence in such cases. Subsequently, it proposes targeted strategies for rule reconstruction, including the formulation of specialized legal guidelines, standardization of forensic procedures, and strengthening of the defendant's right to cross-examination through technical assistance and improved evidence disclosure.The theoretical significance of this research lies in filling the gap in evidence law scholarship regarding emerging cybercrimes. Practically, it aims to provide law enforcement and judicial authorities with a more robust, fair, and efficient framework to combat fourth-party payment-based money laundering and safeguard financial stability.

KEYWORDS
Fourth-party payment; Cyber money laundering; Electronic data forensics; Evidence rules; Right to cross-examination

1 Introduction

1.1 Research background

With the vigorous development of China's digital economy, third-party payment has been deeply integrated into social and economic life. On this basis, the "fourth-party payment" model, which integrates and expands third-party payment services, has emerged. By aggregating multiple third-party payment interfaces, it provides merchants with unified payment solutions, greatly improving transaction efficiency.

However, its convenience and anonymity have also been exploited by criminals, becoming an important tool for cyber money laundering crimes. Through complex fund pools, sub-accounting, and redirection technologies, fourth-party payment platforms can quickly and covertly transfer criminal proceeds and their benefits, making traditional money laundering crimes in cyberspace more concealed, complex, and transnational.

In such new types of cybercrime cases, criminal activities are mainly completed through data interaction, so electronic data has become the core evidence for determining case facts and conviction and sentencing. From user identity information, transaction records, and fund flows to platform backend logs and algorithm models, electronic data runs through the entire criminal process. Therefore, the legal and effective acquisition and use of these electronic data directly determine the success or failure of case investigation.

Currently, academic research on cyber money laundering crimes and electronic data forensics has achieved many results. In the field of cyber money laundering, most studies focus on the money laundering risks and regulatory countermeasures of third-party payment platforms, while specialized research on the emerging fourth-party payment model is still insufficient. In the field of electronic data forensics, scholars mainly discuss issues such as the collection, fixation, and review of traditional electronic data, and there is a lack of systematic discussion on how to adapt to the special forensics needs in complex scenarios such as fourth-party payment.

In judicial practice, courts and investigation organs in various regions often have inconsistent practices when handling such cases due to the lack of clear legal guidance, leading to the phenomenon of different judgments for the same case. This not only affects judicial credibility but also is not conducive to the effective crackdown on crimes. Therefore, systematic research on this issue is of extremely urgent practical significance.

1.2 Research significance

The theoretical significance of this study lies in focusing on the emerging and complex field of "fourth-party payment-based cyber money laundering" and in-depth analysis of the legal difficulties faced in electronic data forensics therein. This helps fill the theoretical gap in China's evidence law when dealing with such new types of cybercrimes, enrich and develop the connotation of electronic data evidence rules, and promote the adaptation of the evidence law theoretical system to the development of the digital age.

Its practical significance is reflected in that this study aims to provide a set of feasible solutions for judicial practice. By clarifying forensics rules, standardizing operating procedures, and strengthening rights protection, it can effectively guide the forensics behavior of investigation organs, improve the quality and court acceptance rate of electronic data evidence, thereby more effectively combating such crimes and safeguarding national financial security and social stability.

2 Characteristics of fourth-party payment-based cyber money laundering crimes and particularities of electronic data forensics

2.1 Concept and operation model of fourth-party payment

"Fourth-party payment" is not a strict legal term but a commercial concept emerging with the development of the payment industry, usually also referred to as "aggregated payment" or "payment of payment". It is essentially different from the well-known third-party payment.

Fourth-party payment itself does not hold a payment license and does not directly conduct fund settlement. Its core business is to integrate multiple third-party payment, bank, and even other fourth-party payment interfaces to provide merchants with a unified, standardized payment entrance. Its core characteristics are reflected in technical neutrality, business aggregation, and information intermediary, and its value is mainly reflected in technical integration and services rather than financial credit intermediary. To evade crackdowns by public security organs, illegal fourth-party payment platforms tend to apply for fund channels using either "shell companies" registered by themselves or purchased corporate registration materials. Each of these fund channels corresponds to a distinct merchant ID, linking the fund accounts of upstream gray and black industries with downstream users, and enabling transactions to switch back and forth between these channels. Although the funds ultimately flow into accounts actually controlled by upstream criminals, the transfer through multiple payment channels scatters the fund transaction data, creating significant obstacles for public security organs to identify and collect such data.

