The Research on the Identification of Accomplice Liability in Telecommunications Network Fraud Crimes

Liu Xiao and Ming-Hsun Hsieh
Krirk University, Thailand
Corresponding Author, E-mail: vance11166516@gmail.com

****

Abstract

As a new type of criminal method, telecommunications network fraud is developing rapidly and has a serious impact on people's lives and property security. This type of crime relies on network science and technology, affects a wide range, defrauds victims of large amounts of money, and is highly harmful to society. Due to its strict organizational structure, clear management levels, and large number of participants, it is difficult to convict and sentence the perpetrators in the joint crime of telecommunications network fraud. From the perspective of common crime, this article summarizes and defines the common crime of telecommunications network fraud, and analyzes its characteristics. Telecom network fraud is basically committed as a joint crime, and its accomplice structure is complex. It needs to be analyzed from the perspective of the joint criminal organization form, and the liability of the accomplice is determined accordingly.

It was found that the content of judicial interpretations has certain limitations, making it difficult to systematically identify the emerging common crimes of telecommunications and network fraud, and sometimes it is difficult to clarify its legal principles. This article provides a comprehensive perspective on the study of accomplice liability in telecommunications network fraud crimes, covering the characteristics of the crime, the form of joint crime, the legal basis, and its challenges and problems in judicial practice.

Keywords: Telecommunications Fraud; Joint Crime; Liability Determination

Introduction

With the rapid development of technology, telecom network fraud is also constantly evolving and upgrading, shifting from traditional methods to online fraud. According to big data from the court, the proportion of telecommunications network fraud is gradually decreasing, but the activities of criminals have also changed, from traditional communication methods such as phone calls and text messages in the past to network services such as social networking sites and instant messaging (Zhang et al., 2021). In recent years, the proportion of online fraud has increased significantly and has exceeded 60% (Li & Wang, 2022). According to the data analysis of related fraud cases, the most common means of contact and communication when conducting fraud activities are QQ and WeChat. Fraud cases using these two contact methods accounted for 73.8% and 24% of all fraud cases, respectively (Chen & Liu, 2023). Overall, telecommunications network fraud is still a serious problem. Especially in recent years, Internet crime has developed rapidly and has become the biggest threat to the security of public property. The rapid development of the Internet and mobile phone communications has caused China's cybercrime to grow at an annual rate of approximately 30%, accounting for one-third of the country's total crimes, making it the most important

*Received: May 8 2027; Revised: May 28 2024; Accepted: May 29 2024

criminal behavior in the world (Wang et al., 2022). According to a survey by the China Judicial Big Data Center, fraud crimes account for the largest proportion of all illegal activities, exceeding 30%, and are still growing (Xu & Zhao, 2021).

At present, telecommunications network fraud is no longer an individual behavior but has gradually become an organized and disciplined group crime. Even different members have participated in the fraud gang at different times, and the specific division of labor in the criminal group is also different. Therefore, when judging the amount of fraud and the responsibility of each member, it is necessary to analyze the specific situation and cannot generalize. It also causes certain difficulties in determining the liability of accomplices in telecommunications network fraud in current judicial practice. The upstream and downstream illegal activities of telecommunications network fraud, such as the trading of personal information, the helping behavior of platform operators, the sale or fraudulent use of bank cards for subsequent withdrawals, etc., also need to be discussed in detail in terms of specific applicable laws.

This means that in the trial process of telecommunications network fraud cases, the role of "accomplice" is extremely important but difficult to determine. In fact, telecommunications network fraud criminal groups have a wide range of coverage, and one telecommunications network fraud incident may be associated with multiple people. However, due to various factors such as the amount limit and the concealment of contact methods in the process of telecommunications network fraud, some of the people involved in the case cannot be sentenced, and it is not clear whether many of the people involved in the case can be judged as accomplices. The first paragraph of Article 25 of the "Criminal Law" (Gao & Chang, 2016) stipulates that "two or three or more people are accomplices". According to the general theoretical proposition, an accomplice must meet three conditions at the same time. First, the practitioners must be two or more individuals. Secondly, the perpetrators must form a common criminal intent. Finally, there must be a connection of interest between the practitioners. However, compared with ordinary crimes, telecommunications network fraud crimes have more hidden intentions and contact methods. The various steps in the overall criminal process are more complex. Hired criminals often focus only on their work and pay no attention to other aspects. This leads to difficulties in determining intended contact.

