ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202410_7(10).0028

The Empirical Research on the Identification of Telecommunication Network Fraud Crime

Jiayue Jia

School of Law, People's Public Security University of China, Beijing, China

Abstract

Telecommunication network fraud crime is a new type of fraud crime which is different from traditional fraud crime. It mainly uses non-contact methods to defraud unspecified objects, and constantly updates the fraudulent means with the help of information dissemination tools and new payment channels, which brings difficulties to the accurate identification of such crimes in judicial practice. Based on the particularity of telecommunication network fraud crime, in order to effectively solve its problems in judicial practice. First of all, through the concept, characteristics and manifestation types of telecommunication network fraud crime, this paper expounds the telecommunication network fraud crime from the legal point of view. Secondly, from the legal status quo of telecommunication network fraud crime, the identification problems existing in judicial practice and their causes, it is pointed out that the problems existing in telecommunication network fraud crime in judicial practice are mainly manifested in the difficulty in accurately identifying the crime amount, the difficulty in accurately identifying the attempted form, the difficulty in distinguishing the principal and accessory offenders, and the difficulty in characterizing the charges of related crimes; The identification of telecommunication network fraud crime is sorted out, and it is pointed out that the main reasons are the scattered existing legal provisions, different legal interests and different judicial cognition of judges. In view of this, making telecommunication network fraud a crime independently is the primary system improvement path to solve the differences in the determination of telecommunication network fraud crime.

Keywords

Telecommunication Network Fraud Crime; Cybercrime; Legal Identification; Independent Criminalization.

1. Telecommunication Network Fraud Crime

The development and progress of science and technology has brought great convenience to people's work and life. People can realize various transactions, obtain or publish various types of information through the Internet, and at the same time, it has also brought about an endless phenomenon of cybercrime. Telecom network fraud is a new form of crime combining traditional fraud crimes with modern network information technology. Such crimes have novel behaviors, diverse means, strong concealment and high deception. There are also many problems in judicial practice. Whether the telecommunication network fraud crime constitutes a crime of fraud in criminal law needs to be further distinguished. In practice, telecommunication network crimes with a “deceptive” shape are often identified as fraud crimes, and this approach needs further discussion. In addition, in practice, there are different approaches to whether professional cashiers constitute an accomplice in the crime of fraud. There are also special groups that provide help behaviors, and the characterization of their behaviors is not completely consistent. This article makes an in-depth analysis and analysis of the above issues.

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202410_7(10).0028

As a new type of fraud crime, telecommunication network fraud crime is not much different from the traditional fraud crime in content, and its difference is mainly manifested in the external manifestations, that is, it is implemented in a flexible form by means of telecommunication network communication and remote operation. Although the traditional crime of fraud is clearly defined in China's current criminal law system, due to the high incidence of telecommunication network fraud in recent years, it was not until December 2016 that the Supreme People's Procuratorate, the Supreme Law and the Opinions on Several Issues Concerning the Application of Laws in Criminal Cases such as Telecommunication Network Fraud (hereinafter referred to as "Opinions") gave corresponding applicable standards for relevant judicial determinations such as conviction, sentencing and punishment suggestions. In recent years, academic circles have defined its concept from various angles. Some scholars believe that the crime of online fraud includes pure online fraud and impure online fraud. The former means that criminal acts can only be realized through the internet, while the latter regards the internet as an unnecessary way to realize their criminal acts. Another point of view regards the crime of online fraud as a new type of fraud that uses the technical characteristics of the network as a criminal tool.

To sum up, this crime can be defined as a crime of illegally occupying other people's property, using telecommunication network as a crime tool, and infringing on other people's property by fabricating facts and concealing the truth. Although there are many forms and means of this crime at present, there are some similarities in the crime patterns. Mainly manifested in the premise of collecting citizens' personal information, carefully planning the fraud scheme, touching the target group with the help of telecommunication network, and implementing fraud with the pre-set scheme, and then extracting and transferring the stolen money by special personnel.

