Science of Law Journal (2024)
Clausius Scientific Press, Canada

DOI: 10.23977/law.2024.030404
ISSN 2616-2296 Vol. 3 Num. 4

Empirical Research on the High Incidence of Crime of Assisting Information Network Criminal Activities in Telecommunication Fraud Cases Based on 26, 121 Judgment Documents

Chenxian Xiang[1,a], Jiayi Li[1,b], Xinrui Xiao[1,c], Wei Zhang[2,d,*]

[1]Law School, Guangzhou College of Commerce, Guangzhou, China
[2]Institute of Legal Psychology, Guangzhou College of Commerce, Guangzhou, China
[a]1006733768@qq.com, [b]1748645364@qq.com, [c]798935890@qq.com,
[d]criminal.minds@foxmail.com
[*]Corresponding author

Keywords: Demographic Factors, High Crime Rate, Telecommunications Fraud, Crime of Assisting Information Network Criminal Activities

Abstract: Since 2020, the offense of aiding and abetting cyber crime through information networks has escalated significantly, reaching epidemic proportions. In 2021, it emerged as the foremost criminal activity within the entire telecommunication fraud criminal chain. This paper empirically examines the current high prevalence of this offense in the context of telecommunication fraud cases. Through an analysis of pertinent cases, it delves into the current landscape and identifies the specific factors contributing to the widespread occurrence of information network-related crimes in Chinese telecommunication fraud. The study concludes with a set of remedial actions, including bolstering public awareness of the rule of law, enhancing internal control systems, clarifying judicial interpretations of the offense of aiding and abetting cyber crime, and strengthening the online banking system. These measures aim to refine judicial practices in China and effectively tackle issues linked to information network-related offenses.

1. Investigation on the present situation of crime of assisting information network criminal activities in Telecommunication Fraud Cases

This paper comprehensively analyzes 26,121 verdicts related to aiding and abetting cybercrime in telecommunication fraud cases from 2019 to 2023. It explores the demographics of perpetrators, including age, education, employment, conviction, and probation rates, aiming to understand the offense's nature, underlying factors, and effective preventive measures. The study seeks to uncover the characteristics and root causes of this criminal behavior and proposes mitigation strategies.

Due to the rapid advancement of internet and mobile technologies, cyber-crime has escalated, posing major societal threats. Among these, aiding and abetting cyber-crime through information networks has gained increasing attention [1]. According to the Figure 1, our analysis of 26,121 such cases reveals a sharp rise from 2019 to 2023, peaking at 21,185 cases in 2021. Despite a slight decline

since, the numbers remain significantly higher than in 2019. The widespread occurrence of these offenses highlights the seriousness of the issue and the critical need for greater awareness and proactive measures.