In judicial practice, the reason why it is difficult to determine the false information of using fake base stations is that there are two problems in determining its subjective intention. On the one hand, criminal suspects who commit fraud often hide in the background. In order to avoid police investigation, they mainly contact the criminals who hired fake base stations to send fraudulent information through non-real-name forms such as QQ and WeChat, making it difficult for the police to detect the person who committed the fraudulent message in the shortest possible time, and they cannot collect relevant testimony to prove the subjective knowledge of the person who hired the fake base station to send the fraudulent text message. The criminal purpose of being hired to send false information is only to obtain money from the hired person, rather than to actually commit fraud. Therefore, criminal suspects who are hired to use fake base stations to transmit false information will give various explanations for their academic qualifications after arriving at the scene. For example, they have not read a book and do not know what they are sending, or they are just sending scamming text messages to make money, thinking that using fake base stations to send text messages is an ordinary crime, and not knowing that the employer is committing fraud, etc. Therefore, in the current social context, the study of accomplices in telecommunications network fraud is a topic worthy of consideration and in-depth discussion.

This study aims to deeply explore the issue of identifying the liability of accomplices in telecommunications network fraud crimes. By analyzing relevant cases and laws and regulations, it is expected to clarify the standards and principles for identifying the liability of accomplices in telecommunications network fraud crimes and provide useful reference for judicial practice.

Research Objective

Objective 1: To clarify the basic principles for determining accomplice liability in telecommunications network fraud crimes.

Objective 2: To conduct an in-depth analysis of the specific behaviors and liability determination of accomplices in telecommunications network fraud crimes through actual case analysis.

Objective 3: To discuss the legal provisions and practical operations on the identification of accomplice liability in telecommunications network fraud crimes, with a view to providing reference for relevant legislation and practice in China.

Literature Review

With the development of communication network technology, new types of fraud crimes have become increasingly popular. Because they cause great harm and are very different from other crimes, they are separately designated as "telecommunications network fraud" in judicial interpretations. Therefore, in the past decade or so, Chinese academic circles have begun to study "telecom network fraud", "Internet fraud" and other related issues. In order to better analyze and prevent and control these problems, academic circles have put forward their own methods in practice. views and try to find a new way to solve such problems.

Professor Zhong Jiansheng pointed out in "Qualification of Helping Withdrawal Behavior in Telecom Network Fraud Crimes" that in terms of the security of personal information, he pointed out the illegal use of citizens' personal information in telecom network fraud. Access and use are the root causes of their occurrence, and countermeasures have been proposed to address these problems from many aspects, including the following: establishing special laws and regulations, improving the real-name system, and strengthening administrative supervision of these problems (Zhong Jiansheng, 2023) .

However, the governance plan in this article mainly focuses on protecting personal information, and does not propose a plan on how to combat telecommunications network fraud crimes. The main point expounded by Professor Li Chaonan in the article "Research on the Identification of Co-Criminals in Telecommunications Network Fraud" is that there are three key points in controlling the crime of telecommunications network fraud. The first is to establish and improve citizens' personal information protection mechanisms; the second is the administrative agencies and the judiciary. Close collaboration is needed between agencies; the third is the information and technology linkage between state agencies, enterprises and institutions, and financial and banking institutions (Li Chaonan, 2023). Starting from the perspective of joint crime, Professor Liang Zilin's article "Research on Qualitative Issues of Helping Withdrawal Behavior in Telecom Network Fraud Crimes" believes that common difficult issues in telecom network fraud such as the intention to contact accomplices, the determination of the degree of knowledge of related crimes, etc. The problem must adhere to

the principle of unity of subjectivity and objectivity, prove subjective intention through objective facts, use the presumption system within a reasonable range, and adopt scientific proof methods (Liang Zilin, 2023).

Chen Yufeng's "Criminal Judicial Identification of Telecommunications Network Fraud-Related Acts" believes that the premise of effective governance is to trace the source of the crime of telecommunications network fraud, and the "crime circle" should be reasonably delineated from the upstream source and downstream tracking of telecommunications network fraud crimes. On the premise of correctly interpreting existing legislation, we should comprehensively examine related behaviors based on the entire criminal chain, so as to achieve a comprehensive criminal justice policy of "strict" governance (Chen Yufeng, 2023).

Shan Chenglin published "Knowing Identification of Accomplices in Telecommunications Network Fraud Crimes", which conducted an in-depth analysis of the criminal liability of parallel and division of labor joint crime models. According to his views, intermediary platform operators were identified as telecommunications network fraudsters. The basis of criminal accomplices is that they are subjectively aware and objectively provide substantial help, but the article does not elaborate on the identification of accomplice liability of personal information providers (Shan Chenglin, 2022).

