ISSN: 2688-9323

Research on Comprehensive Treatment of Telecom Network Fraud

Yan Wang

Chongqing University of Posts and Telecommunications, Chongqing 400000, China

Abstract

The intensified telecom fraud has deeply infringed people's legal rights and interests, and disturbed social order. This paper, based on literature research, investigation and cases analysis, explores the origin of telecom fraud, summarizes its common types, characteristics and bad impacts, discusses the causes of the existing situation, and proposes solutions, that is, to focus on the hard and the serious, to improve technology against fraud, to enhance the rule of law, to intensify punishment, to unify people from different walks of life, and to strengthen regulation.

Keywords

Telecom Fraud; Comprehensive Control; Solution.

1. Introduction

With the rapid development of information technology, telecommunications network fraud is threatening. Due to its low cost and easy replication, many criminals abandon theft, drugs, robbery and gambling to engage in this criminal activity, resulting in an increase in the incidence of fraud for a period of time. Telecommunications network fraud not only endangers the safety of people's lives and property, but also seriously disturbs social security. In order to protect the legitimate rights and interests of the people and maintain social stability and harmony, the Chinese government has adopted a "zero tolerance" attitude towards the big cancer of telecom network fraud, and has actively introduced a series of targeted policies to prevent and accurately crack down on telecom network fraud since 2016. With the "great wall-2020" fraud and the "great wall-510" scam, a large number of scammers have been severely cracked down. However, the current governance model is difficult to eradicate telecom network fraud. Telecom network fraud presents the characteristics of repeated prohibition, repeated deception, repeated success, repeated Deception (fast means update), repeated deception, repeated precision (accurate fraud), repeated deception, repeated wide (cross-border fraud), strong concealment, industrial chain and great harm. The traditional governance model and Countermeasures of relevant departments to crack down on telecom network fraud.

The means are facing great challenges. We need to constantly innovate the governance concept and strengthen the comprehensive management of telecom network fraud from the overall situation of comprehensive management of social security.

2. Overview of Telecom Network Fraud

2.1. Related Concepts of Comprehensive Treatment of Telecom Network Fraud

Telecommunications network fraud refers to the criminal act of fraudsters deliberately transmitting various kinds of false messages to the fraudster by using mobile phones, networks, and other communication methods to induce the fraudster to transfer money. The comprehensive treatment of telecom network fraud refers to the formation of a joint force and the use of law, administration and culture under the unified leadership of Party committees and

ISSN: 2688-9323

governments at all levels, with political and legal organs as the backbone and relying on the strength of the people and all aspects of society.

Means to punish the crime of telecommunication network fraud, transform the elements of telecommunication network fraud, educate and save the personnel who fall into the crime of telecommunication network fraud without subjective will, prevent the crime of telecommunication network fraud, maintain social order, protect the safety of people's property and other legitimate rights and interests, and maintain social stability and harmony.

2.2. Tracing the Source of Telecom Network Fraud

Telecommunications network fraud originated in Taiwan. The people of Taiwan are deeply poisoned by telecommunications network fraud and rated it as the first of the top ten public grievances. According to the statistics released by Taiwan consumer culture and education foundation, the amount of fraud in Taiwan in 2006 alone was as high as NT $656.06 million. In 2005, with the continuous improvement of anti-fraud awareness of Taiwan people, Taiwan police implemented a series of measures such as setting up "165 anti-fraud consultation telephone" and severely cracking down on telecom network fraud. Therefore, Taiwan fraud gangs turned their eyes to the mainland, South Korea, Thailand, Vietnam, Singapore, Malaysia and other places to commit fraud.

2.3. Types, Characteristics and Hazards of Common Telecom Network Fraud

2.3.1. Common Types of Telecom Network Fraud

Relevant data show that at present, China's telecom network fraud is mainly divided into five categories: Loan (32.5%), impersonating customer service (13%), Bill brushing (17%), impersonating public security law and killing pigs.

In the loan type telecommunication network fraud, the fraudsters caught the borrower's eagerness for success, negligence and other psychology, woven various reasons (handling fee, material fee, deposit, etc.) to deceive the borrower into taking the bait, charged fees in advance, and lost contact immediately after the money was entered into their own account.

"Customer service calls" such as quality claim settlement, express lost refund, careless financial transfer and wrong account are common tricks of telecom network fraud pretending to be customer service. Such fraud is closely related to people's daily life. Inexperienced school students, unemployed at home and social young people with low education and low salary often fall into the trap of "swiping the bill to earn pocket money" because of their low income and more leisure time, and then encounter swiping telecom network fraud.

Although the incidence of impersonating the public security organ and killing pigs is not high at present, the amount involved is large, ranging from hundreds of thousands to millions. The harm is prominent and seriously infringes on the safety of people's property.

