Journal of Education and Educational Research
ISSN: 2957-9465 | Vol. 7, No. 2, 2024

Characteristics and Countermeasures of Assisting Information Network Criminal Activities

-- Based on the Analysis of the Sample of the Judgment in a District of Chengdu

Guifang Luo [1], Yijie Hu [1,*], Lixia Fu [2]

[1] Graduate student in the Department of Law, Southwest University for Nationalities, Chengdu Sichuan, CO 610041, China
[2] Jinniu District People's Court in Chengdu City, Chengdu, Sichuan CO 610036, China

[*] **Corresponding author**: Yijie Hu (Email: 2915429489@qq.com)

Abstract: In the context of the era of big data, the crime of assisting in information network crimes (hereinafter referred to as "aiding and abetting crimes") has shown a high incidence and wide coverage, and it is also a key hub for many information network crimes, which seriously hinders the social management order and the property security of the masses, and undermines the normal, safe and orderly development of cyberspace. This article summarizes the types and characteristics of aiding and abetting crimes and the causes of their high incidence by analyzing the adjudication cases of aiding and abetting crimes in a district people's court in Chengdu in 2021 and 2022, and proposes corresponding governance measures to carry out necessary prevention and control of aiding and abetting crimes, in order to minimize the high incidence of aiding and abetting crimes and maintain social order and the legitimate rights and interests of the people.

Keywords: The Crime of Assisting in the Commission of a Crime; Assisting Behavior; Governance Measures.

1. Introduction

On March 2, 2023, the China Internet Network Information Center released the 51st Statistical Report on the Development of the Internet in China in Beijing. While the rapid development of the Internet brings convenience, it also poses great challenges to the governance of various new types of cybercrime. Different from traditional crimes, new types of cybercrime emphasize collaboration between upstream and downstream. The reason why it presents a high incidence trend cannot be separated from various "help behaviors" that provide support for information network criminal activities. In 2015, China promulgated the Criminal Law Amendment (IX) to add the crime of aiding and abetting crimes. In the early stage of the introduction of this crime, due to the lack of relevant judicial interpretations, coupled with the cautious attitude towards the identification of new crimes in practice, it has been in a "sleeping" state. In November 2019, the Supreme People's Court and the Supreme People's Procuratorate issued relevant judicial interpretations. The provisions of the Interpretation highlight the trend of severe punishment for cyber fraud crimes, strengthening the determination to "fight early and fight small" against cybercrime, and clarifying the relevant identification standards for aiding and abetting crimes. Only by completely activating the role of aiding and abetting crimes can we "help" them. According to statistics, in 2021, a total of 129,000 people were prosecuted for the crime of aiding and abetting crimes. In the work report of the Supreme People's Procuratorate at the "Two Sessions" in 2023, the latest summary was made on the development trend of the crime of aiding and abetting crimes in recent years. At present, the crime of aiding and abetting crimes is highly prevalent, involving a wide range of cases, seriously endangering the legitimate rights and interests of the state, society, and individuals. This article is based on the background of the overall national security concept, analyzes the existing verdict samples from the perspective of criminology, explores the reasons for the high incidence of the crime of aiding and abetting in crimes of obtaining illegal proceeds, and proposes corresponding countermeasures.

2. The Regular Characteristics of the Crime of Aiding and Abetting in the Use of Information Technology-- Taking the Existing Judgment of a District in Chengdu as the Analysis Sample

On July 17, 2023, the Anti-Electronic Fraud Office of the Sichuan High Court held a research meeting on social governance and judicial application of the crime of aiding and abetting in the Chengdu area at the Jinniu District People's Court. Chengdu is currently the city with the highest number of cases involving the crime of aiding and abetting in our province. The analysis sample used in this analysis is a total of 277 judgment cases from a district court in Chengdu in 2021 and 2022, which is highly targeted.

2.1. The Crime of Aiding and Abetting Crimes is Increasingly High

According to relevant research reports, the number of cases handled in 2021-2022 was only half of the total number of cases handled in the six years from 2015 to 2020.The number of cases has increased by 40 times, and the number of cases has increased by a spurt. The top three regions in our province with the highest number of cases of the crime of aiding and abetting in the use of information technology are Chengdu, Dazhou, and Yibin, with Chengdu accounting for one third of the province's total number of cases. The crime of aiding and abetting in the use of information technology accounts for a large proportion of related crimes involving telecommunications fraud. Among the upstream and

downstream crimes of telecommunications fraud tried in our province, the crime of aiding and abetting in the use of information technology accounts for more than 50%. Currently, the crime of aiding and abetting in the use of information technology has become the third most prosecuted crime among various types of criminal offences.