Currently, not only some scholars in the fields of law and criminology are concentrating on studying telecommunications network fraud, but some Internet business entities such as online media and Internet technology companies are also conducting research on this type of crime. Compared with scholars in the field of law, they have mastered the A large amount of data also has strong technical capabilities, which makes them more likely to use statistical analysis to conduct research. For example, Tencent launched the Guardian Program in 2016 and releases the "Anti-Telecommunications Network Fraud Big Data Report" every quarter, which discloses relevant cases and basic data on telecommunications network fraud crimes. 360 Internet Security Center released the "China Telecom Network Fraud Situation Analysis Report" in 2016, and also cooperated with the China Academy of Information and Communications Technology to release the "2020 China Mobile Phone Security Situation Report", which includes mobile phone security data, mobile phone fraud overview, Relevant black and gray industrial chains and other content were combined with examples to provide targeted solution suggestions. It can be seen that new crimes developed based on new technical means have also attracted the attention of emerging technology companies, because they may play the role of leakers and victims at the same time (Lv Wenyi, 2022).

Compared with ordinary crimes, telecommunications network fraud crimes have more and more hidden contact methods, and at the same time, each step in the whole process is more cumbersome. Hired criminals are often focused on their job to the exclusion of other components, making it more difficult to determine intent to contact.

In judicial practice, there are the following three issues regarding the determination of joint crimes. First of all, whether the perpetrator constitutes an accomplice or accomplice to the crime of interfering with radio management order or a crime of fraud depends on whether the perpetrator accepts someone else's entrustment and uses a fake base station to transmit false information. Second, there is an operator who is only commissioned to advertise the victim, attract the victim's attention, and then hand the victim off to the next colleague. In this case, the dispute centered on whether the operator was a co-perpetrator of the fraud or whether he was not guilty of the crime because he did not participate in the subsequent scam. Third, it involves "water houses", which are criminal organizations that transfer funds for fraud

organizations. Usually, the "water house" has a long-term cooperative relationship with the fraud organization, but the "water house" is only responsible for transferring money to the account. Regarding this situation, the controversy mainly focuses on whether the "water house" constitutes a fraud accomplice or a criminal act such as covering up and concealing criminal proceeds and proceeds (Xu Guimin and Wang Xiaoyu, 2023).

Both China's criminal law and the traditional theory of accomplices believe that the establishment of an accomplice relationship requires the existence of "intentional connection." The "Opinions on Several Issues Concerning the Application of Laws in the Handling of Criminal Cases such as Telecommunications and Internet Fraud" (referred to as the "Opinions of the Two High Schools and One Ministry of Finance"), issued by the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security, for "knowingly that another party has committed fraudulent activities" "The requirements also have specific requirements. This article believes that to establish the relationship of "accomplice", it is necessary to provide evidence that combines "intentional", "intentional", "intentional", etc. In addition, the "Opinions of Two High Schools and One Ministry of Finance" also pointed out that when understanding this crime, it is necessary to comprehensively consider the suspect's level of knowledge, past experience, method of committing the crime, contact information with other persons, the size of the income, and whether it is due to the telecommunications network. Make a comprehensive and accurate judgment based on subjective and objective factors such as whether you have been punished for fraud and whether you deliberately evaded detection. This clause supplements "knowing that someone else has committed the crime" and is a "mitigation zone" established based on the characteristics of current telecommunications network fraud and national criminal policies, which is similar to the theory of conspiracy in German criminal law.

From the provisions of this article, the following explanations can be made: First, during the investigation process, the police do not have to rely too much on the suspect's confession. Even if they are not aware of this subjectively, they can also collect information from the suspect. We can use clues from aspects such as past experiences, times and methods of behavior, relationships with others, profit status, etc. to determine whether the suspects are subjectively informed, so that they can be investigated in a timely manner and the crimes can be effectively investigated. The criminal liability of the suspect; secondly, as far as the accomplice is concerned, he does not need to be subjectively aware of the way he committed the fraud, but only needs to prove that he was subjectively aware that he committed the illegal act of fraud. However, from daily life experience Judging from the judicial practice, if the perpetrator has not committed any illegal fraud, he should not be considered an accomplice in fraud. For example, an actor who is hired to use a fake base station to send invoice information should usually not be considered an accomplice in fraud. ; Third, prosecutors and judges can mentally determine a criminal suspect based on factors such as his past experience, the number and manner of his behavior, his relationships with others, and his profit-making situation during the review of arrest, review of prosecution, and court hearings. When a person has a high probability, prosecutors and judges can treat him or her as an accomplice in accordance with the law.

