Social Security and Administration Management (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/socsam.2023.040503
ISSN 2523-5796 Vol. 4 Num. 5

Research on Multiple Cooperative Governance Mechanism of Telecom Fraud under the Background of Internet+

Kong Wei

China Jiliang University, Hangzhou, 310018, China

Keywords: Internet plus, Telecommunication fraud, Collaborative governance, Related measures

Abstract: Under the background of internet plus, the high development of network technology has not only greatly promoted the social economy, but also attracted the peep of some lawless elements, and led to the characteristics of transnational, accurate, organized, professional and hidden telecom fraud cases in China. Therefore, the current telecom fraud gangs are gradually showing the embryonic form of industrial operation. If they are not stopped in time, it will inevitably lead to its large-scale expansion, which will cause serious losses to the personal property safety of the people. Therefore, this paper first analyzes the development status of domestic telecom crimes in recent years. Then, it summarizes the main characteristics of telecom fraud cases and the difficulties in detection, and puts forward the management measures of telecom fraud cases based on the multi-collaborative governance mechanism, hoping to play a certain reference role and realize the source governance of telecom fraud crimes.

1. Introduction

In December, 2022, the state promulgated the People's Republic of China (PRC) Anti-Telecommunication Network Fraud Law, which marked the official implementation of the first special legislation against telecommunication network fraud, and clearly put forward that “Adhere to the concept of system, think under the rule of law, pay attention to source management and comprehensive management; Adhere to joint management, group prevention and group governance, fully implement various measures for prevention and control, and strengthen social publicity and education. “ Under the background of the new era, many telecom fraud cases in China have gradually become professional and high-tech, and even a complete industrial chain has emerged in the process of development. Therefore, it is very difficult for the public security system to crack down. In view of this situation, the relevant departments need to adopt a multi-linkage model and agree to adopt a key prevention attitude against the phenomenon of electronic fraud subculture, so as to effectively change the traditional “attack-oriented” into “prevention-oriented” and reduce the occurrence of telecom fraud crimes from the source.

2. The Development Status of Telecom Fraud Crime

According to the statistical data of the Supreme People's Court, China, during the period from 2017 to 2021, 103,000 telecom fraud cases were concluded nationwide, involving 223,000 people and sentenced. At the same time, the Ministry of Public Security of China mentioned in the press conference that by the end of November 2022, 391,000 telecom fraud cases had been detected nationwide, and the number of criminal suspects arrested increased by 64.4% year-on-year, resulting in a 1.3% year-on-year decrease in the total value of property losses. Among them, 240 leaders of electric fraud criminal gangs were arrested in the three campaigns of “cutting the chain”, “Qingyuan” and “Sword”.

According to the data, China's public security departments have taken a series of effective measures against telecommunication network fraud cases, and gained ideal governance effects in the process. However, due to the continuous development of network technology in recent years, the occurrence of telecom fraud is no longer confined to the physical level, and it has begun to show the characteristics of concealment, specialization, diversification and technicalization. Therefore, people are also not allowed to relax their guard, and they need to further transform their work ideas in order to continue to expand their achievements. Therefore, under the background of the new era, relevant departments need to take the initiative to focus on “front-end prevention” mitigation, and actively take multi-governance measures to strengthen the crackdown, so as to effectively control the occurrence of telecom fraud crimes [1].

3. The Main Characteristics of Telecom Fraud Cases in the Context of Internet Plus

(1) Precision

Under the background of “internet plus”, people's work and life are inseparable from network software, and they often leave personal privacy information when browsing the web. As a result, under the influence of many factors, such as program loopholes, phishing websites and internal staff leaks, it is easy for people's personal information to be obtained by pacemakers, which leads to the precise characteristics of telecom fraud in the implementation process. Criminal gangs can “privately order” exclusive fraud schemes according to the actual situation of the victims, making it difficult for the masses to effectively identify and prevent fraud incidents.