A typical transaction process is: a user consumes at a merchant and initiates payment → the payment request is sent to the fourth-party payment platform → the platform routes the request to a suitable third-party payment institution or bank → the deduction is completed and the result is returned to the platform and the merchant. In this process, the fourth-party payment platform acts as a "traffic entrance" and "data hub".

2.2 Behavior patterns and characteristics of fourth-party payment-based cyber money laundering crimes

The "running points" model is the most common. Criminal gangs build platforms, recruit a large number of ordinary people ("point runners"), and use their personal collection codes (such as WeChat and Alipay QR codes) to receive funds from upstream crimes (such as telecommunications fraud and online gambling). After the funds enter the "point runner's" account, they are quickly transferred to the account designated by the gang. This model splits large sums of "dirty money" into countless small transactions, mixes them into normal cash flow, and is highly concealed.

In the "fund pool" model, the fourth-party payment platform collects funds from multiple upstream crimes into one or more "fund pool" accounts actually controlled by it through its aggregation function. Subsequently, the platform quickly splits and transfers the funds to different downstream accounts in accordance with instructions through a complex sub-accounting system, completely cutting off the direct connection between the source and destination of the funds.

In the "fictitious transaction" model, criminal gangs construct fictitious business scenarios, such as fictitious e-commerce platforms and game recharge websites. The proceeds from upstream crimes are "purchased" on these fictitious platforms, and the funds enter the merchant accounts controlled by the gangs through the fourth-party payment interface, thereby completing the "legalization" money laundering.

Such crimes are highly concealed, with long and complex fund links. Transaction counterparty information is isolated by the platform, making it difficult to track the true source and final destination of funds. They are highly dependent on technology. The entire criminal process is highly dependent on network technology and platform systems, with almost no physical traces. At the same time, the crimes are transnational. Platform servers, "point runners", merchants, and upstream criminals are often distributed in different regions, even different countries. In addition, due to the extremely high efficiency of fund circulation, the amount involved in a single case is often much larger than that in traditional money laundering cases.

2.3 Types and evidentiary value of electronic data in cases

In such cases, electronic data is the "lifeline" for conviction and sentencing. Without it, the case can hardly be solved and determined.

Core types of electronic data include:

Account and identity data: including user registration information, real-name authentication materials, bound bank

card and mobile phone number information of the platform. Such data is the basis for determining the identity of criminal suspects and locking the involved accounts.

Transaction flow data: the most core evidence, including order number, time, amount, payment method, and account information of the payee and payer for each transaction. They are the key to constructing a complete fund link and calculating the amount involved in the case.

Platform backend logs: including server access logs, operation logs, data modification logs, etc. These logs can reflect the operating status of the platform and the operation behavior of administrators, and are crucial for proving whether the platform is used for criminal activities.

Communication and interaction data: such as chat records and emails between members of criminal gangs, as well as communication records between the platform and merchants/users, which are direct evidence for proving the subjective intent of the crime and the agreement on joint crimes.

Electronic data has strong relevance. It can completely record fund flows, information flows, and personnel interactions, and is the key evidence chain connecting the various links of "upstream crimes - fund circulation - downstream realization". When not tampered with, electronic data is a direct record of objective facts, and its probative force is much higher than that of verbal evidence such as confessions. In view of the non-physical trace characteristics of such crimes, electronic data is the core basis for proving case facts.