Further specific research based on these theories can also help to make the determination of accessories in telecom network fraud-related cases clearer.

In addition, in order to prevent, contain and punish telecommunications network fraud activities, strengthen anti-telecommunications network fraud work, protect the legitimate rights and interests of citizens and organizations, and maintain social stability and national security, in accordance with the Constitution, the Anti-Telecommunications Network Fraud Law of the People's Republic of China was formulated. It was voted on on September 2, 2022 to crack down on telecommunications network fraud activities committed within the territory of the People's Republic of China or telecommunications network fraud activities committed by citizens of the People's Republic of China abroad. Although this law clarifies the general direction of combating telecommunications network fraud, it proposes various governance measures and elaborates on a series of management methods from three aspects: telecommunications, finance, and the Internet. At the same time, it elaborates on the legal responsibilities of those directly responsible. However, current telecom network fraud gangs often have complex structures, and the identification of "accomplices" is still a question worth pondering.

The identification of accomplice liability refers to the process of determining the responsibility of each person involved in a joint crime. In a joint crime, the liability determination of each accomplice should be comprehensively judged based on their status and role in the crime, as well as whether they have subjective intention and other factors. When we discuss crime, we often mention the two concepts of "single crime" and "joint crime". A solo crime is when one person commits a crime alone, while a joint crime is when two or more people participate together. In joint crimes, the determination of liability of accomplices is a complex and important issue. For example, A, B, and C jointly committed a theft. A was the principal criminal, planning and organizing the entire theft process; B was responsible for the lookout during the theft process; C was an accessory, providing the tools and participating in the theft. In this case, A, as the principal offender, bears the main responsibility. His behavior played a decisive role in the entire joint crime and was the planner and organizer of the entire theft. Therefore, A's punishment should be more severe than that of other accomplices. As an accessory in this case, B’s liability is relatively light. He served as a lookout during the theft and although he participated in the crime, he was not directly involved in the theft. Therefore, when determining responsibility, B’s status and role in the joint crime should be taken into consideration and corresponding punishment should be imposed. As an accessory, C provided the tools to commit the crime and participated in the theft. Although his behavior played a certain role in the success of the theft, in this case, his behavior was secondary to that of A and B. Therefore, when determining responsibility, C’s status and role in the joint crime should be taken into consideration and corresponding punishment should be imposed. In determining the liability of accomplices, the principle of “partial execution, full responsibility” should be followed. That is to say, for each accomplice in a joint crime, regardless of his specific behavior, he should bear legal responsibility for the entire joint crime. However, the degree of responsibility should be judged based on the status, role and behavior of each accomplice in the joint crime.

Research Methodology

1、Research Methodology This study employed a qualitative research methodology, combining literature analysis and case study analysis. The literature analysis involved a comprehensive review of relevant legal theories, judicial interpretations, and academic publications related to accomplice liability in telecommunications network fraud crimes. The case study analysis focused on examining actual telecom network fraud cases to gain insights into the specific behaviors and liability determination of accomplices in real-world scenarios.

2、Source of Data The data for this research was collected from both primary and secondary sources. Primary data was obtained through the analysis of actual telecommunications network fraud cases, which were sourced from legal databases, court records, and official reports. Secondary data was gathered from academic journals, books, legal commentaries, and government publications related to accomplice liability and telecom network fraud crimes.

3、Population and Sampling The population for this study consisted of all telecommunications network fraud cases involving accomplices in China. Due to the large number of cases and the complexity of the issue, a purposive sampling technique was employed to select a representative sample of cases for in-depth analysis. The cases were chosen based on criteria such as the severity of the crime, the complexity of the accomplice network, and the availability of detailed information on the roles and behaviors of accomplices.

4、Data Collecting Data collection for this research involved a systematic process of identifying, retrieving, and organizing relevant information from the selected sources. For the literature analysis, data was collected through keyword searches in academic databases, legal databases, and online libraries. The case study analysis involved retrieving court records, police reports, and other official documents related to the selected telecom network fraud cases. The collected data was then carefully reviewed, and relevant information was extracted and categorized based on the research objectives.

5、Analysis of Data The collected data was analyzed using a thematic analysis approach. The literature analysis involved identifying and synthesizing key themes, principles, and theories related to accomplice liability in telecommunications network fraud crimes. The case study analysis involved a detailed examination of the specific behaviors, roles, and degrees of involvement of accomplices in the selected cases. The findings from both the literature analysis and case study analysis were then integrated to develop a comprehensive framework for determining accomplice liability in telecom network fraud crimes.