For example, in April, 2022, Zhang's street in Quanzhou, Fujian Province swindled the phone, and the other party lied about the customer service staff of the shopping platform, and accurately reported the order number, time and logistics order of Zhang's latest shopping, and claimed that the goods had been lost, and negotiated a compensation plan with Zhang. Later, under the guidance of the other party, Zhang Mo added the contact information of the payment software, and unified the money in the account into the other party's account, and even asked for further cooperation in downloading the online loan APP software for overdraft, with a total loss of 25,000 yuan.

(2) Specialization

At this stage, due to the continuous development of network technology, the deception methods of telecom fraud gangs are more intelligent and professional, which makes it difficult for many victims to detect fraud at the first time when they face fraud. For example, in 2022, in the process of understanding the knowledge of stock trading, Beijing citizen Yu added friends with a personal IP who claimed to be “Big V”, and installed an APP application software under the guidance of the other party, and then followed the other party's “suggestion” to make online investment and successfully withdrew 373,000 yuan. Yu felt that the profit was quite objective, so he transferred 3.47 million yuan for buying and selling stocks ten times before and after. It was not until more than 3 million yuan in the account was completely frozen that it was completely blacked out when contacting the other party [2].

This kind of telecom fraud means is usually that criminal gangs confidently build a false trading platform, which seems very formal, but in fact there are huge hidden dangers inside. Fraudsmen often combine some professional financial knowledge to defraud the victim's trust, and control the rise and fall of “stocks” by adjusting the data in the background, so as to induce the victim to increase the investment amount and realize the purpose of defrauding the victim's property in disguise.

(3) Organization

At present, thanks to the convenience and various forms of Internet communication, the current domestic telecom fraud crime has gradually developed from gang crime to organized crime, and its internal links have the characteristics of orderly operation, unconnected and well-organized, which leads to higher fraud efficiency and wider harm.

For example, the current telecom fraud group includes script making team, information collection team, bank card processing team, hacking technology and web page writing team, and so-called “water room group” and “traffic group” and so on. Such organizational characteristics enable telecom fraud to form a complete black-gray industrial chain from obtaining victim information to successful property transfer, and to complete the crime in the shortest time and re-conceal it. And each link is completely isolated physically, even if one end of the organization is exposed, it will not affect others, and it can resume operation in a short time. Therefore, it greatly increases the difficulty of governance, and it is difficult to completely eradicate telecom fraud gangs [3].

(4) Transnational

Through the investigation of telecom fraud cases in recent years, it can be found that most of the current fraud gangs are from coastal cities in China, such as Fujian and Guangdong. At the same time, these organizations generally set up pseudo base stations in Africa, Thailand, the Philippines, Malaysia, Cambodia and even southern Europe where the social environment abroad is chaotic, and then use the network platform to commit fraud crimes against domestic people. For example, in September 2019, the police in Shaanxi Province cracked eight telecom fraud cases, and the gang dens were all established in the Philippines and other regions, and 301 suspects were arrested by extradition.

The reason for this feature lies in the fact that people's economic exchanges under the current Internet background have no time and space constraints and can be carried out freely in cyberspace. As a result, many fraud criminal groups have adopted a low-risk operation mode of “cross-border crime”, which can not only realize remote control and command, but also quickly transfer the amount involved to different countries, making it more difficult for public security departments to follow up and investigate.

4. The Way to Build a Multi-Collaborative Governance Mechanism for Telecom Fraud in the Context of Internet Plus

(1) To create an internal linkage mechanism of the public security system

At present, due to the continuous development of Internet technology, the current telecom fraud groups are scattered, and the related industries and criminal chains are extended, which makes the public security departments face great difficulties in the process of obtaining evidence and arresting. In view of this situation, the public security internal system needs to change its own investigation mode according to the development characteristics of telecom fraud cases, actively rely on the network platform to build a national police information website, and at the same time adopt a cooperative investigation mode of multi-regional cooperative investigation for telecom fraud cases, so as to comprehensively improve the efficiency of mobile response of public security departments to fraud cases [4].

