Proceedings of the 4th International Conference on Educational Innovation and Philosophical Inquiries
DOI: 10.54254/2753-7048/17/20231214

Research on Evidence Issues in Telecommunications Network Fraud Cases

Jinfeng Yan[1,a,*,†], Xinyi Xu[2,†], and Keyuan Zhang[3,†]

[1]*Department of Social Sciences and Humanities, North China Electric Power University, Beijing, 102206, China*
[2]*College of Humanities and Law, Henan Agricultural University, Zhengzhou, 450046, China*
[3]*Department of Economy, Shanghai University of Political Science and Law, Shanghai, 200000, China*
a. 120191240211@ncepu.edu.cn
**corresponding author*
[†]These authors contributed equally.

Abstract: With the development of communication tools such as mobile phones and computers, telecommunications network fraud crimes in China have continued to be rampant, causing huge financial losses to the public. Due to the particularity of telecommunications network fraud, its evidence presents characteristics such as difficulty in the collection, differences in electronic certification, and a high degree of electronification. There are many problems in evidence collection, examination, and determination. Given the above issues, this paper proposes suggestions such as improving the custody chain regulations and using experience rules to assist the proof model based on the "Anti-Telecommunications Network Fraud Law of the People's Republic of China", to more effectively combat telecommunications network crimes.

Keywords: telecommunications network fraud, electronic evidence, proof model

1. Introduction

Cybercrime fraud is one of the emerging forms of crime nowadays, and its harmfulness radiates widely, so combating telecommunication network fraud crime has been the people's wish, and is one of the key concerns of society nowadays. In the current practice of punishing cybercrime, China has taken the main means of establishing the "Anti-Telecommunication Network Fraud Law of the People's Republic of China" to make a clear regulation of cybercrime governance. However, there are still many difficulties and challenges regarding the study of evidence in cybercrime, as evidence is difficult to obtain and difficult to identify, and the increasing degree of electronic features also makes the relevant problems gradually appear. This paper focuses on the study of evidence in cybercrime and the related proposals to solve the problem, the discussion of these issues for China to solve the determination of cybercrime has a reference significance.

This paper summarizes the main evidentiary problems in China's telecommunication network cases by reading a lot of literature and analyzing actual cases, tries to analyze the existing evidentiary problems, and concludes from the research that they are in the aspects of evidence collection, evidence examination, and evidence determination respectively. At the same time, specific

DOI: 10.54254/2753-7048/17/20231214

suggestions are given for the relevant problems, which are expected to provide the theoretical basis for the relevant evidence problems in the future.

2. Basic Features of Evidence Issues in Telecommunication Network Fraud Cases

2.1. Complexity of Evidence Collection and Densification

Traditional fraud means upgraded to the industrialized fraud system under the Internet, the evidence collection and identification become more difficult, cybercrime cross-border crime leads to evidence dispersion, the formation of multiple crime nests, as the world has not signed a consistent policy for the governance of cybercrime, so this causes difficulties for the collection of evidence forensics, the distribution of cybercrime evidence has a hidden nature, currently requires personnel and technical support to collect evidence, evidence also has a wide range around the world, alone under a country's judicial power can not fully collect the complete evidence of cybercrime, coupled with the huge amount of cybercrime fraud, fraudulent number of people, the complexity of the crime network, resulting in the identification of evidence to add to the difficulties, increasing the difficulty of the work of evidence collection. Different from traditional crime evidence identification, the evidence of cybercrime is usually expressed in the form of electronic information, virtualized data exists, and its immateriality leads to evidence with fickleness, and instability, which can be deleted. To sum up, the complexity of evidence collection and determination is an important issue currently faced.