Research Conceptual Framework

Conceptual Framework The conceptual framework for this research is based on the integration of legal principles, judicial interpretations, and real-world practices related to accomplice liability in telecommunications network fraud crimes. The framework consists of three main components:

1、Basic Principles: This component focuses on establishing the fundamental principles and guidelines for determining accomplice liability in telecom network fraud cases. It draws on relevant legal theories, such as the theory of joint crime and the principle of "partial implementation, full responsibility," to provide a solid foundation for assessing accomplice responsibility.

2、Specific Behaviors and Liability Determination: This component examines the various roles, behaviors, and degrees of involvement of accomplices in actual telecom network fraud cases. It seeks to identify patterns and criteria for determining the liability of accomplices based on their specific actions and contributions to the crime.

3、Legal Provisions and Practical Operations: This component analyzes the current legal provisions and operational practices related to accomplice liability in telecom network fraud cases in China. It aims to identify strengths, weaknesses, and areas for improvement in the existing system and provide recommendations for enhancing the effectiveness of combating these crimes.

Research Results

In cases of telecommunications network fraud crimes, the impact of identification of accomplice liability and defense statements can be reflected in the following cases:

Case 1: Chen Mouwang organized a transnational fraud group, used online chat software to trick victims into participating in gambling, and defrauded victims through background manipulation. Xie Mouhao and Chen Mouwang were identified as the principal criminals and were sentenced to 15 years and 13 years in prison respectively, as well as fines. The defendant Lin was sentenced to six years in prison and fined for helping to transfer criminal proceeds.

Case 2: Long Moudong case: Long Moudong knew that others were committing telecommunications network fraud crimes, but still provided them with software development and technical support. His behavior was regarded as direct assistance to the crime of fraud, and he was punished as an accomplice in the crime of fraud and sentenced to five years in prison and a fine. This case shows that if the act of providing technical support directly helps the crime of fraud, it can constitute an accomplice in the crime of fraud.

Case 3: Chen Wenhui and 7 others Case: Chen Wenhui and 7 others purchased student information and citizen housing purchase information through the Internet, pretending to be state agency staff to commit fraud. They were convicted of fraud and infringement of citizens' personal information. Chen Wenhui was sentenced to life imprisonment for his role in organizing and directing the fraud. This case reflects the infringement of citizens’ personal information and the damage to social integrity caused by telecommunications and network fraud crimes.

Case 4: Case of Liu Moumou and others: Liu Moumou and others formed a telecommunications network fraud criminal group and used posing as the person in charge of the company to trick financial personnel into transferring large amounts of money. Liu Moumou, as the planner, organizer and leader of a criminal group, was sentenced to life imprisonment. Other persons involved were also sentenced to varying degrees of fixed-term imprisonment.

The specific behaviors and subjective intentions of these cases show that in telecommunications network fraud crimes, the determination of accomplice liability needs to comprehensively consider the degree of help from the perspective of the perpetrator. Excuses and statements can serve as an important basis for judging the perpetrator's degree of knowledge and responsibility, but they need to be combined with other evidence to accurately determine the responsibility of the accomplice.

1. Liability determination of accomplices in telecommunications network fraud crimes

The determination of liability of accomplices in telecommunications network fraud crimes is a complex issue involving many aspects. According to the "Opinions on Several Issues Concerning the Application of Laws in the Handling of Telecommunications and Internet Fraud and Other Criminal Cases" (hereinafter referred to as the "Opinions"), telecommunications and Internet fraud crimes are usually joint crimes, and the responsibilities of different accomplices need to be clarified in order to accurately convict and impose sentences. In telecommunications network fraud crimes, there are two modes: "parallel fraud" and "division fraud". In parallel fraud, multiple actors are directed and led by the same person to commit fraud against different targets, and each actor independently completes the fraud activities. Division-of-labor fraud is a fraud in which each actor is responsible for a certain stage or module of behavior according to a pre-agreed fraud method, and jointly completes the fraud. The "Opinions" also stipulates the principle of "partial implementation of full responsibility", that is, the behaviors of each principal offender objectively use and complement each other, so that his own behavior and the behavior of others lead to the occurrence of the result. Therefore, even if the perpetrator only shares part of the principal responsibility for the commission of the act, he must bear principal responsibility for the entire result. In addition, regarding the issue of knowingness of accomplices, the subjective determination of knowingness of accomplices in telecommunications network fraud crimes is very critical. An accomplice must be someone who knows others to commit a telecommunications network fraud crime, rather than just knowing others to commit a crime. The "prior conspiracy" mentioned in the "Opinions" is different from "knowingly knowing that others have committed the crime of telecommunications and network fraud." Prior conspiracy means that before the crime is committed, the accomplices have formed a common criminal intention and have planned and carried out the crime. Negotiate.