For example, in the process of detecting some inter-provincial telecom fraud cases, the criminals

are widely distributed and the victims are located in many parts of the country. Therefore, in order to obtain criminal evidence quickly, the public security department can share the case information with different public security organs through the police information platform, especially inquire, count and investigate the victims of the case respectively, and upload the obtained victim statements and case clues to the police platform to sort out the evidence chain in a unified way, so as to grasp the complete criminal facts of the fraud gang within the prescribed time limit. On this basis, the public security department set up the corresponding task force members to be responsible for the unified dispatch of local police forces and centralized arrest and interrogation of relevant people involved in the case, thus effectively eliminating criminal gangs. Tonggu Zeyang's way can not only effectively reduce the difficulty of handling cases, but also ensure that members of fraud organizations scattered in different regions can be caught in the net, which can avoid omissions and fugitives to the greatest extent.

(2) The establishment of overseas judicial cooperation system.

The continuous development of network technology provides great convenience for the implementation of telecom fraud crime, and makes it successfully spread to the direction of “no borders”, which greatly affects the governance efficiency of domestic judicial organs. Therefore, under the background of the new era, the public security department needs to take the initiative to adopt the way of overseas judicial cooperation to enhance the efficiency of monitoring and tracking telecom fraud, and then effectively improve its own work efficiency. Specifically, it includes the following measures:

1) Information sharing mechanism. In view of the current characteristics that telecom fraud groups generally adopt transnational operations, domestic judicial departments need to actively strengthen information sharing and cooperation with foreign ideological departments, so as to be able to more closely grasp the evidence of criminal groups' actions and achieve the purpose of prevention and control in advance. For example, the judicial department of our country can contact the local judicial department and ask the local police to conduct surveillance and investigation in advance after investigating and obtaining evidence or analyzing the gathering dens of criminal suspects in a foreign country. However, foreign judicial departments have the obligation to collect personnel information and verify with China after discovering that a number of overseas personnel suddenly appear in this area to live in groups, so as to determine whether there are telecom fraud suspects [5].

2) Law enforcement rights in different places. From the previous practical experience of international judicial assistance, in most cases, in the process of tracking cross-border crimes, local judicial organs can only be asked to investigate on their behalf in the form of “entrustment”, which will not only cause certain information gap, but also increase the local law enforcement burden invisibly, which is not conducive to obtaining good evidence collection results. Therefore, in the current situation of cross-border fraud organizations becoming more and more rampant, China's judicial organs need to establish judicial agreements with relevant foreign departments as soon as possible, giving the public security departments certain power to enforce the law in different places or cooperate with investigations to a certain extent, thus further enhancing work efficiency.

3). Initiate an extradition treaty. It is necessary to establish perfect legal extradition regulations and form a long-term and stable judicial cooperation relationship for the countries that are hardest hit by telecom fraud, such as Vietnam, Malaysia, Cambodia, Philippines, Indonesia, Myanmar and so on, so as to further strengthen the pursuit and investigation of criminals abroad.

(3) The establishment of enterprise collaborative supervision and operation mechanism

1) Improve legislation and standardize business practices. At present, with the development of telecom fraud in the direction of specialization and intelligence, its relationship with telecom operators, network technology enterprises and banks and other financial institutions has become increasingly close, and some loopholes in the company's operating system are often used to implement fraud, which greatly increases the difficulty of telecom fraud prevention. Therefore, the

judicial organs need to further improve the relevant laws and regulations, and further clarify the regulatory responsibilities of related industries in view of the development trend of telecom fraud cases in recent years, so as to standardize the business operation mode and reduce the incidence of fraud.