2.2. Evidence Determination Varies from Country to Country

Transnational cybercrime is wide in scope and deep in harm, so it requires increased cooperation between countries. However, the different recognition of cybercrime and different conviction standards in different countries leads to the variability of transnational crime evidence determination. Usually will face a crime of multiple determinations occurs, and there are no consistent international conviction standards, making cybercrime evidence determination quite flexible. For China to continue to improve the legislation, detailed incrimination standards, fraudulent public, and private property up to 3000 yuan is the amount of the standard of incrimination, in two years the cumulative amount of the standard also constitutes a crime [1]. Reducing the threshold of incrimination makes cybercrime strictly controlled in China; however, in the UK and for impure cybercrime, is still regulated by traditional criminal law [1]. In contrast, we can see that the UK has a milder means of cybercrime governance, and China has a stricter prevention and control of cybercrime, with a lower threshold of incrimination, which means that the identification of evidence is also more stringent. Secondly, the identification of transnational crime evidence is still a problem, due to the principle of territoriality, personal principle, and the protective principle of cybercrime in different countries lead to a certain degree of restriction on the identification of evidence, which leads to different sovereign countries have different stance attitudes towards cybercrime governance, which causes differences in the identification of evidence.

2.3. High Degree of Electronic Evidence

Electronic evidence is developed from computer evidence, also known as electronic data evidence, network data evidence [2]. Nowadays, cyber fraud usually relies on the Internet, text messages, and electronic communication which makes electronic information increase rapidly. For example, cyber fraud uses phishing websites to defraud victims, creating virtual network information to lure victims to click on fake websites; using social networking platforms to deceive victims through chatting to carry out fraudulent acts; or setting Trojan horses to steal victims' personal information to carry out cyber crimes, etc. All of them reflect that electronic technology is an essential foundation in today's

DOI: 10.54254/2753-7048/17/20231214

network fraud methods. In addition, the increasing circulation of electronic money has led to an increase in the flow of third-party electronic trading platforms, in which electronic evidence such as transaction statements and electronic bank details have also become important evidence for the determination of crime and an important criterion for conviction and sentencing of cybercrime. The offender to the victim is close in the electronic data, enough to show that the degree of electronic evidence deepened greatly.

3. Main Evidence Issues in Telecommunications Network Cases

In telecommunications network fraud cases, the collection, examination, and identification of evidence are crucial stages for conviction and sentencing, with their impact on the final judgment being significant. In judicial practice, many contradictions and issues have arisen in the collection, examination, and identification of evidence for the numerous and scattered victims of telecommunications network fraud cases.

3.1. Evidence Collection

Telecommunications network fraud criminals use internet technology to distribute fraudulent information to a large and scattered number of victims, making it extremely difficult for investigating agencies to collect evidence. Furthermore, due to the lack of legal awareness among the victims, many are reluctant to admit to being defrauded for fear of inconvenience, especially in cases involving logging onto pornographic websites and online gambling. In addition, electronic evidence in telecommunications network fraud cases is highly digitized and numerous, making it difficult for law enforcement agencies to obtain evidence and increasing the obstacles to accurate investigation. Moreover, the extraction of electronic evidence in telecommunications network fraud cases requires specialized technology such as data analysis and electronic evidence integrity analysis. However, China's electronic evidence discovery and extraction technology are not yet mature, and there is a lack of specialized technology, equipment, and experience in electronic evidence collection.

3.2. Evidence Examination

In practice, the examination of electronic evidence faces the following issues: First, the examination of the carrier of electronic evidence. Electronic data is carried by a certain medium or carrier, so it is necessary to comply with the legal requirements for the seizure, transfer, and custody of electronic evidence carriers. The original storage medium of electronic evidence must be related to the case to prevent the disqualification of electronic data as evidence due to improper handling of the electronic evidence carrier [3]. Electronic evidence only exists in the original carrier, and once it is destroyed, the integrity and authenticity of the electronic evidence are compromised [4]. At the same time, when electronic evidence is transferred between different carriers, it is difficult to maintain the uniformity of the original data carrier. Second, the examination of the content of electronic data, which is directly related to whether electronic data can be used as evidence. The collection, extraction, and freezing of electronic evidence should follow specific procedures to ensure the authenticity and reliability of electronic data. However, due to the unique nature of electronic evidence, it depends on computers for input, storage, and transmission. It is difficult in practice to determine whether the evidence is original or a copy and whether the copy is identical to the original during transmission.