2. The Characteristics of Telecommunication Network Fraud Crime

2.1. The Criminal Subject is Divided into Industrial Chains

Summarizing the telecommunication network fraud cases exposed by the media and the trials of such cases, we can find that telecommunication network fraud gangs are characterized by networked organizational structure, cross-regional crime and professional criminal behavior, and obviously show the trend of scale and collectivization. Moreover, different fraud gangs assume different roles internally, and the refined division of labor makes them show obvious professional characteristics in all aspects such as making calls, transferring money and setting up platforms. For example, telecommunication network fraud needs network experts, so it is necessary to crack the network technology through hackers to find and steal the needed information; Online fraud requires not only applying for domain names, making web pages, updating pages, technical maintenance, etc., but also avoiding supervision and control, which also requires people with special skills to operate. In addition, mobile phone cards and bank cards used for telecommunication network fraud also need to be familiar with such people who handle business; In order to gain the trust of the victim, it is more necessary for people who understand the victim's psychology to design fraud schemes; And after the fraud is successful, how to successfully withdraw money while avoiding investigation also needs the assistance of people with certain anti-investigation means.

In specific fraud cases, except for senior partners, other auxiliary work is carried out by several sub-gangs with clear division of labor, which are responsible for telephone calls, transfer, withdrawal, money laundering, provision of crime tools, technical support and so on. Taking the case of Dai Chunbo as an example, according to the facts explained by Dai Chunbo in court, in the process of fraud, like other defendants, he has never seen a real boss, who is responsible for making calls to unspecified people. Firstly, it establishes a fraud platform through

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202410_7(10).0028

outsourcing, then finds someone to plan the fraud scheme, then induces it by the telephone group, and finally withdraws money through various channels. During the period, the organizational relationship between the various parts was subordinate or parallel, and they were relatively independent and unfamiliar with each other. Even the members of the sub-gang did not know the real names of others who worked with them, and they were more in single-line task command contact through the network or mobile phone. Therefore, in the whole criminal process, the organizational division of labor within criminals is extremely clear, and the criminal subject presents industrial chain division of labor.

2.2. Criminal Means Mainly Rely on Gigh Technology

In the crime of telecommunication network fraud, almost all of them are carried out by professional technicians around the high technology of communication industry, financial industry and network, and the methods of committing crimes are constantly changed to avoid the blow. For example, in overseas telecom network fraud, criminals mostly use local anonymous mobile phone numbers, and most of them do not display the numbers, thus committing fraud on the mainland, making it impossible to start the arrest process, and even the investigation of this case has no clue; Another example is that with the advent of the era of electronic payment, the forms of the outflow end of criminal money are becoming more and more diverse, including the use of other people's bank card transfer, POS machine transfer, ATM machine cash withdrawal and other forms, and more are cross-used, showing the characteristics of fast and multi-level; In addition, fraud gangs are mostly conducted by means of single-line contact, telephone manipulation, cross-regional crimes, etc., so the criminals caught are often at the end of the criminal gang chain, which makes it difficult to effectively crack down on senior partners and recover the proceeds of crime.

Take the case of fraud, cover-up and concealment of criminal proceeds by Wang and others as an example. The defendant used the identity of employees of Shanghai Oriental Collection Company and Hongsheng Auction Company to get in touch with the defendant by using the network virtual number telephone and special crime mobile phone, and then forged a series of relevant certificates, pretending the handicrafts purchased at a low price to be collectibles to defraud the victim. By taking advantage of people's reasonable trust in authoritative organizations, a series of forged related documents are even more indistinguishable.

2.3. The Mode of Crime is Non-contact.

The non-contact nature of criminal methods is mainly manifested in radiation, immediacy and cross-region. The rapid development of the Internet has expanded the society from the original "point-to-point" communication mode to "point to face" and "face to face". Radiation is spreading around with the actor as the center, which makes the object of its infringement very uncertain and the consequences of its infringement very superimposed. Instantaneity is completed by the instantaneous spread of information technology, breaking the time barrier.

Cross-regionality breaks the space limitation, making the scope of fraud no longer limited to a certain area. This is because telecommunication network fraud mainly starts with network data and information to commit fraud crimes. For example, criminals take advantage of the defects in real-name registration of internet and mobile phone numbers, and use temporarily registered websites and mobile phone numbers under the guise of other people's identity. This kind of fraudulent crime in a non-contact way under the guise of other people's identity information is highly concealed, which not only leads to the victims' irreparable losses, but also brings certain difficulties to judicial investigation. And because the fraud mode has changed from the fraudulent end to the deceived end, that is, criminal gangs buy a large number of detailed information of specific groups from specialized institutions in advance, and then implement targeted and accurate fraud. Even when committing a crime, the victim's name, nickname, recent situation, latest situation and other relative personal privacy closely related

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202410_7(10).0028

to the victim are pointed out to enhance the trust of the victim, so that the victim can relax his vigilance and improve the success rate of the crime. Take Wang Zhikun and other fraud cases as an example, they conduct stock investment and financial management by purchasing domain names, copying business licenses, organization code certificates, tax registration certificates, account opening licenses, and purchasing customer service telephones. This way of committing crimes is to make the victim's vigilance to a minimum by packaging his behavior, using false websites and customer service numbers, and using the convincing power of government agencies.