2.3.2. Characteristics of Telecom Network Fraud

First, technical. Fraudsters illegally use various technologies and equipment to defraud, including artificial intelligence, machine learning, big data mining, pseudo base station, number change software, trojan virus, free WiFi and other technologies, as well as host computers, laptops, mobile phones, SMS group senders, SMS senders, bank card thieves, "cat pool" (network telephone group call transfer agent platform), goip, "multi card treasure" and other equipment.

Second, concealment. In order to achieve the purpose of hiding their identity and evading the attack, fraudsters often choose to remotely use goip devices to make fraud calls and send and receive text messages. Once they are aware of the danger, they will escape to the small cities on the China Myanmar border to take shelter from the wind, and carry out fraud activities again after the wind. Even if the judicial authorities spend a lot of human, material and financial

ISSN: 2688-9323

resources to handle cases, most of them catch the bottom of the telecom fraud industry chain, such as "drivers" and "horsemen" (responsible for bank withdrawal), and the behind the scenes perpetrators are still at large.

Third, group. In a large number of fraud cases, fraudsters do not act alone, but commit gang crimes in an organized and planned way. In order to avoid and reduce the crime risk, many fraud gangs employ personnel in the name of company recruitment and clarify the level and division of labor of "employees". Taking online prize-winning fraud as an example, special personnel are responsible for opening a bank account, sending fraudulent emails, inducing the fraudster to remit, withdraw money, money laundering and other links.

Fourth, accuracy. Fraudsters obtain citizens' privacy information through illegal channels, including personal basic information, occupation, recent areas of concern, etc., and customize fraud techniques for individuals. In Xu Yuyu's case, Xu Yuyu just applied for financial aid at the local education bureau. Two days later, she received a fraudulent call for financial aid. This kind of precision fraud has become the mainstream fraud mode. It is deceptive and confusing. It is impossible to prevent it. It is difficult for people who are cheated to see through the scam.

Fifth, diversity. According to the monitoring statistics of China Academy of communications, renzihang Network Technology Co., Ltd. and other units, there were more than 260 new fraud methods between January and October 2020 alone. Moreover, fraudsters no longer repeat the old-fashioned fraud, and the fraud mode is rapidly upgraded. Multi-link, multi technique and multi-platform fraud is the norm. It must be said that there are various forms of telecom network fraud, and the renovation speed of fraud means is very fast.

Sixth, profitability. A series of costs for fraud gangs to purchase mobile phones, computers, mass SMS senders, bank card swiping devices and other crime tools and train new members are not high compared with the total amount of fraud. Affected by the low cost, easy replication and high profit of fraud, many criminals abandon theft, drugs, robbery and gambling to engage in this criminal activity, resulting in an increase in the incidence of fraud.

Seventh, cross regional. Cross region refers to cross-border telecom network fraud in a broad sense and cross province, cross city and cross district (county) telecom network fraud in a narrow sense. At present, the crime of telecom network fraud shows a transnational development trend, in which the existing crime dens are abroad and the defrauded groups are domestic citizens. There are also cases where the crime dens are in China and the defrauded groups are foreign Chinese or foreigners who understand Chinese.

3. Analysis on the Current Situation, Problems and Causes of Telecom Network Fraud Governance

3.1. Current Situation of Telecom Network Fraud Governance

In order to protect the legitimate rights and interests of the people and maintain social stability and harmony, the Chinese government has adopted a "zero tolerance" attitude towards the big cancer of telecom network fraud, and has actively introduced a series of targeted policies to prevent and accurately crack down on telecom network fraud since 2016. In April 2020, the Ministry of public security deployed the national public security organs to carry out the "cloud sword-2020" action, severely cracked down on the crime of telecom network fraud according to law, arrested and sentenced a large number of criminals, and achieved good social governance results. According to the data released by the Ministry of public security in January 2021, in 2020, the number of telecom network fraud cases cracked nationwide was as high as 25 60000 cases, and 26.6 million suspects were arrested 30000; Intercept fraud calls 1 400 million, 800 million fraudulent text messages 700 million, directly avoiding economic losses of more than 120 billion yuan for the masses [2]. On October 10, 2020, the inter-ministerial joint

ISSN: 2688-9323

meeting of the State Council launched a nationwide "card breaking" operation, the first round of centralized network collection (as of October 20), and more than 4600 illegal suspects involved in "two cards" were arrested in various places, and telephone cards and bank cards were seized More than 50000. On April 2, 2021, the fourth round of centralized network collection was carried out nationwide. More than 460 illegal suspects were arrested and 1.5% of telephone cards and bank cards were seized More than 50000 pieces, involving more than 13.6 million yuan.

3.2. Analysis on the Problems and Causes of Telecom Network Fraud Governance

Through the efforts of multiple departments and industries, China has achieved phased results in combating telecom network fraud, but there are still some problems to be solved.

Low technology. at present, the update frequency of domestic information system for monitoring telecom network fraud is not high and needs to be improved. Anti-fraud technical means such as mining and identifying fraud information and early warning of potential fraud risk also need to be improved, which is difficult to reduce the difficulty of telecom network fraud investigation and attack.