3.3. Evidence Determination

The process of determining criminal facts through evidence runs through the entire process of criminal proceedings. However, in practice, there are still a series of issues that judicial administrative

DOI: 10.54254/2753-7048/17/20231214

organs encounter in determining certain case facts. First, there are difficulties in determining the principal and accessory offenders. Compared with other types of fraud cases, the responsibility determination of telecommunication network fraud is more complex because the use of virtual environments makes it difficult for a criminal to determine their location, which leads to the inability to use uniform standards in determining joint criminal responsibility. Determining the principal and accessory offenders' position in criminal activity through evidence determination is often a difficult issue for investigating agencies. Second, there are difficulties in determining the amount of fraud. The determination of the amount of fraud is related to the severity of criminal responsibility for the offenders. Due to the use of internet transfers in telecommunication network fraud, which involves multiple victims, fast transaction speeds, and a wide range of impact, it is easy to determine the total amount of a criminal gang, but there is a lack of sufficient evidence to prove the amount of fraud committed by each criminal.

4. Suggestions for Dealing with the Problem of Evidence of Telecommunication Network Fraud

4.1. Improve Chain-of-custody Provisions

Regarding telecommunications network fraud, most of the evidence belongs to electronic evidence. The medium and carrier of electronic evidence are unique. Besides, the original storage medium has the nature of easy to be destroyed, and the data is easy to be tampered with. Therefore, it is necessary to further improve the chain of custody system in China in the following aspects.

First, in the process of evidence collection, transportation may involve some complex technical methods or skills, so the department concerned should set more targeted and professional personnel to carry out the relevant work to reduce potential risks such as loss of evidence. Also, the number must be greater than or equal to two in one particular case. In addition, this kind of custodian should testify in court. If any party challenges the authenticity of the evidence record or the absence of a link in the chain of custody, the custodian related should provide reasonable explanations. In this way, it will not only ensure the authenticity and procedural legality of electronic evidence but also protect the rights of both parties to obtain evidence in their favor.

Second, establish more stringent rules for the custody of evidence. In the process of transporting electronic evidence, the relevant departments should ensure that its medium is in a suitable environment to avoid being affected by something like radio, temperature, and other interference leading to the destruction of data and to make sure that it is "sealed", which means the contents in it can not be tampered with or changed until somebody opens it through legal procedures. There are no specific regulations regarding how electronic evidence should be transported between different departments legally and properly [5]. Thus, more specific and detailed legislation for electronic evidence is needed to regulate the behavior during the flow of this evidence in various departments. For example, the procedures required for the transfer of evidence, each transfer, identification, post-investigation changes, investigator information, time, and other records need to be more uniform and detailed to avoid the destruction or impact on electronic evidence during the necessary "unsealing" process. Third, introduce an evidence labeling system. The current system in China relies excessively on sketchy transcripts to record the information of electronic evidence in various stages, easy to make its way to prove the authenticity and legitimacy of the evidence become a mere formality. The improvement of the labeling system over the existing system is that it can prove the originality and validity of the internal data while ensuring the consistency of the links before and after the examination at the same time. The main functions of labeling are: to prevent confusion among technicians when the evidence is "sealed"; the content, time, status, and person responsible for changes in evidence can reflect in the label. While using physical labels, technical means should be

DOI: 10.54254/2753-7048/17/20231214

actively utilized to set encryption passwords for virtual labels simultaneously to prevent external tampering leading to inaccurate records [6]. “If the chain of custody of evidence breaks at any point, the evidence will likely be inadmissible or lose its legal value”, some scholars have suggested that it needs to be treated strictly to emphasize the legality of the procedures [7]. In conclusion, China has to improve the chain of custody system further to ensure the legality and authenticity of the evidence, especially the electronic evidence, and to reduce the obstacles to the conviction of telecommunication network fraud while protecting the legal rights of the accused.