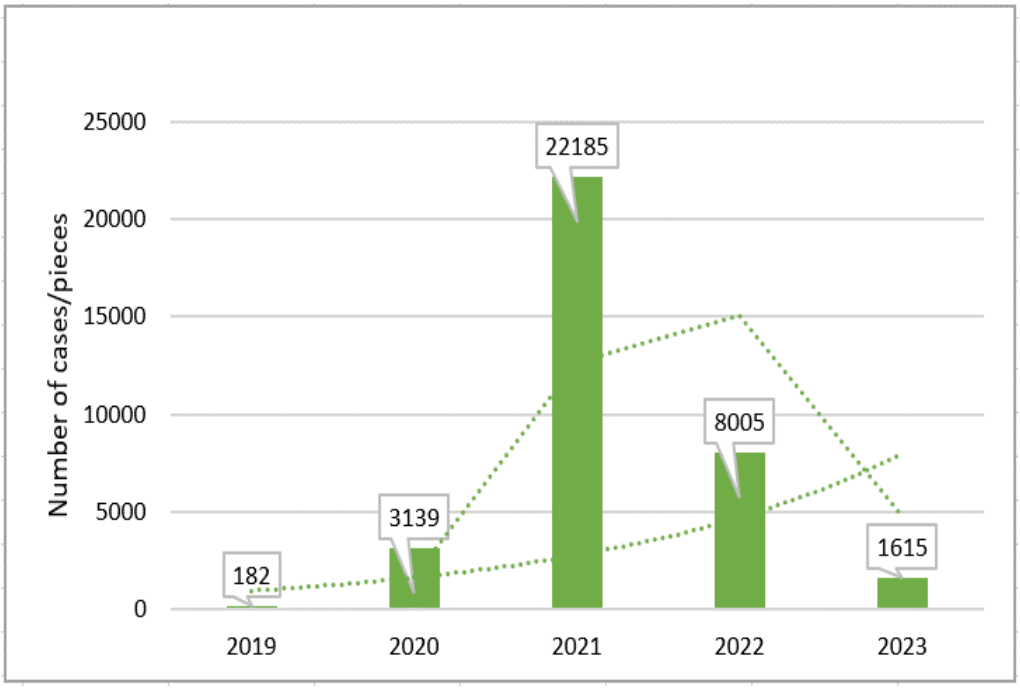

Figure 1: The distribution of the number of 26,121 cases of crime of assisting information network criminal activities in 2019-2023

1.1. Analysis of Demographic Factors of Offenders in Information Network Crime Cases

Based on an examination of 26,121 cases of aiding and abetting information network crimes, this paper delves into the demographic characteristics of the perpetrators, including age, educational attainment, and employment status. As illustrated in Figure 2, the age distribution of offenders reveals that 13.2% are under the age of 20, 22.7% are aged between 20 and 25, 47.6% fall within the 25 to 30 age bracket, and 16.5% are over 30. Evidently, the majority of perpetrators in these cases are young individuals. The notable preponderance of youth can be attributed to the misuse of modern network information technology.

Figure 3 presents the educational breakdown of the offenders. Notably, 68.3% possess an education level of junior high school or below, 22.3% have completed high school or technical secondary education, and 9.4% hold a junior college degree or higher. [2]Furthermore, the fact that 9.4% of offenders hold a junior college degree or higher underscores the need for improved legal awareness and education on campuses. Students may inadvertently become accomplices in information network crimes due to a lack of awareness and the allure of common online marketing tactics.

The employment status of the perpetrators is another significant factor to consider. As depicted in Figure 4, 64.8% of the offenders are unemployed, while only 13.5% are employed as legal representatives of companies. The remaining 21.7% are engaged in various occupations such as small-scale business transactions. Among these, those employed as legal representatives of companies often play a pivotal role in facilitating criminal activities, providing programs, tools, or other cutting-edge network technologies to aid in these endeavors. In some instances, offenders even establish companies solely for criminal purposes. The high proportion of unemployed offenders

(64.8%) suggests that the lure of low economic investment and relatively high returns associated with aiding information network crimes is a significant motivating factor, given their lack of stable income.