2.2. More Unemployed People and More First-time Offenders

Based on the existing 277 judgment samples, most of the involved persons are young adults without fixed occupations, mainly from the post-80s, post-90s and post-00s generations. Such subjects are mostly social idle people. They often hope to use faster ways to obtain a short-term income to meet their current needs, so "part-time jobs" with low economic and physical investment and fast income return characteristics are very attractive to such behavior subjects. Even if they know that the behavior may be helping others commit crimes, they still choose to take a chance and believe that they are only involved in the gray area and will not be labeled as criminals. And most of the people suspected of "aiding and abetting crimes" are first-time offenders. Among the 389 involved persons in the existing samples, there are 17 recidivists, accounting for only 4.37%.

2.3. The Perpetrators have Characteristics of Gender Differences

Based on the existing sample of 277 court verdicts, in the court verdicts of 2021, the proportion of cases where women alone committed the crime of aiding and abetting was 14.68%, while the proportion of cases where women and men jointly committed the crime was 6.42%. The rest were all male crimes committed alone or jointly. In the court verdicts of 2022, the proportion of cases where women alone committed the crime of aiding and abetting was 8.33%, while the proportion of cases where women and men jointly committed the crime was 3.58%. The rest were all male crimes committed alone or jointly.

Table 1. The proportion of men and women in the court of a district in Chengdu in 2021 and 2022

Year of Judgment	Female crimes alone	Women and men joint crime	Men alone or joint crime between men
Year 2021	14.68%	6.42%	78.9%
Year 2022	8.33%	3.58%	88.09%

3. Reasons for the High Incidence of Cases of Aiding and Abetting Crimes

3.1. The Perpetrator is Greedy for Small Profits and has a Sense of Luck

The "cost-benefit" theory was proposed by Gary Becker. Crime costs and benefits are important factors that affect the implementation of crimes. When the crime costs are significantly lower than the crime benefits, the perpetrators are more likely to commit crimes. Payment and settlement, as the main criminal means of the crime of aiding and abetting, are characterized by easy profit and low cost. Most teenagers have shallow social experience and weak legal awareness, and they are easily tempted to believe in the "make a fast buck" message on the Internet. In order to make a small profit, they become accomplices of others; according to Article 287 of the Criminal Law, there are many different types of assistance behaviors in the crime of aiding and abetting. The cost input of each behavior type varies greatly, and the payment and settlement type assistance behavior dominated by selling telephone cards and bank cards can be described as a zero-cost crime. Therefore, in practice, criminals who provide paid telephone cards and bank cards for others to use and provide payment and settlement methods for others are identified as criminals who commit the crime of aiding and abetting, which accounts for a very high proportion of this crime.

3.2. Due to the Concealment of Cyberspace Reduce the Risk of Crime

As a rational criminal, before committing a crime, the first step is to estimate the likelihood of the criminal behavior being discovered, that is, how likely it is that they need to bear legal responsibility for the criminal behavior. Compared to high-risk crimes such as intentional homicide and robbery, low-risk crimes are more favored by criminals. The temporal and spatial context of the crime of aiding in crime has concealment and privacy, greatly reducing the risk of crime. Analysis of existing samples reveals that there are two spatiotemporal contexts for the crime of aiding in trust. One is the virtual cyberspace. The inherent characteristics of the network world make the crime of helping and trusting have a certain invisibility. suspect can commit crimes in any corner of the world through the virtual Internet, which is also the reason why many network fraud criminal groups have been stationed abroad for a long time. When criminals use cyberspace as a crime scene, they communicate through codes and codes to evade online supervision. Once discovered, they immediately destroy electronic evidence, greatly reducing the risk of crime and increasing the difficulty of case investigation. Second, public places and private spaces that are not easily noticed. The former include tea houses, restaurants, etc., while the latter include hotels, homestay rooms, etc. Although such criminal situations do not have the virtual characteristics of the Internet, the hidden nature of public places and the concealment of private spaces are not easily detected by others.