4.2. Apply Experience Rules to Support Verification Model

Applying Experience Rules in telecommunication network fraud cases has a certain rationality. In the prevailing situation of less direct evidence, the Verification Model is a commonly used mode of proof in the justice of such cases. However, due to the intense subjectivity of the Verification Model, relying only on it can easily lead to wrongful convictions. So, the necessary practice of using Experience Rules can reduce judicial pressure while safeguarding the correct application of the model.

First, The judge should combine Experience Rules with Verification Model when convicts and sentences, for example, in cases involving large amounts of property of unknown origin or the determination of subjective “knowing” in cases with aiders. Because there are too many victims of telecommunications network fraud to trace, it would inevitably waste a large number of judicial resources to corroborate the proceeds of crime one by one. However, denying the proceeds of crime is unreasonable simply because the victims cannot be identified or found. For example, suppose there is only indirect evidence, such as objective transaction flows, account statements, bank account transaction lists, accounting expertise, et cetera, without further relevant proof from the victim or other direct evidence. In that case, it is possible to draw a comprehensive inference that the proceeds from unknown sources are the proceeds of fraud considering the defendant’s income(it is evident that the personal income situation of the defendant would not allow him or her to obtain such a large sum of money in a short period), based on the Experience Rules and generally accepted common sense. In the process of practical application, the vast majority of inferred facts are “rebuttable inferences”, i.e., “an inferred fact is established on the premise that no contrary fact exists, and if a contrary fact presents, the inferred fact is overthrown” [8]. Thus, after the presumption has arisen, the defendant has a certain burden of proof and is obliged to present facts to the contrary to prove that the presumption is not established. Under the principle of the presumption of innocence, the defendant’s burden of proof at this point does not need to be comparable to the standard of the prosecutor’s burden of proof, nor does it require him or her to prove his or her innocence, but only to raise a reasonable doubt in the judge’s mind as to the reliability of the inferred facts, at which point the burden of proof beyond a reasonable doubt once again returns to the prosecutor’s office.

Second, apply Experience Rules to verify whether the use of the Verification Model is reasonable and correct. When the judge uses the Verification Model to prove facts, he or she must combine it with the Experience Rules to ensure its reasonableness and legitimacy and avoid forcing corroboration. When the consistency of the evidence confirms the facts, they should also be challenged by the Experience Rules to prove them beyond reasonable doubt and to meet the standard of proof [9].

Third, the application of sampling determinations. Due to the improved anti-surveillance capabilities of internet fraudsters, Opinions Of The Supreme People’s Court, The Supreme People’s Procuratorate, And The Ministry Of Public Security On Several Issues Concerning The Application Of Law In Handling Criminal Cases Of Telecommunication Network Fraud provides for the inclusion of the frequency of frauds in addition to the proceeds of frauds in the criminalization criteria for telecommunications network frauds. In the absence of evidence, or when it is difficult to identify the number of frauds in the sea of evidence, it is vital to introduce new scientific and statistical methods