The "Opinions" also stipulates the principle of "partial implementation of full responsibility", that is, the behaviors of each principal offender objectively use and complement each other, so that his own behavior and the behavior of others lead to the occurrence of the result. Therefore, even if the perpetrator only shares part of the principal responsibility for the commission of the act, he must bear principal responsibility for the entire result.

In addition, regarding the issue of knowingness of accomplices, the subjective determination of knowingness of accomplices in telecommunications network fraud crimes is very critical. An accomplice must be someone who knows others to commit a telecommunications network fraud crime, rather than just knowing others to commit a crime. The "prior conspiracy" mentioned in the "Opinions" is different from "knowingly knowing that others have committed the crime of telecommunications and network fraud." Prior conspiracy means that before the crime is committed, the accomplices have formed a common criminal intention and have planned and carried out the crime. Negotiate.

When handling telecommunications network fraud criminal cases, it is necessary to comprehensively consider the specific model of the crime, the roles and responsibilities of each perpetrator, and their degree of subjective knowledge to ensure the accurate determination of the liability of accomplices.

In telecommunications network fraud crimes, the identification of accomplice liability is a complex issue involving many aspects.

In actual cases, these principles and regulations are used to accurately determine and allocate the liability of accomplices. For example, in a division-of-labor fraud case, some people are responsible for technical support, such as making fake websites or writing fraudulent information, while others are responsible for contacting victims and implementing fraud. In such cases, all participants are considered accomplices and are held liable based on their role and knowledge in the fraud.

Therefore, when dealing with telecommunications network fraud cases, it is necessary to comprehensively consider the specific model of the crime, the roles and responsibilities of each perpetrator, and their degree of subjective knowledge to ensure the accurate determination of the liability of accomplices.

2. How to specifically judge the degree of knowledge of accomplices in actual cases.

In actual cases of telecommunications network fraud crimes, determining the degree of knowledge of accomplices is an important judicial practice issue. This typically involves a comprehensive assessment of the accomplice's behavior, intentions, background knowledge, and the degree of communication and collaboration between them. Here are some key factors in determining an accomplice’s level of knowledge:

A. If the perpetrator has relevant professional background, such as information technology, finance, etc., this may indicate that they have a deeper understanding of the nature and purpose of the fraud.

B. The perpetrator's specific role and degree of participation in fraudulent activities are important basis for judging the degree of knowledge. For example, technical support personnel may have a clear understanding of the purpose of the scam when providing technical assistance.

C. If the perpetrator has obtained improper benefits from fraudulent activities, this may indicate that they knew that their actions were part of participating in the fraud.

D. Communication records between perpetrators, such as text messages, emails, social media chats, etc., can provide evidence of whether they are aware of fraudulent activities.

E. The actor's explanation and statement of his behavior are also important factors in judging the degree of awareness. If they provide a reasonable explanation for their actions, this may affect the assessment of their level of knowledge.

F. The specific circumstances of each case are unique, so the specific facts and context of the case need to be considered when determining the degree of knowledge.

In actual cases, courts will combine these factors to assess the degree of knowledge of accomplices and determine their liability accordingly. For example, if a technical support staff knows that the services they provide will be used for fraud and continues to provide those services, they may be found to have knowledge and therefore be held liable as an accomplice. It should be noted that these factors are not used in isolation, but are interrelated and influence each other. In specific cases, the court will comprehensively consider these factors based on the specific circumstances of the case to accurately determine the degree of knowledge of the accomplice.

3. What impact does the accomplice’s excuses and statements have in determining the degree of knowledge.

The accomplice's excuses and statements have a significant impact on determining his degree of knowledge in telecommunications network fraud, because they are directly related to the perpetrator's subjective intention and cognition. The following are the possible effects of excuses and statements on the determination of knowledge:

A. If the accomplice voluntarily admits that he knew that his actions were part of his participation in the fraud, this confession can be used as important evidence to determine the degree of knowledge. A voluntary, candid admission of guilt may indicate that the perpetrator knew that his or her actions were in aid of fraud.