2.4 Particularities of electronic data evidence

The objects of forensics are massive and complex.From the perspective of prosecutorial case handling, in recent years, cybercrime cases have generally been characterized by a large number of victims, massive bank transaction records, and enormous volumes of call and chat logs. Criminals specifically exploit the difficulties faced by investigative authorities—such as the inability to trace each individual transaction or communication to a specific person and the challenge of conducting corresponding verification—by fragmenting activities including the acquisition of citizens' personal information, the commission of criminal acts, and the transfer of criminal funds. These fragmented activities are then assigned to multiple perpetrators, broken down into numerous criminal links, and scattered across massive capital flows. A case may involve millions or even hundreds of millions of transaction records, with a huge amount of data. At the same time, data is scattered across multiple nodes such as the user side, merchant side, fourth-party payment platform server, and third-party payment institution, requiring correlation analysis to restore the whole picture of the case.

The forensics process is highly technical. From on-site investigation of servers, seizure and fixation of data, to decryption of encrypted data and analysis of massive data, each step requires professional technical means and equipment, placing high demands on the technical capabilities of investigators.

The state of evidence is volatile and fragile. Electronic data is extremely vulnerable to tampering, deletion, or destruction due to human operations, system failures, or network attacks. In particular, transaction data is time-sensitive and may be automatically overwritten by the backend system, making evidence preservation difficult.

Forensics jurisdiction is transnational. Platform servers, involved personnel, and fund flows may be distributed in different provinces, cities, or even different countries, leading to jurisdiction conflicts and difficulties in cross-regional collaboration.

3 Legal dilemmas of electronic data forensics in fourth-party payment-based cyber money laundering crimes

Currently, in the investigation and forensics of fourth-party payment-based cyber money laundering cases, the existing evidence legal system faces multi-dimensional adaptation problems. These dilemmas directly affect the legality, authenticity, and admissibility of electronic data evidence.The institutional framework and rules are generally constructed based on traditional measures such as surveillance and wiretapping, undercover investigation, and controlled delivery, rather than being designed for emerging technical investigation measures targeting electronic data. China's existing technical investigation system has inherent deficiencies, such as a relatively narrow scope of applicable cases and ambiguous application conditions. When technical investigation measures are applied to electronic data forensics, many new problems arise due to the inherent characteristics of electronic data itself.

3.1 Insufficient adaptability of forensic legal basis

Although China's current "Criminal Procedure Law" and relevant judicial interpretations have provisions on electronic data forensics, these provisions are mostly aimed at traditional electronic data and cannot fully cover the particularities of the fourth-party payment scenario, leading to investigators often falling into the dilemma of having no law to rely on or having difficulty in applying the law in practice.

3.1.1 Laggardness of legal rules

As an "intermediary of intermediaries" for fund circulation, the fourth-party payment platform has significant differences in its business model, fund links, and account system from traditional banks or third-party payment. For example, in traditional financial cases, investigation organs can inquire about and freeze involved accounts in accordance with clear legal provisions. However, in the "running points" model of fourth-party payment, funds flow through thousands of ordinary people's collection codes. How to define the authority and scope of freezing these massive, small-value, and instantaneous transaction accounts, the current law lacks clear guidance. Similarly, for the collection of massive transaction logs in the platform backend, whether to apply the "Notice for Evidence Collection" or the more stringent "Search Warrant", the ambiguity of legal provisions has brought great troubles to investigation work.

3.1.2 Ambiguity of power boundaries

When investigating organs collect data such as user identity information, transaction records, and fund flows, they often face conflicts between citizens' right to privacy, right to personal information, and protection of enterprise trade secrets. The law does not clearly define the scope of "case-related data", which easily leads to the abuse or insufficiency of forensics power, affecting the efficiency of case investigation and the balance of citizens' basic rights.

3.2 Lack of forensic procedural norms

The volatility and tamperability of electronic data determine that its forensics procedures must be strictly standardized. However, in practice, there are obvious shortcomings in the forensics procedures for electronic data in fourth-party payment cases.

3.2.1 Ideally, electronic data forensics should adopt an "integrated model" to present the data in its original stored state.

However, a blanket requirement to submit the original storage medium may lead to difficulties in adducing evidence or even failure to do so. For this reason, when the original storage medium is inconvenient to transport, difficult to preserve, or shall be kept, handled by the relevant authorities in accordance with the law, or lawfully returned, forensics models such as "separate extraction" and "converted collection" may be adopted. [3] Ambiguity of full-process procedures: In the data collection link, there is a lack of special seizure and extraction norms for fourth-party payment platform data, leading to inconsistent operating standards among investigators in practice. For example, failure to conduct compliant "write protection" processing on data storage media may damage the originality of data. In the fixation and preservation link, there is a lack of unified technical standards and operating procedures for freezing and backing up dynamic transaction data (such as real-time flowing fund flows), which is likely to cause the loss of key evidence.