DOI: 10.54254/2753-7048/17/20231214

that are appropriate. Many scholars have proposed the method of sample determination, i.e., taking a sample of "X" days, calculating the average number of fraudulent messages sent in a day as "Y," and then calculating the total number of messages based on the duration of the crime that can be determined for "Z" days, so as to determine whether it constitutes an attempted telecommunication network fraud (total=Y*Z). This approach has a relatively well-developed operational model and technical specifications in statistics and can therefore be directly applied [10]. However, the relevant conditions should also be met when applying. Firstly, sampling determinations can only be applied when it is difficult to collect evidence, such as the number of calls made or messages sent, or when it is inconvenient to determine in the face of a large amount of evidence. To a large extent, criminal sampling is a compromise in the face of difficulties in proving [11]. Second, the subject of identification needs to be professional. Sample determination belongs to statistical methods and is not objective and direct evidence. What's more, the results of the determination are inferences, which require experts to use professional knowledge and scientific identification. It is worth noting that in the transfer of evidence, the process should also comply with the chain of custody system requirements mentioned above. Finally, a combination of the Verification Model and sampling methods should be used to ensure that the results of sample determinations and more in line with reality. The data used in a sample determination must be derived from real, objective evidence, and where time is difficult to ascertain, consideration may be given to corroborating statements provided by the perpetrator with existing evidence (e.g., the earliest available records of the fraudulent transfers) to arrive at a reasonable total time. Of course, it cannot be ruled out that some criminal groups also have rest days, in which case the rest days should be subtracted from the determination of the time, depending on the circumstances. The purpose of sampling is to save judicial resources while reasonably applying the evidence to bring out a result that is infinitely closer to the truth rather than to create a new, abstract, or doubtful fact. Therefore the result should be fully explained and reasoned scientifically when applied.

Whether the Experience Rules or the Verification model is applied, it is not the traditional simple use of direct pointing facts to prove a crime, so this method of proof requires a higher level of literacy on the part of the judge to avoid wrongful application leading to wrongful convictions.

4.3. Scientific and Comprehensive Identification of Accomplice Association Evidence and Crime Amount in Joint Crimes

First, the clarification of laws and regulations and judicial interpretation. In the joint crime of telecommunication network fraud, the determination of the principal and accomplice should be strictly by the law. The Opinions of the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security on Several Issues Concerning the Application of Law in Handling Criminal Cases of Telecommunication Network Fraud, and the Opinions of the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security on Several Issues Concerning the Application of Law in Handling Criminal Cases of Telecommunication Network Fraud (II) (hereinafter referred to as Opinion II) all mention relatively specific circumstances of being an accessory, but there are still imperfections. For example, the provisions of Opinions II for accomplices "especially those who have participated for a relatively short period, have a relatively low amount of fraud or are engaged in auxiliary work and receive a small amount of remuneration ....." do not indicate the relatively short period and relatively low amount of remuneration. , the length and amount of a small amount of remuneration. Therefore, it is still a difficult problem to be solved in judicial practice whether the criminals in the fraudulent group should be considered accomplices or principals for sending SMS, making phone calls, and taking commission or receiving salary from them. Therefore, to improve the judicial interpretation, establish a systematic, comprehensive, and unified standard, such as the specific time of participation, the specific amount of a small amount of

DOI: 10.54254/2753-7048/17/20231214

compensation, what behavior can be considered as an accessory and other circumstances can be considered as an accessory, which is conducive to the judicial practice of judges to better apply the law and reduce the impact of subjective factors on the characterization of the principal and accessory.

Second, the scientific and comprehensive determination of the amount of the crime of the accomplice in the accomplice. After being identified as an accessory, the amount of the crime cannot be directly determined by the total amount of the crime of the fraudulent group or by the amount of the criminal liability that should be paid, otherwise, it is contrary to the principle of compatibility of crime and punishment. In judicial practice, some judges have joined the fraudulent gang as the starting point, the time after the gang of all fraudulent proceeds identified as the proceeds of crime, is also unreasonable. For example, in the Wen Yanyan and Yin Yin fraud case ((2020) Chuan Criminal Final No. 173), the location of the fraudulent gang involved in Cambodia, the original judgment in the first trial, the above method, calculated and found that one of the defendant's accomplice Yin involved in the amount of up to more than 1.5 million, and the second trial review found that Yin was not in Cambodia in about half a month, can not participate in any period of fraudulent activities, re-identified, the case involved The difference of $600,000 has a significant impact on sentencing, so the simple use of time and the number of fraudulent profits to determine the culpability of an accomplice is a wrong presumption, and judges must strictly adhere to the requirement of "sufficient evidence and facts" when using evidence and experience. The ideal method of determining the amount should be through the victim's confession, the victim's transfer records, chat records, as well as the accomplice's participation in the fraud evidence (transfer records, chat records, call records, punch cards, work content, etc.), the pattern of mutual corroboration between the accomplice's criminal proceeds, and then according to the provisions of the law on mitigating punishment comprehensive consideration of the length of sentence. The evidence here should be directly related to the accomplice, and the role of the accomplice should also be directly related to the amount of duty that can prove his crime. Of course, due to the difficulty of evidence collection in most cases, the number of victims can not be corroborated one by one, and the victim's verbal evidence is not completely reliable, the feasibility of the application of this method of determining the amount is low. Therefore, in practice, it is necessary to scientifically and comprehensively determine the amount of the crime of the accomplice. In the case of less evidence, the amount of fraud and personal income of the accomplice should be confirmed by the above-mentioned corroboration methods and rules of thumb, and the size of the role of the accomplice and the degree of subjective malice should be judged. The process of confirmation should be combined with the standard of sufficient evidence, the principle of favoring the defendant, and the judicial rules such as the benefit of the doubt, to make an accurate determination of the scope of the defendant's culpability [12]. In this way, the circumstances of the crime of the accessory can be more accurately determined, and the sentencing is more scientific and reasonable.