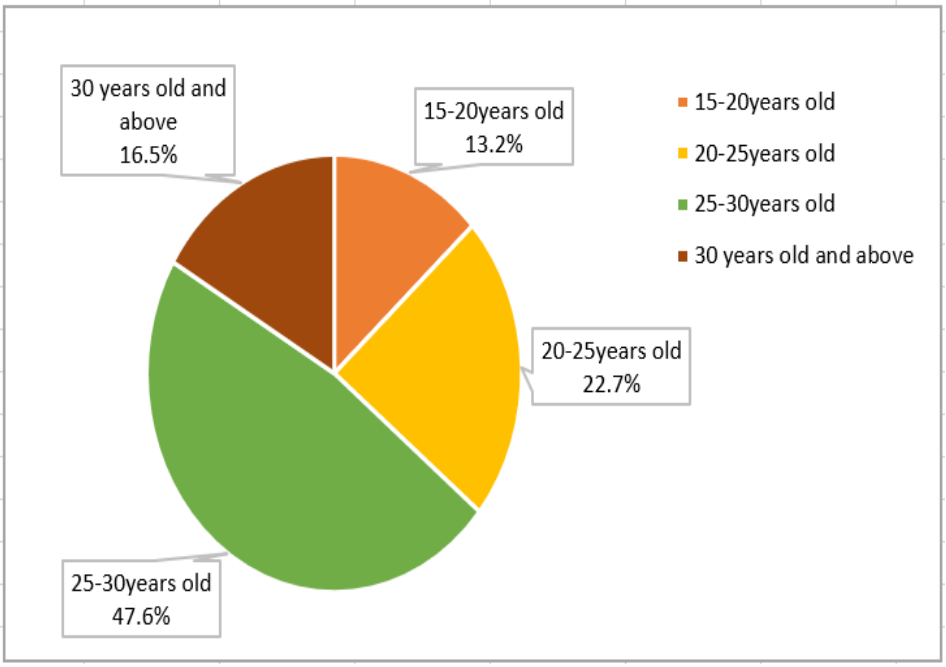

Figure 2: Age of offenders in 26,121 cases of crime of assisting information network criminal activities

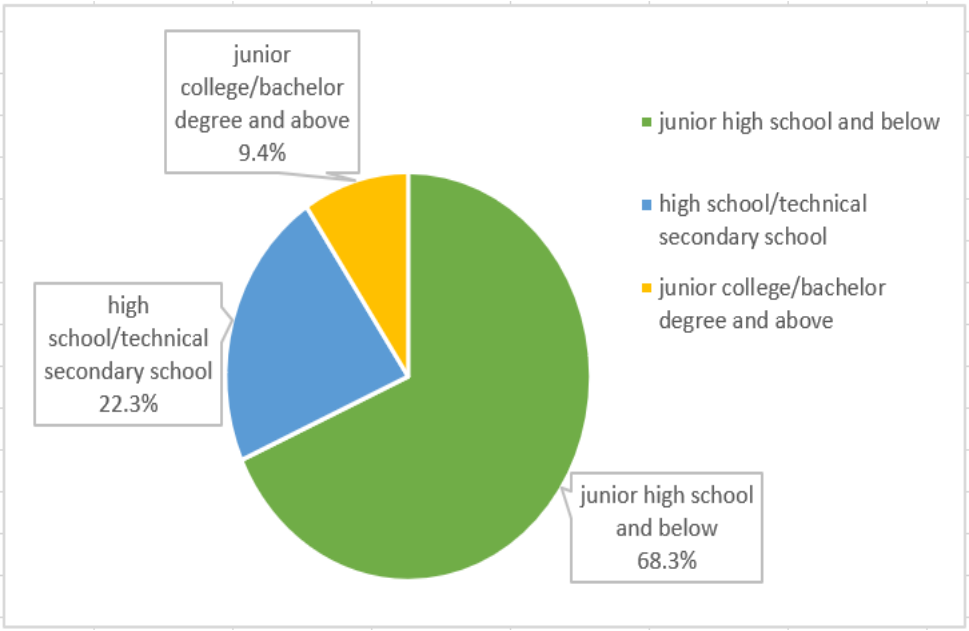

Figure 3: Education breakdown of the offenders in 26,121 cases of crime of assisting information network criminal activities