3.3. The High Incidence of Telecommunications Network Fraud Intensifies the Crime of Aiding and Abetting.

The high incidence of the crime of aiding and abetting in the use of information technology is positively correlated with the high incidence of telecommunications network fraud. As the domestic crackdown on telecommunications network fraud increases, criminal personnel are shifting to Southeast Asia and other overseas regions to commit fraud against Chinese residents. Overseas criminals are highly hidden and their crimes are dispersed, making it difficult to crack down on them. However, such criminals commit fraud against Chinese residents, and the flow of funds obtained from fraud often requires domestic personnel to provide relevant technical, payment and settlement support. The high incidence of telecommunications network fraud and the difficulty of cracking down on it have, to a certain extent, induced the crime of aiding and abetting in the use of information technology. In practice, judicial personnel often

easily capture the perpetrators who sell "two cards" through real-name authentication, bank statements, and other anomalies. However, "card heads", "card traders" and more entrenched subordinates in overseas upstream criminals are much more hidden, making it difficult to grasp their identity information and location information. Moreover, such criminals have a strong sense of counter-investigation and are difficult to detect.

3.4. The Supervision of Relevant Institutions is not in Place

The reason why payment and settlement can become the main criminal means in the case of aiding and abetting crimes is that on the one hand, its threshold is low, and on the other hand, the supervision of banks, telecommunications operators, market supervision departments, etc. is not in place, leaving room for criminals to take advantage of it. First, the supervision of relevant departments of banks is not in place, and there is a formalized examination of the verification of the establishment of corporate accounts by companies and enterprises. Under the environment of complying with banking supervision regulations, there are different situations regarding the strict and loose standards for opening accounts among banks. Some criminals aim at this loophole and handle multiple accounts at the same bank in some regions. Criminals often use the loopholes in the supervision information sharing among banks, data barriers, and transmission delays in mobile phone card handling information to handle accounts at multiple banks and business halls for multiple times, which provides assistance for their information network crimes. Second, the market supervision registration review is not in place, which provides a convenient way for buying and selling corporate accounts. The proliferation of "scalpers" in industrial and commercial registration, as well as the low cost and simple procedures for opening corporate accounts, make it extremely easy to establish corporate accounts. In many cases, criminals use forged documents to register business licenses through government "XX office" APPs, and use business licenses to open corporate accounts and sell them to others for criminal activities.

4. Governance of the Crime of Assisting in the Crime of Information Countermeasures

4.1. Strengthening the Publicity of the Rule of Law and Enhance the Concept of Rule of Law

According to the above analysis of the article, the main actors of the crime of aiding and abetting crimes are mostly young men with low educational backgrounds, and most of them are first-time offenders. With the advent of the era of big data, the Internet has continuously integrated into our daily lives, and young people have more opportunities to encounter new things and have strong learning abilities. However, due to the lack of social experience of young people with low educational backgrounds, in the face of "different styles" of recruitment information on the Internet, their ability to identify is weak, and their self-control ability when facing temptation is not in place, which is likely to lead them to commit crimes.

In view of this, relevant departments should increase their efforts in promoting legal education in society. For example, in the existing samples, many students from vocational and secondary schools have joined the "part-time brushing" positions, providing their bank cards for others to use for a small profit. We can increase the publicity efforts for these schools by introducing public security, procuratorial and legal education into the campus, so that these young people who are not deeply involved in the world can understand the relevant provisions of the crime of aiding in trust, understand what kind of behavior will violate the crime of aiding in trust, and avoid falling into the abyss of crime; For idle and unemployed individuals in society, publicity can be carried out through easily accessible means, such as recording relevant propaganda content on standby screens in internet cafes, KTVs, and other places, such as "Be wary of helping others commit crimes.". Only by helping the public understand the hazards of selling bank cards, WeChat, Alipay and other personal accounts to others, establishing correct legal awareness, and strengthening the awareness of prevention of helping and trusting crimes, can we effectively reduce the occurrence of helping and trusting crimes from the source.