3.2.2 Dilemmas in the initiation and standards of identification procedures

Electronic data identification is a key link in judging its authenticity and relevance, but the law does not clearly specify the specific circumstances for initiating identification in fourth-party payment cases, such as what complex data must be identified. In practice, investigators often decide whether to conduct identification based on experience, resulting in some complex data requiring professional technical analysis (such as algorithm models, encrypted transaction records) being difficult to be adopted by the court due to not being identified. At the same time, there is a lack of unified standards for how to connect judicial accounting identification and electronic data identification for the illegal purpose of "money laundering".

3.3 Standard dilemmas in the review and judgment of electronic data evidence

In the court cross-examination and authentication stages, due to the complexity of fourth-party payment electronic data, it brings great challenges to judges' review and judgment.

3.3.1 Difficulties in determining authenticity and completeness

Fourth-party payment data often undergoes multiple encryption, splitting, and transfer, with long and complex data chains. The prosecution has difficulty providing a complete evidence custody chain to prove that it has not been tampered with, while the defense often challenges its authenticity on the grounds that "data may be modified by platform or third-party technical personnel". For example, how to prove the completeness of massive transaction data through technical means such as hash value verification and log auditing, the law has not established clear review standards.

3.3.2 Dilemmas in logical proof of relevance

In such cases, electronic data is mostly "fragmented" evidence such as massive transaction records, IP addresses, and

device information. How to establish an effective connection between these indirect evidences and the subjective intent ("knowing that it is criminal proceeds") and objective behavior ("providing fund transfer services") of money laundering crimes, there is a lack of clear judicial confirmation rules. Judges often have difficulty forming an inner conviction due to the lack of financial and technical background.

3.4 Obstacles to the realization of the defendant's right to cross-examination

The defendant's right to cross-examination is the core component of the right to defense and a basic guarantee of judicial justice. However, in fourth-party payment electronic data cases, the realization of this right faces severe challenges.

3.4.1 Structural imbalance in cross-examination capabilities

Fourth-party payment electronic data involves complex financial knowledge (such as fund pool operation models) and technical principles (such as API interface data interaction). Defendants and their defenders often lack professional knowledge and have difficulty in effectively challenging the legality of data sources and the scientificity of analysis methods, forming a "technical capability gap" with the prosecution.

3.4.2 Limitations on the scope of cross-examination

The prosecution masters all data in the platform backend during forensics, but the evidence disclosed to the defense before the trial is often screened. The defense has difficulty obtaining complete original data, algorithm models, system logs and other key information, and cannot fully understand the generation and analysis process of data, resulting in cross-examination only staying on the surface and unable to touch the core controversial points.

3.4.3 Weakening of cross-examination effect

Due to the technicality and complexity of electronic data, the defendant's cross-examination opinions (such as challenging the rationality of data statistical methods) are often not adopted because they lack professional expression or exceed the judge's cognitive scope. Even if an expert assistant is applied to appear in court, the cross-examination often becomes a formality due to issues such as the identification of expert qualifications and the effect of opinions, and it is difficult to have a substantial impact on the judgment.

4 Rule reconstruction and path optimization of electronic data forensics in fourth-party payment-based cyber money laundering crimes

In response to the above dilemmas, systematic reconstruction is needed from the levels of legal rules, procedural mechanisms, and rights protection to build an electronic data forensics system adapted to the fourth-party payment scenario.

4.1 Improvement of forensic legal rules

4.1.1 Formulate specialized guiding opinions

The Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security jointly issue the "Guiding Opinions on Electronic Data Forensics in Handling Fourth-Party Payment-Based Cyber Money Laundering Cases", clarifying the definition of electronic data, qualifications of forensics subjects, scope of forensics (such as distinguishing between "case-related data" and "unrelated data") in such cases, as well as special forensics rules for models such as "aggregated payment" and "fund secondary clearing", filling the legal gap.