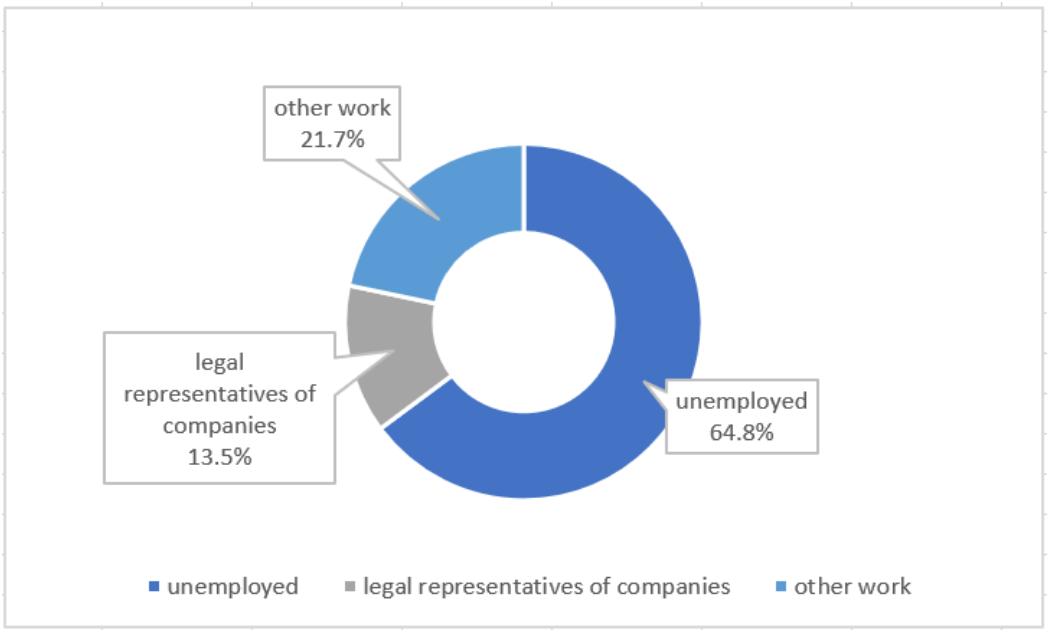

Figure 4: Employment status of the perpetrators in 26,121 cases of crime of assisting information network criminal activities

1.2. Analysis of the actual types of information network crime cases

Beyond convictions, the application of probation is a significant data point. As depicted in Figure 5, an examination of probation cases related to aiding and abetting information network crimes from 2019 to 2023 reveals that approximately 20% of convicted offenders in this category ultimately receive probation. This rate surpasses that of other criminal offenses, including theft and robbery. This statistic suggests that individuals convicted of aiding and abetting information network crimes tend to exhibit lower levels of subjective malice and societal harm compared to perpetrators of other crimes, often resolving matters through civil compensation. However, this trend also indicates that some actions, which could potentially be addressed without resorting to criminal measures, are nonetheless being prosecuted, highlighting the urgent need to address the underlying issues surrounding information network crimes.

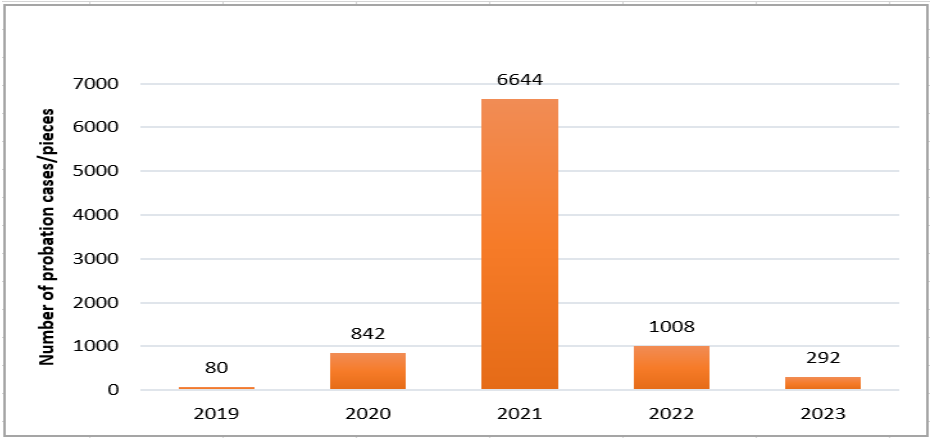

Figure 5: Number of probation cases in 26,121 cases of crime of assisting information network criminal activities

1.3. Analysis of the characteristics of typical cases of crime of assisting information network criminal activities

Through the analysis of the case samples, can see that the crime cases of crime of assisting information network criminal activities in telecommunications fraud cases mainly have the following three characteristics:

1.3.1. Criminal behavior has obvious technical characteristics and high concealment

The perpetration of information network crimes involves the use of modern technologies and requires specific professional knowledge, particularly in computer programming, network security exploitation, and system vulnerability identification. These skills are often used to create malicious software, fashion attack tools, or undermine system security. Criminals leverage these capabilities to provide crucial infrastructure and technical support for their criminal activities. Information network crimes primarily occur within the virtual network and via mobile devices, with perpetrators communicating and executing offenses mostly through the Internet. This reduced offline contact and use of proxy servers and anonymous technologies pose challenges to investigations due to the crimes' inherent concealment and anonymity, complicating tracking efforts. Understanding the techniques used by information network crime perpetrators is crucial to dismantling these illegal activities. Technical departments must continuously strengthen their research and development, as well as their network security defenses, to counter evolving criminal tactics. Additionally, it's important to increase public and practitioners' understanding and prevention capabilities regarding these crimes, through enhanced network security awareness and relevant technical training.

1.3.2. Most criminals are profit-driven

Criminals often participate in criminal activities for economic benefits. They may get paid by providing related technologies or services, or make profits by lending "two cards" in a low-cost and high-yield way. This kind of interest-driven is one of the important causes to help the information network crime.

First of all, some criminals participate in information network crimes as technicians or service providers. They have rich computer knowledge and technical skills, and use their expertise and positions to facilitate the implementation of criminal acts in cyberspace. These people are often extremely difficult to track down, and have been employed by criminal organizations for a long time, providing them with stable support and technical services in order to get corresponding remuneration. Secondly, criminal organizations provide a profitable platform for participants suspected of crime of assisting information network criminal activities by recruiting, cooperating or purchasing technical services. Participants and criminal organizations jointly plan and implement information network criminal activities and share the economic benefits. In addition, criminals also make profits by illegally selling stolen personal information and credit card information, or obtain economic benefits by illegal means such as extortion and gambling through criminal activities.

1.3.3. Form diversity and variability

Criminals with technical means can provide attack tools aimed at specific targets to help other criminals gain illegal control or sensitive information. Under this technical means, by providing a proxy server to hide the real IP address, it will greatly increase the difficulty of tracking, further increase the difficulty of cracking down on cyber crimes, and make the relevant law enforcement departments need to invest more resources and energy in investigation and tracking. [3]

Providing criminals with Internet access, server hosting, network storage, communication

transmission and other technical knowledge, advertising promotion assistance, payment and settlement assistance are all common situations to crime of assisting information network criminal activities. The cases are diverse and involve a wide range, and the network technical means are updated at any time, and the criminals will adjust their modus operandi and methods in time, which will increase the cost for law enforcement agencies to identify and crime of assisting information network criminal activities.

2. An analysis of the reasons for the surge in cases of crime of assisting information network criminal activities in telecommunications fraud cases

2.1. High income, low cost and fast profit

Telecommunication network fraud and online gambling have emerged as significant contributors to the landscape of criminal activities involving information networks, accounting for approximately half of such offenses. Since the inclusion of the crime of assisting information network criminal activities in the 2015 Criminal Law Amendment (IX) of the People's Republic of China (PRC), this particular offense has escalated rapidly. Notably, in 2021, it ranked among the top ten criminal cases for the first time, with nearly 130,000 individuals prosecuted by procuratorial organs in China, elevating it to the third most prevalent criminal offense.

The appeal of information network crime stems from its profitability, low cost, and quick ROI. In telecommunication fraud, the unlawful sale of phone and bank cards provides a lucrative, unethical income. These crimes attract segments of society, especially students, the elderly, and the unemployed, who may be swayed by fraudsters' promises. This minor profit motive inadvertently makes them accomplices, providing opportunities for other criminals.