Incomplete legislation. There is no special legislation on personal information protection and data security in China, so it is impossible to cut off the source of telecom network fraud. In addition, the existing laws and regulations still have the problems of "inadequate application and inconsistent application".

The punishment is not heavy. at present, there is no unified punishment standard in China, and the sentencing is too light. Cases of heavy attack by public security departments and light punishment by procuratorial organs occur from time to time. Based on the characteristics of low cost and high profit of fraud, many fraudsters choose to resume their old business of fraud after their release from prison. Experienced fraudsters know the methods to avoid investigation, which increases the difficulty of arrest by public security organs.

Poor collaboration. First, public security, procuratorates, courts, banks, telecommunications, Internet companies and other departments and industries have not yet established the idea of a game of chess, and the cooperation is insufficient; Second, there are pain points in the governance of cross regional telecom network fraud between domestic provinces and cities, between the mainland (mainland) and Hong Kong, Macao and Taiwan, and between China and foreign countries.

Lax supervision. at present, there are many management problems and loopholes. For example, in the field of telecommunications, people can buy mobile phone cards and handle broadband services by registering their ID cards at will. The public security department has repeatedly found telephones with non-real name registration in the investigation of cases, which shows that the real name system has not been really implemented. In addition, there is no clear competent department to supervise and manage the field of overseas server hosting, so that fraudsters can take advantage of it.

4. Discussion on the Countermeasures of Telecom Network Fraud

The fight against and governance of telecom network fraud needs to be in line with China's national conditions and governance status. Under the unified leadership of Party committees and governments at all levels, we should focus on the important, difficult and painful points of governance, improve the technical level of anti-fraud, improve the foundation of the rule of law, intensify punishment, pool forces from all walks of life, strengthen industry supervision, and "fight, prevent, manage, control and publicize" to comprehensively deal with telecom network fraud.

ISSN: 2688-9323

Improve anti-fraud Technology. First, speed up the update frequency of fraud related information monitoring system; Second, improve anti-fraud technical means such as mining and identifying fraud information and early warning of potential fraud risks. We can use big data to deepen the construction of anti-fraud technology, including the construction of anti-fraud big data technology platform, the formulation of relevant standards, the research and development of phishing web pages and virtual dialing technology.

Improve the foundation of the rule of law. First, promote special legislation on personal privacy information protection and data security, and cut off the source of telecom network fraud; Second, formulate legal and effective regulations to regulate the use and restriction of app, applet and communication equipment; Third, explore and formulate relevant laws and regulations to link the credit of individuals and enterprises with the governance of telecom network fraud.

Increase the intensity of punishment. Formulate unified punishment standards for telecom network fraud, especially to raise the cost of crime and make fraudsters fear. All cities, counties, districts and units should be fully aware of the extreme harmfulness and severe complexity of telecom network fraud, crack down on Governance in the whole chain, ensure that the whole people have anti-fraud awareness, and resolutely curb the high incidence of telecom network fraud.

Gather strength from all walks of life. First, establish a reward and education mechanism, publicize and popularize fraud prevention knowledge and the harmfulness of assisting fraud in the whole society, online and offline, encourage citizens to actively report telecommunications network fraud, and educate and save those who fall into telecommunications network fraud crimes without subjective will; The second is to consolidate the main responsibility. All districts and counties should set up leading groups to crack down on new violations and crimes of telecommunications networks. The main leaders of Party committees and governments should sign a certificate of responsibility and establish a joint meeting system; Third, optimize the cross industry cooperation mechanism, strengthen cooperation and linkage, improve investigation strategies, coordinate law enforcement resources, and strengthen the joint fight against telecom network fraud; Fourth, explore the construction of international cooperation mechanism, jointly study the international framework agreement on anti-fraud, and formulate the prevention and governance plan of transnational telecom network fraud.

Strengthen industry supervision. First, we should establish the information sharing mechanism of telecom network fraud in the whole industry, which is an important means of scientific supervision; Second, build a big data basic resource base platform for telecom network fraud, which is an important carrier to improve the quality of supervision; Third, supervise enterprises to strengthen their supervision in advance and in process to ensure the standardization of business processes.

References

[1] Mitnick, K.D, W.L. Simon. The art of deception: controlling the human element of security[M]. Indianapolis, Ind.: Wiley Publishing, Inc., 2002.

[2] Allen M, Currie L M, Bakken S, et al. Heuristic evaluation of paper-based Web pages: a simplified inspection usability methodology[J]. Journal of biomedical informatics, 2006, 39(4): 412-423.

[3] Spinapolice M. Mitigating the risk of social engineering attacks[J]. 2011, 9(3): 21-23.

[4] He B Z, Chen C M, Su Y P, et al. A defence scheme against identity theft attack based on multiple social networks[J]. Expert Systems with Applications, 2014, 41(5): 2345-2352.

[5] Dzomira S. Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe[J].2014, 4(2): 2-4.