4.1.2 Establish applicable standards for the principle of proportionality

The law should clearly stipulate that when investigating organs collect fourth-party payment data, they must follow the principles of "necessity" and "minimum infringement". For example, only transaction data of specific accounts and specific time periods directly related to the case can be collected, and "one-size-fits-all" collection of all user data of the platform is not allowed. At the same time, a strict approval procedure (such as approval by the person in charge of public security organs at or above the municipal level) should be established to balance the crackdown on crimes and the protection of rights.

4.2 Systematic construction of forensic procedural rules

4.2.1 Standardize full-process forensic operations

Collection link: Clearly stipulate the seizure procedures for fourth-party payment platform servers and involved terminals, requiring that they must be operated by personnel with electronic data forensics qualifications, and detailed

"Electronic Data Forensics Records" should be made to record the time, place, method, and data status of forensics to ensure procedural traceability.

Fixation and preservation link: Unify the technical standard of "mirror backup + hash value verification" to fix data, which should be signed and confirmed by investigators, platform parties, and witnesses. For real-time flowing fund data, a "real-time freezing + synchronous backup" mechanism should be stipulated to prevent data from being overwritten or deleted.

4.2.2 Improve the review mechanism of identification opinions

Clearly define the legal circumstances for initiating identification. For example, when the amount of case-related data is huge, involves complex algorithm analysis, or there is suspicion of tampering, identification must be conducted.

Standardize the qualifications of identification institutions and personnel, establish a national directory of electronic data identification institutions, and require that appraisers not only have technical capabilities but also understand the constituent elements of financial money laundering crimes.

Strengthen the substantive review of identification opinions. Judges should focus on reviewing the scientificity of identification methods, the authenticity of inspection materials, and the standardization of the identification process, and allow the prosecution and defense to cross-examine the appraisers. When necessary, expert assistants can be invited to assist in the review. From the perspectives of legislation and institutional framework, China's current laws contain relatively broad provisions on appraisals, lacking systematicness and completeness. Additionally, there is overlap among technical appraisal institutions, leading to insufficient authority. Instead of establishing rigid and overlapping regulations for expert assistants, appraisers, and persons with specialized knowledge, as well as distinguishing between different terms such as "appraisal opinions" and "specialized reports, " consideration may be given to drawing on the expert witness system stipulated in the Federal Rules of Evidence of the United States. Specifically, appraisers, expert assistants, and persons with specialized knowledge could be uniformly incorporated into the regulatory scope of a single-track expert witness system, rather than maintaining a parallel three-track system. This approach would help make up for the lack of scientific and technological knowledge among judicial personnel, enhance the credibility of relevant experts, safeguard the authority of appraisal results, and effectively prevent erroneous appraisal opinions from entering the trial process and affecting the outcome of judgments.

4.3 Strengthening the mechanism for protecting the defendant's right to cross-examination

4.3.1 Establish a technical-assisted cross-examination mechanism

The law should grant defendants the right to apply for "technical defense", allowing them to entrust professionals with financial and technical knowledge (such as data analysts and network security experts) as "technical consultants" to participate in the case, assisting them in sorting out evidence and preparing cross-examination opinions. At the same time, legal aid institutions can set up special funds to provide free technical support for defendants with financial difficulties.

4.3.2 Improve the electronic data evidence disclosure system

Establish the principle of "full disclosure + key explanation". Before the trial, the prosecution must disclose all original carriers of case-related electronic data, analysis reports, identification opinions, and data source explanations (such as platform API interface documents and data statistical rules) to the defense. For those involving state secrets or trade secrets, "filtered disclosure" (disclosure after concealing irrelevant information) can be adopted, but the court must review the rationality of the disclosure scope.

4.3.3 Optimize the court cross-examination procedure

Establish a special "electronic data cross-examination session" and extend the cross-examination time to ensure that the defense has sufficient opportunities to challenge the evidence.The emphasis on rights protection in the standardized development of electronic data investigation measures does not mean abandoning the pursuit of objective truth; instead, it requires balancing the protection of citizens' rights in the process of pursuing objective truth.