For example, Jiangdong Liang from Jilin Province sold nine bank cards to a criminal gang for just 4,400 yuan and faced legal consequences. Similarly, Na Zhang from Beijing sold five bank cards to fraudsters for only 300 yuan but attracted anti-fraud authorities' attention due to excessive transactions, leading to disciplinary action. Many such cases show an increasing trend of renting and selling phone and bank cards, significantly contributing to the rise of information network crimes, making it a major offense in telecommunication fraud. The profitability and ease of providing settlement assistance through transfers also contribute to the frequent occurrence of this crime.

2.2. Most criminals are not clear about criminal behavior

The lack of legal awareness among the general public contributes significantly to the increasing prevalence of information network crimes in telecommunications fraud. Most individuals involved in these crimes have limited education, lack professional proficiency, and are often unemployed, leading to inadequate understanding of the seriousness of renting or selling bank and telephone cards. This ignorance fuels various criminal activities, resulting in severe societal consequences.

The offense of aiding and abetting information network crimes was added to the Criminal Law Amendment IX of the PRC in 2015. However, until 2020, few cases were resolved due to inadequate publicity and education about this crime, leading to a general lack of awareness among the public. Some suspects have limited knowledge of disciplinary measures and overlook the long-term effects of their actions, driven by short-term gains.

Analysis of relevant cases shows that most perpetrators aiding and abetting information network crimes in telecommunications fraud are under 30, with 75% falling into this age group, including nearly 10% of minors. College students, targeted for their lack of stable income and high expenses, are particularly vulnerable. Despite their education, many lack legal awareness and underestimate the consequences of their actions due to inadequate legal education and a weak sense of personal

information protection. In a criminal case heard by the Shaoshan People's Court in Hunan Province, the 20-year-old defendant Guo was convicted of aiding and abetting information network criminal activities. Guo provided his bank cards, phone, and SIM for funds transfer in September 2021, receiving a monetary reward. These were then used in multiple telecommunication frauds. Guo was sentenced to four months' detention and fined RMB 2,000.

2.3. Difficult to crack down on crime

Social development has ushered in a new digital era, facilitating easier public access to information and services via the Internet. However, this shift has also opened doors for criminals to engage in illicit activities like gambling, fraud, and money laundering. Consequently, the offense of aiding and abetting information network crimes has escalated, becoming the third most prosecuted criminal offense, posing a risk of evolving into a widespread criminal epidemic.

The "card-breaking" initiative targets the increasing internet-based crimes to purify the online space. Card-breaking operations have fueled information network-related crimes. China's Criminal Law Article 287 bis defines aiding information network criminal activities as knowingly providing technical support to those committing crimes via the information network. However, the interpretation of "aiding" is still broad. The Electric Fraud (II) opinion defines renting and lending of two cards as "aiding behavior" in the context of "card-breaking". However, this involves offline supply mechanisms, unlike technical assistance. Viewing physical card supply as aid seems simplistic. The broad interpretation of "aiding" has contributed to the crime's widespread nature.

Ambiguity surrounds the subjective cognition of "knowingly providing support to commit network crimes". The loose interpretation of "knowingly" includes actual, constructive, or potential knowledge. Many college students providing cards or receipts for online jobs have been deemed "knowledgeable", assuming they knew or should've known. This presumptive approach has led to the misuse of "knowingly", criminalizing non-criminal behaviors, affecting those with limited education seeking small profits.

The vagueness in defining the crime of aiding information network crimes, along with the high conviction rate, has burdened China's judicial system. This has led to an imbalanced allocation of judicial resources, implicating many ordinary individuals. Meanwhile, some lawbreakers escape legal action, making it hard to tackle the problem's core.

Additionally, network detection complexity is noteworthy. Cybercrime methods have diversified with the rapid advancement of information technology. Criminals use various high-tech tactics, making cybercrimes endlessly varied and concealed due to the network's openness, uncertainty, and transcendence of time and space. This complicates evidence extraction, preservation, and examination, making cybercrime harder to combat than conventional crimes. The virtual nature of online transactions also hinders thorough investigations, increasing detection complexity.