B. The perpetrator may argue that he misunderstood the situation or did not know that his behavior was assisting in fraud. This defense needs to be verified by other evidence, such as the perpetrator's professional knowledge, communication records with others, etc. If the perpetrator can provide reasonable explanations and evidence to support his statement of ignorance, this may affect the determination of his degree of awareness.

C. In some cases, the perpetrator may claim that he was forced or induced to participate in the crime. This defense may affect the assessment of the degree of knowledge but will usually need to be supported by corroborating evidence. If the perpetrator can prove that his or her actions were prompted by threats or misdirection, this may reduce liability.

D. The perpetrator may argue that he does not understand the law or has misunderstood the provisions of the law. This defense may be taken into account, especially where the perpetrator lacks legal knowledge. However, the law generally assumes that citizens have some knowledge of the law, so this defense may not be a complete exoneration.

E. If the perpetrator demonstrates knowledge of the fraud in multiple communications and actions, this may weaken their defense of ignorance. Continuity of behavior may indicate ongoing awareness of the fraud.

F. The relationship between the perpetrator and other accomplices, as well as their interactions, are also important factors in assessing the veracity of excuses and statements. If the perpetrator has close connections and collaborations with other accomplices, this may indicate a deeper understanding of the fraud.

In judicial practice, the court will comprehensively consider the accomplice's defense and statement and other evidence, such as the perpetrator's background, degree of participation, communication records, etc., to evaluate his degree of knowledge. If the excuses and statements are contradicted by other evidence or are deemed untrustworthy, the court may rely on other evidence to determine the perpetrator's level of knowledge. On the contrary, if the defense and statement are supported by other evidence and considered reasonable, then this may affect the determination of the perpetrator's degree of knowledge.

Discussion

From the current research status, we know that first of all, telecommunications network fraud crimes are often closely related to the security of citizens’ personal information. The successful implementation of this type of crime usually relies on the personal information obtained. Serious leaks and transactions of personal information have nourished a large number of black and gray crimes. industrial chain. Data shows that from January 1 to August 31, 2021, courts across Guizhou Province accepted a total of 867 cases of telecommunications network fraud and upstream and downstream related crimes involving 1,808 people, with a total amount of 2.293 billion yuan involved. Among them, 103 cases of telecommunications network fraud involving 247 people were concluded, 5 cases of infringement of citizens’ personal information involving 7 people; in addition, 467 cases of assisting information network criminal activities involving 724 people, and 14 cases of covering up or concealing criminal proceeds and proceeds of crime involving 47 people (Ayinigar Aisha, 2021).

In this year, the promulgation of the new "Personal Information Protection Law" demonstrated the attitude of the Chinese government in protecting citizens' personal information, and also demonstrated the measures taken by the Chinese government to combat telecommunications network fraud. Secondly, if a person's behavior is judged according to the constituent elements of a criminal case, many people's behavior cannot be characterized as a crime and can only reach the level of administrative punishment. After joining the fraud group, some criminal suspects and defendants failed to commit the crime and the numbers they dialed did not reach the amount required by the Criminal Law, so they could only be considered "attempts." If the theory of joint crime is integrated into the analysis process and the principle of "partial implementation, full responsibility" is followed, then the criminal crackdown on telecommunications network fraud crimes can be increased to a certain extent, and the upstream and downstream gangsters can be punished. The gray industrial chain has a deterrent effect and can also enhance the whole society's awareness of the illegality of telecommunications network fraud-related crimes.

As a new type of fraud, telecommunications network fraud crimes appear frequently, and their crime patterns are also unique to the background of today's information society. They mainly refer to criminal suspects constantly and deliberately fabricating false identity information and events, using the Internet, telephone, WeChat, text messages and other communication tools as well as new Internet banking technologies are used as carriers to commit criminal activities to defraud the masses. This crime originated in Taiwan, and later gradually developed from the coast of Fujian to the whole country and spread throughout Southeast Asia. The conclusion of the main article on this crime is consistent with the provisions of the Anti-Telecommunications Network Fraud Law of the People's Republic of China, and is also consistent with the criminal law's protection of the rights and interests of natural persons, legal persons and other subjects. It is clarified that the "principal offenders" and "accomplices" who engage in telecommunications network fraud activities committed by foreign institutions or personnel against the People's Republic of China, or provide goods or services for other telecommunications network fraud activities committed within the country, shall be punished in accordance with the relevant provisions of the Criminal Law and cannot No one involved should be allowed to go unpunished. The Anti-Telecommunications Network Fraud Law of the People's Republic of China also clarifies: "Whoever organizes, plans, implements, or participates in the implementation of telecommunications network fraud, or assists in the implementation of telecommunications network fraud, shall comply with the Civil Code of the People's Republic of China, etc. Relevant provisions bear corresponding civil liability. "However, as long as the joint criminal behavior of joint offenders is defined, the specific content of the criminal law can be implemented and made effective.