4.2. Upgrade the Risk of Crime Increase the Cost of Crime

Strengthen the supervision of crime scenes, increase the likelihood of crime being detected, and achieve the goal of deterring crime. One is to improve the real name system for internet platforms. Network service providers themselves should establish a correct legal perspective, do a good job in real name authentication, require users to provide real identity information for registration, refuse to provide "human relations" services, and refuse to provide network services for those who cannot provide identity information or whose information verification is false. In addition, the current network authentication mostly uses SMS verification code, ID number and other methods to verify and log in. Some platforms can also choose to log in through a third party such as QQ. Helping the helped people in the crime of trust, by using a simple authentication method, they can purchase other people's real name authenticated social accounts, send recruitment information such as "part-time job, swiping orders" and buy a large number of "double cards" or commit fraud. Therefore, digital identity certificates can be used with intelligent USBKEY as the carrier and network identification symbols generated by fingerprints and ID number as the content, or real name registration can be carried out by using the method of "mobile phone number+ID card information+ face recognition". The second is to build a unified monitoring system. Telecommunications, finance, internet and other institutions should improve their monitoring mechanisms in this field. Communication institutions should improve the monitoring mechanism for identifying abnormal numbers and promptly identify and handle abnormal situations; Financial institutions should strengthen the monitoring of suspicious online transactions and take corresponding measures in a timely manner for abnormal financial accounts; Internet institutions should strengthen long-term monitoring and prevention mechanisms, and focus on monitoring, intercepting, and disposing of illegal and criminal accounts. In addition, when the cost of the crime of aiding and abetting is low and the benefits are high, even if there is a risk of being arrested for committing the crime, some criminals will still have a sense of luck and choose to take the risk and commit

the crime. Therefore, we should step up the fight against the black market, such as social platforms for "double card" transactions, communication equipment trading markets such as Duobao Card and Luomanbao, and fourth-party payment platforms or foreign exchange platforms; we should improve the online transaction supervision mechanism, strengthen the background review of transaction personnel, and timely detect and feedback transaction clues suspected of aiding and abetting information network crimes.

4.3. Insist on Source Governance and Crack Down on Telecommunications Fraud

For the governance of the crime of aiding and abetting in the use of information technology, in addition to cracking down on the crime itself, it is necessary to trace its roots and severely crack down on upstream crimes, curbing the demand for financial circulation channels from the source, and striving to eradicate the breeding ground for the crime of aiding and abetting in the use of information technology. First, continue to promote the "stopping cards" special action. The public security organs, procuratorial organs and judicial organs should unify their law enforcement and judicial concepts, refine their case handling standards, and crack down on crimes effectively and efficiently. Second, carry out in-depth "strike and rectify telecommunications network fraud" special action, paying special attention to telecommunications network fraud cases involving elderly people's pension. Crack down on them in a quick and strict manner according to law. Third, actively participate in the prevention of "fund chain" governance of telecommunications network fraud. Add "case verification, cause investigation and management functions" to the case handling system of the public security organs, procuratorial organs and judicial organs, discover and collect bank card information related to telecommunications network fraud, and promote the implementation of disciplinary measures for individuals who buy and sell bank cards and accounts. In addition, the modernization of national governance system and governance capacity is being comprehensively promoted. The governance capacity in the field of digital network is an indispensable part of the governance system and an important requirement for modernizing governance capacity. As a crime closely related to various types of cybercrime, aiding and abetting in the use of information technology is mainly a service provided for various types of cybercrime. Therefore, the public security organs, procuratorial organs and judicial organs should focus on improving their data governance capabilities, strengthen data sharing and communication among various departments, transfer criminal clues in a timely manner, and use relevant data support to predict crimes. The greatest possible prevention of aiding and abetting in the use of information technology should be carried out from the source.

4.4. Strengthen Institutional Supervision and Review Doubtful Accounts

Since the launch of the "Card Blocking Action" in 2020, significant results have been achieved in cutting off the channels for cybercrime from the source of opening new cards, and it should be continued to be implemented. At the same time, as criminals cannot open new bank cards, they turn to "card farmers" to purchase bank cards for payment and settlement. Relevant departments of banks should conduct self-inspection in a timely manner, suspend the implementation of various businesses for blank bank cards that have not been used by customers for a long time, and prevent them from becoming "card farmers".

In response to the current problems of easy application for corporate accounts and difficult follow-up management, two reference measures are proposed: First, from the source, reduce the registration of abnormal "shell companies". Relevant market supervision departments should avoid "formal review" in the process of handling business license registration for applicants. Pay attention to verifying whether the registered address of the enterprise is real and whether the registered address is the general business address of the enterprise. For enterprises that have or may have abnormal conditions that do not meet registration standards, they should be refused to handle business licenses. At the same time, for enterprises that do not have the aforementioned circumstances and have been approved to handle business licenses, corresponding supervision and management measures should be formulated, and they should be visited at any time. Do not "let them do it". If problems are found in the visit, they should be required to make timely compliance corrections or take corresponding control measures. For enterprises that refuse to rectify or have major violations of laws and regulations, their business licenses should be revoked. Second, implement the follow-up management work well. Banks must strengthen their attention to the use of corporate accounts opened by them and continue to do a good job in follow-up visits. For accounts with suspicious conditions such as abnormal transaction time, frequent transactions in a short period of time, and huge transaction amounts, timely control measures should be taken to prevent further losses. At the same time, banks should arrange special personnel to carry out annual inspections of corporate accounts, focusing on verifying whether the enterprise is in operation. For enterprises that have stopped operating, they should be handled according to relevant regulations, and cannot leave room for criminals who resell corporate accounts.