3. Relief measures to prevent and reduce the high incidence of information network crimes

3.1. Consciousness of rule of law, internal control mechanism and monitoring and identification ability

Telecommunication fraud methods have multiplied, and individuals' susceptibility depends on their protective awareness. A clearer understanding of information network crimes among the public makes it harder for fraudsters to succeed, preventing such crimes. Weak legal awareness fuels these crimes' growth. To tackle this, it's crucial to address root causes, boost prevention awareness, protect people's interests, and enhance their sense of well-being and security.[4] Implementing targeted prevention measures for high-risk groups and industries is vital to prevent those with limited legal

awareness from unwittingly aiding illegal activities. At the same time, legal education for high-risk industry employees, using case studies, warning education, improving occupational safety, and fostering online legal compliance are crucial.

In fighting information network crimes, legal publicity is crucial for boosting the public's law-abiding awareness. [5] It emphasizes avoiding greed and quick profits, recognizes the illegality of buying/selling "two cards," and guides the public to adopt proper behavioral norms. Remaining vigilant in daily life and work to avoid card traps is vital. Preventing personal information leaks, enhancing card security awareness, and improving risk awareness, such as protecting credit card passwords, are essential measures. Exercising caution when clicking unknown links and avoiding disclosure of personal information are essential, as criminals use viruses in links to steal data and commit fraud. Trusting third-party agencies handling credit cards should be avoided to prevent illegal activities.

In summary, strengthening public legal awareness, guiding correct behavioral norms, and conducting legal education are urgent to prevent information network crimes. The high incidence of these crimes poses a challenge to the online legal environment. Strengthening internal controls to trace and disrupt cybercrime is crucial.

Financial, telecommunications, and network departments must fulfill duties to oversee implementation of the Anti-Telecommunication Network Fraud Law provisions by institutions and providers. Promoting preventive mechanisms and jointly building safety nets with enterprises is crucial to safeguard public property interests.[6]

Compacting business management responsibility is crucial for combating information network crimes through strict identity verification. Clarifying responsibilities, incorporating crime supervision into business cycles, normalizing investigations, limiting account openings, real-time information linking with public security, and monitoring the account system reduce risks. Controlling effective identity document identification, examining account holder information, maintaining records, and strengthening inspections of operators and bank outlets are essential. Suspicious individuals involved in buying/selling "two cards" must be promptly identified, especially in high-involvement areas, requiring thorough investigations.

3.2. Clarify judicial determination and solve judicial practice problems

In recent years, defining the crime of aiding information network activities has proven challenging in judicial practice, leading to a high conviction rate. "Information network crime" refers to criminal activities using electronic devices over information networks. "Activity" implies lawful actions capable of altering legal relations. This crime focuses on individual behavior and its legal consequences.

Clarifying the interpretation of the crime of aiding information network activities and educating citizens about this offense will help reduce judicial pressure and balance resource allocation. This can prevent the misuse of presumptions and misclassification of behaviors, protecting those who shouldn't be criminalized, such as farmers selling bank cards for minor profits. Due to unspecified perpetrators and concealed online transactions in cybercrime, law enforcement faces challenges, complicating judicial practice. Rational judgment in the judicial application of the crime of aiding information network activities is crucial.[7] Authorities should comprehensively evaluate the perpetrator's "aiding" behavior, considering its social harmfulness from multiple angles, avoiding subjective qualification solely for crime suppression. Crime combat should prioritize guidance and education to reduce crime incidence, preventing suspects from exploiting loopholes. Rational judicial application aids judges in making reasonable and lawful decisions, reducing conviction likelihood from a human rights angle, and tackling law enforcement challenges.

3.3. Strengthen the construction of online banking system and build a network security system

To reduce information network crimes, it's vital to strengthen banking network security. The rise of online banking has led to increased hacker and virus threats. Credit card usage has also surged, leading to more criminal activity. Boosting online banking security is crucial to cut down on these crimes.