3. The Analysis of the Reasons for the Differences in the Identification of Telecommunication Network Fraud Crimes

Telecommunication network fraud is significantly different from traditional fraud, and the reasons for the identification differences should be analyzed from a different perspective from traditional fraud. At present, the organizational form and behavioral characteristics of telecommunication network fraud have impacted and challenged the traditional elements of fraud crime, which has led to differences in the determination of telecommunication network fraud crime by judicial personnel.

3.1. Reasons for Differences in the Determination of Charges

Traditionally, a crime is a crime in the sense of criminal law only if the conditions stipulated in criminal law are met. However, telecommunication network fraud has different manifestations from traditional crimes, which leads to the identification of this crime and that crime. Taking the crime of fraud as an example, property loss is the only incriminating standard of traditional fraud. However, due to the non-contact nature of telecommunication network fraud, the definition of property is different from that of traditional fraud, which makes it difficult to identify the charges. The property involved in telecommunication network fraud crime can be virtualized as data or graphics and commands existing in computer data carriers, that is, the property in this sense can exist in the form of electronic data instead of entities. Therefore, telecommunication network fraud crimes may not cause property losses in the connotation of traditional fraud crimes, such as electronic money, virtual money, bitcoin and other forms of property are difficult to be included in the category of traditional property. This makes it easy for judicial personnel to get into trouble when choosing crimes: on the one hand, there is no clear theoretical basis for judging telecommunication network fraud as fraud, but it depends on judicial personnel's discretion; On the other hand, some crimes committed by using blockchain may not be suitable for fraud, but can be identified as other crimes such as concealing or concealing the proceeds of crime, or infringing citizens' personal information. In practice, the analysis of the constitutive elements of crime should follow the principle of unity of subjective and objective. To identify the crime of telecommunication network fraud, it is necessary to link the objective behavior of the perpetrator with his subjective cognition and subjective will, which increases the difficulty of judicial identification.

3.2. The Reasons for the Differences between the Principal and The Accessory in Subjective Intention and Joint Crime

Generally speaking, members of traditional criminal organizations have a relatively unified understanding of each other's socially harmful behaviors and results through daily communication and exchange, while members of telecommunication network fraud criminal organizations perform their respective duties, are anonymous to each other and are distributed in different spaces. Due to the limitation of physical space, they don't know much about the operation of other links, which leads to the subjective intention of the actors and the differences between the principal and the accessory in joint crime.

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202410_7(10).0028

It is difficult to identify the subjective intention of the accomplice in the crime of helping information network crime and fraud. Judging from the collected cases, before 2019, most of the aiding criminals in telecommunication network fraud crimes were identified as accomplices of fraud, but the number of crimes identified as aiding information network criminal activities increased sharply. In 2019, the National People's Congress and the National People's Congress issued the Interpretation on Several Issues Concerning the Application of Laws to the Crime of Illegal Use of Information Network and Helping Information Network Crimes, in order to help the crime of information network crimes to identify the related organizations of telecommunication network fraud crimes. However, the situation in practice is quite complicated, and how to identify the "knowing" of the crime of helping information network crimes is still a difficult problem. The legislative purpose of the crime of helping information network crime is to solve the problem of specialization and industrial chain of the help behavior of telecommunication network fraud crime. Criminals don't know each other. If we want to deal with it as an accomplice of fraud crime, we generally need to find out the joint criminal intention of the helper. However, people in different links of cyber crime often don't know each other, and there is no clear connection of criminal intent, so its subjective intention is difficult to identify.

In the telecommunication network fraud group, it is difficult to distinguish the principal from the accessory. China's criminal law theory is divided into principal and accessory according to the status and function of joint criminals, but in the telecommunication network fraud crime with dual chain structure, its members only complete the tasks on their respective chain nodes, in other words, the whole criminal process is composed of nodes on the criminal chain. For example, among the members involved in the same telecommunication network fraud crime, some are responsible for contacting the behavior object, some are responsible for logistics work, and some are responsible for managing daily accommodation. In this case, although the members play different roles in the crime, they are all indispensable, so it is difficult to distinguish their respective roles in telecommunication network fraud.