4.5. Maintain a High-pressure Situation and Appropriately Increase the Fine Penalty

Considering that the crime of aiding and abetting crimes is mainly a profit-making crime, and the current fine scale is relatively low, it is appropriate to increase the number of fines to increase the expected crime costs of the perpetrators, so that they can deeply understand the "loss outweighs gain" and prevent the risk of re-offending. In practice, there are still cases where the application of fines is not uniform. Taking the existing samples as an example, defendant Liu, who was charged with aiding and abetting crimes, provided bank cards for payment and settlement, with a settlement amount of 11 million yuan and illegal proceeds of 32,200 yuan. He was sentenced to eight months' imprisonment and fined 7,000 yuan. The defendant Song, who was charged with aiding and abetting crimes, paid a settlement amount of 5.19 million yuan and obtained illegal proceeds of 10,000 yuan. He was sentenced to ten months' imprisonment and fined 9,000 yuan. Comparing the two cases, although Liu's payment settlement amount was higher than Song's, and his illegal proceeds were higher than Song's, Song's fine was higher than Liu's. When proposing procuratorial suggestions and making final judgments, the procuratorial organs should comprehensively consider the defendant's criminal facts and unify the use of fines. The fine should be commensurate with the crime. The crime of aiding and abetting in the use of information

technology is a property loss for the victim, and does not pose a direct personal risk. The risk is far lower than traditional violent crimes such as theft and robbery, and it is not appropriate to punish it as a serious crime. China's Criminal Law stipulates that the maximum statutory punishment for the crime of aiding and abetting in the use of information technology is three years, which reflects the principle of proportionality. The author does not agree with some academics who propose that the maximum statutory punishment should be increased.

5. Conclusion

At present, information network crimes such as telecommunications network fraud are increasingly occurring with the development of information network technology. Such crimes are mostly committed by groups, and the core of the group is mostly based overseas. The crime shows obvious characteristics of chain and industrialization. The activity of cybercrime cannot be separated from the promotion of information-aided network activities. Therefore, it is necessary to place the fight against the crime of aiding and abetting in the prominent position of the governance of information network crimes such as telecommunications network fraud, and strive to cut off the supply of telephone cards and bank cards, so that criminals dare not commit crimes and cannot commit crimes. Based on the analysis of the characteristics and causes of the crime of aiding and abetting in the sample of judgments in a district of Chengdu in 2021 and 2022, in the future crime prevention and control, relevant subjects should continue to maintain a high-pressure situation, strive to minimize the criminal gains, strengthen supervision and publicity of the rule of law, increase domestic and foreign collaborative efforts, and combat cybercrime throughout the entire chain.

Acknowledgments

Thank to Associate Professor Bin Hou from the Law School of Southwest University for Nationalities and Judge Lixia Fu from Jinniu District People's Court in Chengdu for your guidance and support on this work. This work has been funded by the Southwest University for Nationalities Graduate Innovation Research Project (Project No. ZD 2023954) and is the result of the Southwest University for Nationalities Graduate Innovation and Entrepreneurship Key Project.

References

[1] Yujia Fang, Song Zhang, “The regulatory logic and development trend of aggregated payment”, China Credit Card, 2017 (05): 53-55.

[2] Yuqiu Ye, Tao Sang, Shen Panpan, “Research on Several Issues in the "Disrupting Card" Action Cases”, China Procurator, 2021(14): 26-31.

[3] Wei Xu, Ye He, “The formation mechanism and prevention and control countermeasures of college students' helping information network criminal activities - based on an empirical analysis of 327 criminal cases”, Juvenile Delinquency Issues, 2023(03): 18-28.

[4] Yuanhong Lin, “Exploration on the prevention and control of the crime of assisting in information network criminal activities”, Cyberspace Security, 2023, 14(02): 98-102.