Card issuers must implement strict safeguards, starting with comprehensive investigations during card issuance, including risk and creditworthiness assessments. Collaboration with security platforms is needed to monitor and protect cardholder transactions. Banking institutions must update their network security and develop modern, intelligent online banking systems to prevent credit card information leaks. Card issuers and banks must prioritize real-time transaction monitoring, closely watching online banking data and risks, establishing effective warning and prevention measures, and integrating early warning with controls to block information network crime channels, achieving a closed-loop approach to crime containment.

Combating crime relies on early warning and prevention to protect citizens' property and network security, reducing information network crimes. We oppose banking crimes that violate management systems and infringe upon property rights. Addressing credit card fraud requires collective efforts among individuals, society, and laws. [8] Prioritizing prevention, we must enhance our anti-fraud measures, promoting social governance modernization with Chinese characteristics, safeguarding people's interests.

4. Conclusion

This paper employs methods of big data analysis and case retrieval to examine the demographic characteristics, educational backgrounds, employment status, and actual case types of offenders involved in information network crimes. The findings reveal that the majority of perpetrators in these cases are young to middle-aged individuals with low educational attainment and a high proportion of unemployment. Furthermore, these cases exhibit a low conviction rate but a high crime rate.

The analysis also identifies four primary characteristics of information network crimes in telecommunication fraud cases: distinct technical attributes, exceptional concealment, profit-driven motives, and diverse case manifestations. Additionally, this paper delves into the underlying causes of the frequent occurrence of such cases. Firstly, these crimes are characterized by low costs, high returns, and quick financial gains. Secondly, offenders are typically young and lack a clear understanding of the criminality of their actions. Thirdly, the ambiguous identification of this crime in judicial practice, the prevalent phenomenon of "pocketing," and the challenges in detecting cybercrimes contribute significantly to the frequency of these offenses.

Based on these insights, this paper proposes four remedial measures to address issues in the judicial handling of these crimes. These include enhancing public awareness of the rule of law, refining internal control mechanisms, clarifying judicial determinations related to aiding information network crimes, and strengthening online banking systems. Overall, curbing the frequent occurrence of information network crimes in telecommunication fraud cases is a systemic endeavor that necessitates collaboration among families, schools, social institutions, online platforms, public security and legal authorities. By fulfilling their respective responsibilities and working in unison, these stakeholders can improve the governance system for such cases and better safeguard the legitimate rights and interests of Chinese citizens.

References

[1] Lizhi Wu, Xiaojia Zeng.Crime of assisting information network criminal activities research on the application of

justice[J]. Journal of Taiyuan Normal University (Social Science Edition), 2023, 22 (03), pp. 54-61.
[2] Zitong Feng, Ruiheng Wang. Assist in the investigation of the governance of the crime of information network criminal activities[J].Journal of Dalian Official, 2023, 39(08), pp. 58-64.
[3] Hongping Guo. Be wary of being an "accomplice" to online fraud [J]. Fangyuan Magazine, 2022 (7), pp. 7.
[4] Cuiping Li. Reflections on Computer Cybercrime and Prevention [J]. Journal of Jilin TV & Radio University, 2011(6), pp. 2.
[5] Wenlong Xue. Research on difficult judicial issues of the crime of infringing on citizens' personal information[D]. Shanghai Normal University, 2023.
[6] Shuyu Wang. Research on the causes and prevention measures of credit card fraud[J].Journal of Jiamusi Vocational Institute, 2022, 38(11), pp. 55-57.
[7] Tianhong Lu. The Judicial Application of the Crime of Assisting Information Network Criminal Activities: Current Situation, Controversy and Path Selection[J].Journal of Hebei Vocational College of Public Security Police, 2022, 22(3), pp. 52-55.
[8] Kai Zhang. A scientific and reasonable explanation of the question - comment two high network rumor judicial interpretation[J].Journal of Guizhou Police College, 2014, 26(03), pp. 41-47.