3.3. The Reasons for the Differences between One Crime and Several Crimes and Between Accomplished and Attempted Crimes.

Generally speaking, the legal interests of traditional crimes in China are relatively simple. Telecommunication network fraud is a chain of organizational forms, and its criminal object is a complex object, which leads to the identification of one crime and several crimes, as well as accomplished and attempted crimes.

There are differences between one crime and several crimes. Telecommunication network fraud is not enough to be identified by a single crime, but it is difficult to judge it in judicial practice, which leads to differences in the identification of one crime and several crimes. Judging from the overall situation of the judgment documents, it is difficult for the judges to measure the diversity of the objects infringed by the telecommunication network fraud crime. By combing the legal interests infringed in these cases, it is found that the legal interests infringed by telecommunication network fraud crimes include public and private property ownership, personal information security, public information security and so on. Therefore, the academic circles have discussed the types, quantity and degree of infringement of legal interests. Some scholars believe that telecommunication network fraud not only violates the ownership of public and private property, but also may violate citizens' personal information security, information network management order, financial management order and normal business order, which are not possessed by traditional fraud crimes; Judging from the harmfulness and influence of the objects it infringes, the violation of network management order bears the brunt, because even if the act of defrauding money is attempted, the act of destroying network management order has been accomplished. Some scholars believe that

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202410_7(10).0028

telecommunication network fraud not only infringes on citizens' property legal interests, but also poses a serious threat to citizens' information legal interests, and divides it into information security legal interests, information environmental legal interests and information resources legal interests. For example, the case of He Moule and Rao Mou mentioned above involves a variety of criminal objects, and there are differences on whether to be convicted and punished according to the crime of fraud or whether the crime of fraud is combined with the crime of obstructing credit card management.

It is difficult to judge accomplished and attempted. With regard to the determination of accomplished and attempted telecommunication network fraud, some scholars believe that "telecommunication network fraud crime should be regarded as a behavioral crime, marked by the successful sending of fraudulent information. If the perpetrator successfully sends fraudulent information to an unspecified majority, it will be regarded as a crime accomplished; If the perpetrator fails to successfully send fraudulent information for reasons other than his will, it will be regarded as an attempted crime. " This is based on whether the unilateral sending of information is completed, and it is considered that fraudsters can achieve fraud without contacting the victim. However, some scholars have suggested that "if the evidence shows that the victim's money is directly transferred to the bank card and payment code account provided by the perpetrator, at this time, the victim is disposing of the property under the deception of the upstream criminals, and the crime has not yet been completed. When the victim's money enters the bank card and payment code account provided by the perpetrator, the crime will be completed", that is, the transfer of money is a process, and it is not when the victim unilaterally transfers the money to the account provided by the perpetrator that all the money has entered the perpetrator. It can be seen that the non-contact influence of telecommunication network fraud on the judgment of accomplished and attempted crimes has not yet reached a consensus in the academic circles on the judgment criteria of accomplished and attempted crimes.

4. Telecommunication Network Fraud Should Be Independently Criminalized.

At present, telecommunication network fraud is still a crime with a high incidence rate in China. With the blessing of network information technology, its unique organizational form leads to many differences in the determination of telecommunication network fraud crime by judicial personnel, which makes the traditional judicial governance seem stretched. In order to crack down on telecommunication network fraud, both academic and practical circles have called for making telecommunication network fraud an independent crime. The author believes that this approach is both necessary and feasible.

4.1. The Views of Telecommunication Network Fraud that Controversy

In the context of traditional fraud crime, the criminal law practitioners and theorists in China have long identified telecommunication network fraud crime as fraud crime. Some scholars believe that the particularity of telecommunication network fraud can be solved through the interpretation of criminal law, and this particularity is not the reason why criminal law must be legislated. [12] Some scholars believe that the telecommunication network fraud crime belongs to the traditional crime of being networked, and it does not belong to the crime born with the network itself, but is a traditional crime that uses the network as a criminal tool or is implemented in cyberspace. If all crimes committed by means of telecommunication network technology are included in special cyber crimes, the scope of cyber crimes will be endless. Because of the structural conflict between telecommunication network fraud crime and traditional crime, the traditional identification method is far from enough to solve the problem of telecommunication network fraud crime. Another part of scholars support making telecommunication network fraud a separate crime. Some scholars believe that based on the