As our country enters a period of modern development, China's communications industry and financial industry are developing rapidly and with strong momentum, especially the rapid spread of information. New electronic products and companies based on emerging industry services are constantly emerging and changing our lives, social networking The network is complex and diverse. The development of the telecommunications industry has promoted the normalization of online shopping and online payment, completely changing our production and life. At present, China has become one of the countries with the largest number of Internet users and developed Internet in the world. At the same time, the number of electronic products purchased online by Chinese citizens is also increasing rapidly. The replacement of electronic products is fast and the time is short. The number of downloads and users of some

online APPs such as Sina Weibo and WeChat continue to grow. The development of the Internet is making things easier for us. While living, it inevitably induces the frequent occurrence of telecommunications network fraud crimes; it shows outstanding characteristics such as cross-regional crimes, group forms of criminal organizations, diversified, intelligent, and concealed fraud methods.

Behind the rampant and high incidence of telecom network fraud crimes, many problems in the punishment and prevention of such crimes have gradually been exposed. Its high frequency and diversified methods determine the importance and necessity of effectively punishing and preventing telecom network fraud crimes. , Preventing telecommunications network fraud crimes is the top priority for maintaining the long-term stability of our society and the happiness and well-being of the people. From the perspective of legal theory, combined with domestic and foreign theories and judicial practices, through the definition, characteristics, and countermeasures of accomplices in telecommunications network fraud, etc. Conduct research to promote theoretical circles and judicial and law enforcement practitioners to pay more attention to this type of crime, thereby clarifying the criminal liability of each perpetrator and forming relatively unified regulations in judicial judgments. Let all those involved in telecommunications network fraud be punished accordingly, so as to warn many people who are lucky.

Suggestions

1、Suggestions for this research work

1) Telecommunications network fraud crimes should prioritize the protection of citizens' personal information and establish a sound personal information protection mechanism.

2) The theory of joint crime should be integrated into the analysis process of telecommunications network fraud cases, and the principle of "partial implementation, full responsibility" should be followed to increase the crackdown on such crimes.

3) Theoretical circles and judicial and law enforcement practitioners should pay more attention to telecommunications network fraud crimes, clarify the criminal liability of each perpetrator, and form relatively unified regulations in judicial judgments.

4) All those involved in telecommunications network fraud should be punished accordingly to warn potential criminals.

2、Suggestions for further research

1) Future studies should investigate the long-term impact of the proposed liability determination principles on combating telecommunications network fraud crimes.

2) Researchers should explore the potential of integrating technology into the identification and prevention of telecommunications network fraud crimes, such as using big data analysis and artificial intelligence to detect and prevent such crimes.

References

Zhong Jiansheng, Tan Liang. (2023). Qualification of helping with withdrawals in telecommunications network fraud crimes [J]. Journal of Wuhan Public Security Cadre College. 37 (02), 42-46.

Shan Chenglin. (2022). Identification of knowing accomplices in telecommunications network fraud crimes [J]. *China Prosecutor*. (09), 11-14.

Wen Deng, Guangjun Liang, Chenfei Yu, Kefan Yao, Chengrui Wang & Xuan Zhang. (2023). An Early Warning Model of Telecommunication Network Fraud Based on User Portrait. Computers, Materials & Continua (1).

Chen, J., & Liu, Y. (2023). Analysis of contact methods in telecommunications network fraud cases. *Journal of Criminal Investigation*. 12 (3), 45-52.

Gao, M., & Chang, M. (2016). *Criminal Law*. Beijing: Law Press China.

Li, H., & Wang, S. (2022). Trends and characteristics of online fraud crimes in China. *Crime Research.* 8 (2), 112-121.

Wang, L., Zhang, M., & Chen, T. (2022). The development and prevention of cybercrime in China. *Chinese Journal of Criminology*. 15 (4), 78-89.

Xu, G., & Zhao, L. (2021). A survey of fraud crimes in China based on judicial big data. *Legal Science.* 39 (5), 22-31.

Zhang, Y., Liu, J., & Wang, H. (2021). The evolution and countermeasures of telecommunications network fraud in the era of big data. *Journal of Public Security Science and Technology.* 18 (3), 55-63.