On the one hand, the concept of coordinating and balancing the discovery of objective truth with the protection of citizens' rights is consistent with the legislative purpose of the Criminal Procedure Law, which aims to balance crime punishment and human rights protection. This provides a shared value foundation for the compatibility between the new investigation measure system and the traditional one. On the other hand, the concept of coordinating and balancing the discovery of objective truth with the protection of citizens' rights may enable the mutual promotion of these two functions. The protection of citizens' rights in criminal proceedings includes not only fundamental rights such as the right to life and property but also citizens' procedural rights. Safeguarding citizens' procedural rights in criminal proceedings can effectively address the imbalance in the confrontation between the prosecution and the defense; meanwhile, the equal confrontation between the prosecution and the defense is also an important means to promote the discovery of

the objective facts of a case.

Promote "visual cross-examination", requiring the prosecution to intuitively present complex fund links and transaction relationships through charts, animations, etc., to help judges and defendants understand.

Clarify the status and role of expert assistants, stipulate that they have the right to raise technical challenges to the prosecution's evidence and identification opinions, and require their opinions to be included in the judge's ruling considerations, enhancing the substantive effect of cross-examination.

4.4 Construction of Cross-Regional and International Cooperation Mechanisms

In view of the transnational nature of fourth-party payment-based money laundering crimes, it is necessary to establish multi-level cooperation mechanisms:

4.4.1 Domestic cooperation

Establish a "electronic data forensics cooperation platform" among public security organs at or above the provincial level to realize evidence sharing and technical mutual assistance among investigation organs in different regions. For example, investigation organs in Place A can request assistance from organs in Place B through the platform to collect data from fourth-party payment platforms located there, avoiding repeated forensics and jurisdiction conflicts.

4.4.2 International cooperation

Draw on international rules such as the "Convention on Cybercrime", establish judicial assistance mechanisms with major payment service-providing countries, clarify the procedures, time limits, and evidential effect of cross-border electronic data collection, solve problems such as difficulty in collecting data from overseas servers and difficulty in evidence conversion, and form a joint force in combating transnational cyber money laundering crimes.

5 Conclusions and Prospects

Electronic data forensics in fourth-party payment-based cyber money laundering crimes is an emerging focal point at the intersection of evidence law and criminal law in the digital era. Its core challenge lies in identifying the typical problems inherent in electronic data forensics and reconstructing the relevant rules accordingly. The current legal predicaments stem from outdated regulations, ambiguous procedures, and a mismatch in capabilities between the prosecution and the defense. To address these, systematic reforms are imperative, including the development of specialized rules, the standardization of forensic procedures, and the enhancement of safeguards for the right to cross-examination.

Looking ahead, as technologies such as artificial intelligence and blockchain become more deeply integrated into the payment sector, electronic data forensics will encounter even more complex challenges. This necessitates continuous innovation in both the theory and practice of evidence law to construct a more scientific, just, and efficient evidence system suitable for the digital age.

References

[1] Xu Z. F. (2023). Application of data-driven investigation in fourth-party payment crime cases. Journal of China People's Police University, (02), 11-17.

[2] Cheng L., Hou R. Y., & Zhao W. (2022). Understanding and application of the "Opinions on Several Issues Concerning the Application of Criminal Procedure Procedures in Handling Information Network Crime Cases". People's Procuratorate, (19), 23-28.

[3] Xie D. K. (2025). On technical investigation measures for electronic data: From the perspective of the UN Convention against Cybercrime. Chinese Journal of Criminal Law, (02), 106-124.

[4] Du M., & Tian K. (2024). On the review methods of electronic data in cybercrime cases. Evidence Science, (01), 28-38.

[5] Wang J. (2025). Evidentiary law dilemmas of virtual currency crimes and their solutions. Oriental Law, (02), 93-105.

[6] Ye X. Y. (2024). Path selection and system construction for the standardized development of electronic data investigation measures: From the perspective of amending the Criminal Procedure Law. Journal of China Criminal Police University, (04), 117-128.