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202410_7(10).0028

scientific criminal legislation, the needs of criminal policy and the needs of judicial practice, it is necessary and feasible to make telecommunication network fraud a separate crime. Some scholars believe that telecommunication network fraud cannot be evaluated accurately and completely based on the existing charges, and telecommunication network fraud should be criminalized separately in our criminal law. [15] In terms of system classification, some scholars believe that under the current criminal law system, the crime of telecommunication network fraud should be incorporated into the crime of disturbing public order in the crime of disturbing social management order. However, this will lead to the reduction of the legal interest in protecting citizens' property. Most scholars believe that the crime of telecommunication network fraud should be classified as property crime according to the existing criminal law system, and the amendment model should be stipulated as one or a separate article of Article 266 of China's Criminal Law.

The dispute between the above two viewpoints stems from the fact that telecommunication network fraud crime has many characteristics different from traditional crime, which has a strong impact on the composition of traditional crime. In fact, the crime of telecommunication network fraud is not a special crime in criminal law, but a collection of crimes. As early as 2012, some scholars suggested that the crime of telecom fraud should be added because of its particularity different from that of ordinary fraud. This is a symbolic turn in the thinking of identifying telecommunication network fraud crime.

4.2. The Necessity and Feasibility of Independent Criminalization of Telecommunication Network Fraud

The necessity of independent criminalization of telecommunication network fraud. First, the traditional crime of fraud cannot regulate all telecommunication network fraud. Specifically, although the telecommunication network fraud crime evolved from the traditional fraud, it is similar to the traditional fraud on the surface, but the telecommunication network fraud crime presents a binary chain-like organizational form, and its criminal elements break through the behavior mode of the traditional crime, which is essentially different from the traditional fraud. Second, it is very complicated to identify telecommunication network fraud crime in practice. Opinions on Handling Telecommunication Fraud (I) stipulates: "If it is really impossible to collect the victim statements one by one due to the limitation of objective conditions such as the large number of victims, the criminal facts such as the number of victims and the amount of fraudulent funds can be comprehensively determined by combining the collected victim statements, verified bank account transaction records, third-party payment settlement account transaction records, telephone records and electronic data." It shows that the current judicial personnel take a comprehensive approach to the crime of telecommunication network fraud, which has greater discretion. According to the judicial department, there are still a large number of telecommunication network fraud crimes that cannot be applied according to the existing laws and regulations. Many judicial personnel expect the Supreme People's Court and the Supreme People's Procuratorate to issue judicial interpretations. However, the situation of telecommunication network fraud crimes in each region is different. Even if the judicial interpretation is issued by the "two high schools and one department", the specific situation of all regions cannot be taken into account, and the judicial interpretation cannot achieve a unified and standardized effect. From this point of view, the interpretation of criminal law can not solve the current differences in the identification of telecommunication network fraud crimes, and can not fundamentally solve its identification problems.

The feasibility of independent criminalization of telecommunication network fraud. From the perspective of criminal policy to prevent the risk of telecommunication network fraud, the state has responded to telecommunication network fraud to varying degrees one after another. For example, Opinions on Handling Telecommunication Network Fraud (I) in 2016, Notice on

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202410_7(10).0028

Strengthening Publicity and Education Activities for the Elderly to Prevent Telecommunication Network Fraud in 2017, Guidelines for Procuratorial Organs to Handle Telecommunication Network Fraud Cases in 2018, 10 Typical Cases of Telecommunication Network Fraud Crimes in 2019, and Notice on Severely Cracking down on Cross-border Gambling and Telecommunication Network Fraud Crimes during the COVID-19 Epidemic in 2020, In 2021, "Opinions on Several Issues Concerning the Application of Laws in Handling Criminal Cases such as Telecommunication Network Fraud (II)" and so on, gradually highlighted the criminal policy of the state to crack down on telecommunication network fraud crimes. However, the above provisions are not strictly legal, and the crime of telecommunication network fraud is still facing many difficulties in judicial practice. Therefore, based on the grim situation of telecommunication network fraud crime, the legal interests of criminal law can be protected in advance by stipulating telecommunication network fraud crime as an independent crime, which is more feasible to solve the problem of telecommunication network fraud crime identification. How to systematically determine the conviction and sentencing standard of telecommunication network fraud crime is also a realistic challenge. The author believes that we can improve the realization path of independent conviction of telecommunication network fraud from the following two aspects. First, measure the rank of infringement of legal interests. Although the crime of telecommunication network fraud has developed from the crime of fraud, and the ownership of public and private property is the most direct and main infringement of legal interests, with the continuous development of telecommunication and network technology, the legal interests of network security and information will be highlighted for a long time to come, which requires an accurate grasp of the order of infringement of legal interests. Second, further explore the attribution of charges. As mentioned above, there is a cross relationship between telecommunication network fraud crime and traditional fraud crime. On the basis of measuring the infringement of legal interests, it is necessary to clarify the attribution of telecommunication network fraud crime, so as to further refine the relationship between telecommunication network fraud crime and its related crimes.