5. Conclusion

Currently, telecommunications network fraud is growing and still evolving. The highly electronic nature of its evidence has made it significantly more difficult to collect evidence in judicial practice. It has to rely heavily on verbal evidence as a basis for conviction and sentencing. By examining the chain of custody system in foreign countries, the application of the Verification Model and Experience Rules in China, and the issue of complicity, this article provides three points of view on the impact of evidence on judicial practice to more effectively protect people's property rights, punish fraudsters and combat rampant telecommunication network fraud. In the judicial practice of this type of crime, the general application of the Verification Model and the use of the Experience Rules in combination require a high level of knowledge for judges, so there is still a need for more in-depth research on the evidence, such as the development and application of relevant high-tech products to

DOI: 10.54254/2753-7048/17/20231214

reduce the difficulty of proof and ensure the credibility of the judiciary, and the protection of the fundamental rights of the victims and the basic human rights of the defendants.

References

[1] *Li, Y., & Qi, P. (2022). Research on International Cooperation in Combating Cross Border Telecom Network Fraud Crimes. Journal of Shandong Police Academy, No.34(03), 113-123.*

[2] *Li, Q. (2022). Research on Electronic Forensics in Telecommunication Network Fraud Cases. Police Research, 06, 52-57.*

[3] *Zhi, J. (2022). Research on the Issue of Evidence in Telecom Network Fraud Cases. Journal of Law Application. Journal of Law Application, No.486(09), 168–176.*

[4] *Zhao, H., Huang, X., & Li, X. (2022). Research on the Authenticity of Electronic Evidence in Criminal Proceedings. Journal of Shandong Police College, 34(04), 120–124.*

[5] *Peng, H. (2022). Research on Rules for the Review and Judgement of Electronic Evidence in Criminal Proceedings. Central China Normal University.*

[6] *Kong, X. (2018). Research on the Authentication Rules of Real Evidence ——Based on the Existing Problems in the System of the Chain of Evidence Custody. East China University of Political Science and Law.*

[7] *K. Lee Lerner & Brenda Wilmoth Lerner(eds.), World of Forensic Science, Kentucky: Gale, 2005, p.548.*

[8] *Chen, R. (2015). On The Presumption In Criminal Law. Law Science, 05, 105–116.*

[9] *Long, Z. (2021). Issues in the Application of the Experience Rules in Criminal Proof. Chinese Criminal Science, 05, 55–70.*

[10] *Li, L. (2022). Research on Rules for Determining the Number of Crimes in Telecommunications Network Fraud Cases. Southwestern University of Finance and Economics.*

[11] *Yang, F. (2019). Rule of Law Responses to Criminal Sampling in the Context of Massive Evidence. Law Review, 37(05), 105–112.*

[12] *Wu, C. (2017). Discussion of Difficult Issues in Telecommunication Network Fraud Cases. Legal Application, 21, 40–50.*