2) Strengthen interaction and establish an interview mechanism. At present, in the process of business development, telecom, network and other related enterprises should not only cooperate with the public security departments to strengthen the prevention and control of fraud crimes, but also actively provide certain technical and human support, and jointly establish a perfect protective wall mechanism with the help of high-tech resources they have mastered, so as to dynamically grasp the flow of fraud funds and trace the source of information with the public security organs. For this reason, the grass-roots public security departments can set up a special telecom fraud management team, which is responsible for taking the initiative to conduct docking interviews with enterprises in the daily work process to ensure that they can cooperate with the work needs of the public security departments to jointly collect criminal evidence of fraud groups [6].

3) Strengthen supervision and curb violations. The public security department needs to strengthen the supervision and management of related enterprises, and comprehensively grasp the business information of enterprises through the supervision and analysis of the business data of business outlets to avoid illegal operation in their daily operations. For example, whether there are more than a specified number of accounts or SIM cards for one person in a bank or telecom business hall; Whether there is a single-day cash withdrawal amount of more than 20,000 in an individual account, and so on. In order to ensure that the loopholes in business operations can be effectively eliminated and to avoid providing opportunities for criminals.

(4) Build a multi-theme joint publicity pattern

Telecom fraud not only takes a lot of police and material resources to track after the incident, but also the property losses suffered by the masses are often difficult to recover completely. Therefore, local public security departments need to take the initiative to change the focus of their work and move the former “detection-oriented” to the “prevention-oriented” link, so as to effectively improve the governance efficiency of telecom fraud.

For example, the public security department can take the initiative to cooperate with sensitive institutions such as communities, schools, hospitals, banks and online shopping platforms, and adopt multi-measures to strengthen education and publicity work to ensure that the occurrence of online fraud can be reduced from the root cause. For example, if advertisements are put in the city subway, some common fraud methods will be listed, so that the masses can master effective measures to identify telecom fraud during the ride; Another example is to arrange special personnel to be stationed in front of the ATM of the bank, find out the abnormal customer groups in time, and dissuade them and understand the situation. So as to ensure that the occurrence of telecom fraud can be effectively reduced.

5. Conclusion

To sum up, this paper discusses and studies the multi-collaborative governance mechanism of telecom fraud under the background of “internet plus”. It is emphasized that on the basis of strengthening judicial governance, relevant departments should take the initiative to cooperate with social pluralistic institutions to carry out supervision and control, so as to ensure that governance efficiency can be effectively strengthened and the property safety of the people can be further guaranteed.

References

[1] Shan Yong. Governance transition, the crime that digital society is going to the front-end-centered on "People's Republic of China (PRC) Anti-Telecommunication Network Fraud Law (Draft)" [J]. Journal of Shanghai Normal University (Philosophy and Social Sciences Edition), 2022, 51(3):58-66.
[2] Xie Ling. Research on capital flow control of telecommunication network fraud crime [J]. Journal of Chinese People's Public Security University (Natural Science Edition), 2021, 27(2):47-55.
[3] Chen Zhenxing, Dong Hanwei, Hao Qing, et al. Construction and analysis of index system of influencing factors of telecom fraud susceptibility [J]. Journal of Xi'an University of Science and Technology, 2022, 42(2):389-396.
[4] Jia Guowei, Cui Jipeng, Wang Shunbing, et al. Research on countermeasures against telecommunication network fraud with the help of science and technology [J]. Journal of Shandong Police College, 2022, 34(2):126-131.
[5] Tang He, Zhao Min. The evolution and governance path of "Shazhupan" telecommunication network fraud crime model-based on the analysis of the regulatory effect under the influence of network media [J]. Journal of Chinese People's Police University, 2022, 38(12):12-17.
[6] Qin Changsen. The type judgment and limitation of aggravated crime of fraud-taking telecommunication network fraud as the breakthrough point [J]. Journal of Jiangsu Ocean University (Humanities and Social Sciences Edition), 2022, 20(2):25-36.