5. Summary

The differences in the identification of telecommunication network fraud crime are the key problems to be solved urgently in the judicial governance of telecommunication network fraud crime. Although the relevant departments in China have issued laws and regulations to explain and respond to this in succession from 2011 to 2021, there is no special law to stipulate telecommunication network fraud crime, and the legal provisions on the identification of telecommunication network fraud crime are not high. The telecommunication network fraud crime is essentially different from the traditional crime. We should distinguish the telecommunication network fraud crime from the traditional crime instead of the traditional crime thinking, so as to effectively deal with the identification problems of this crime and that crime, one crime and several crimes in the trial process. In this sense, the author agrees to make telecommunication network fraud a crime independently, hoping to bring further thinking and discussion.

References

[1] Xiang C ,Li J ,Xiao X , et al.Empirical Research on the High Incidence of Crime of Assisting Information Network Criminal Activities in Telecommunication Fraud Cases Based on 26, 121 Judgment Documents[J].Science of Law Journal,2024,3(4).

[2] Yan J ,Xu X ,Zhang K .Research on Evidence Issues in Telecommunications Network Fraud Cases[C]//Sam Houston State University, Faculty of Business, Law and Social Sciences, Birmingham

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202410_7(10).0028

City University,Northumbria University.Proceedings of the 4th International Conference on Educational Innovation and Philosophical Inquiries(part6).Department of Social Sciences and Humanities, North China Electric Power University;College of Humanities and Law,Henan Agricultural University;Department of Economy,Shanghai University of Political Science and Law;,2023:8.DOI:10.26914/c.cnkihy.2023.106613.

[3] Du X .Research on improving the quality and efficiency of interrogation in telecommunication network fraud cases[J].International Journal of Frontiers in Sociology,2023,5(1).

[4] LanY,QiyanC ,SixinL .Study on International Cooperation to Address Cross-border Telecommunication Network Fraud Offence[J].Journal of Politics and Law,2024,17(2):51-51.

[5] Peifeng N ,Quanxiu W .Internet and Telecommunication Fraud Prevention Analysis based on Deep Learning[J].Applied Artificial Intelligence,2022,36(1).

[6] Aijiao L ,Jie Q .The Formation and Prevention Path of Telecommunication Fraud Crime1[J].Journal of Asia Social Science,2022,Vol.6 No.2(2).

[7] Hanrui G .The Dilemma of Telecommunication Fraud Crime--An Analysis of China's Governance Model as a Sample[J].SHS Web of Conferences,2022,148.

[8] Aijiao L ,Jie Q .The Formation and Prevention Path of Telecommunication Fraud Crime1[J].Journal of Asia Social Science,2022,Vol.6 No.2(2).

[9] Amin M M ,Mohamed M A ,A Z , et al.Detecting Telecommunication Fraud with Visual Analytics: A Review[J].IOP Conference Series: Materials Science and Engineering,2020,884(1):012059-.

[10] Qianqian Z ,Kai C ,Tongxin L , et al.Detecting telecommunication fraud by understanding the contents of a call[J].Cybersecurity,2018,1(1):1-12.

[11] Zhangliao X ,Xisong M ,Huanyu W , et al.Research on Measures of Prevention Against Network Telecommunication Fraud in a University[C]//,2022.

[12] Wu B ,Li M ,Zhou C .Application of Adaboost Algorithm and Immune Algorithm in Telecommunication Fraud Detection[C]//Wuhan Zhicheng Times Cultural Development Co., Ltd.P roceedings of 2018 International Conference on Network, Communication, Computer Engineering (NCCE 2018).School of Communication University of China;,2018:5.