Pisco Med Publishing

Original Research Article

Reflection on Prevention and Control of Telecommunication Network Fraud in Big Data Era

Xingrui Wang*

Xingrui Telecommunication Equipment Co., Ltd. E-mail: xingrui@qq.com

Abstract: With the rapid development of smart phones and communication technology, the frequency of communication between the public and society through telecommunication equipment is increasing. At the same time, some lawless elements often cheat the public through telecommunication equipment, which brings irreparable economic losses to the society and the masses to a certain extent. In view of the above problems, this article takes the source of telecommunication fraud as the breakthrough point, analyzes the existing telecommunication fraud processing technology and points out its shortcomings, and then proposes a method of telephone fraud analysis based on big data technology. This technology fills the defects of the existing telecommunication interception technology and provides a new idea for effectively avoiding telecommunication fraud in the future.

Keywords: Big Data; Communication Technology; Telecommunication Fraud

1. Introduction

Since entering the 21st century, the quality of social security has been greatly improved, which decreases the burglary rate in society year by year. However, criminals never stop. As people's communication equipment has undergone many times of upgrading, criminals take advantage of the old people's lack of awareness of new technologies to implement telecom fraud. At the same time, the reason why criminals choose the elderly as the target of fraud is that most of them have a considerable amount of retirement wages. According to the investigation of relevant departments, the incidence of telecom fraud in China has been kept in a high range at an increasing rate of more than 20% every year. Although the current telecommunication fraud governance work in China has made good achievements, the problem of telecommunication fraud crime has not yet solved from the source. Therefore, in order to effectively crack down on telecommunication fraud, it is necessary for all parties in the society to intensify research on emerging technologies and try to prevent telecommunication fraud as much as possible, so as to effectively protect the property safety of the public.

2. The characteristics of telecommunication fraud

2.1 High incidence

According to the *Analysis Report of China Telecom Network Fraud* jointly released by the People's Public Security University of China and ND Personal Information Security Research Center, the telecom network fraud cases in China increased rapidly at a rate of 20%-30% every year before 2015. After 2017, the number of cases dropped for the first time and gradually stabilized. However, the overall situation of frequent and high incidence of cases has not changed fundamentally. According to statistics, telecommunication fraud still causes direct economic losses of more

doi: 10.18282/jnt.v2i2.1103

than 10 billion yuan every year.

In addition, the *Special Report on Judicial Big Data of Telecommunication Network Fraud* issued by the Supreme People's Court indicates that from 2016 to 2017, the proportion of telecommunication fraud in telecommunication network fraud cases decreased from 78.25% to 64.56%; online fraud, as a new means of fraud, greatly increased from 34.66% to 60.89%. According to the report, online fraud will continue to add to telecommunication network fraud cases in the future, and it will become more difficult to guard against it.

2.2 Complexity and variability

The *White Paper of Anti-Fraud* released by Tencent in 2019 points out that there are 10 types of fraud and 192 fraud methods in 2018. The telecommunication network fraud methods are changeable, showing a cross-border and diversified development trend. Divided by the types of fraud, in emotional fraud (including making friends and pornography), the number of male victims is nearly 3 times that of female victims; in financial fraud (including credit, investment and wealth management), the number of male victims is twice that of female victims; in daily life fraud (part-time job, free delivery, etc.), the number of female victims is twice that of male victims. In addition, criminals continue to adopt new tools and new methods for fraud, which is highlighted by the use of short video platforms, of quick spread and wide range, to achieve cross-platform crimes. The way to obtain an account number has changed from the precious high-cost registration number to a rental number, greatly reducing the cost of crime. Fraud dens have gradually moved overseas, concentrated in Southeast Asian countries such as Cambodia, Thailand and Laos, even to Africa areas.

2.3 Universal coverage

In the past, the elderly has long been the main targets of fraud because of their poor awareness of prevention and lack of understanding of new things and technologies. However, according to Tencent's research report on governance of telecommunication network fraud in the first half of 2019, middle-aged and elderly people have been defrauded with the highest amount, while the generation after 90s has the highest probability of being cheated, reaching 54%. Although the generation after 90s is born with the Internet, they have become the group with the highest probability of being cheated because of the large base of netizens. In contrast, although the 45-year-old victims of network fraud accounted only for 5%, the average amount of fraud was as high as 7,000 yuan, far exceeding that of other age groups. In addition, government departments and companies have also become targets of fraud. On December 29, 2015, the Construction Bureau of Economic Development Zone in Duyun City, Qiannan Prefecture, Guizhou Province was defrauded by criminals for 117 million yuan, which is the telecom fraud case with the highest amount cheated in one case up to now. In 2016–2017, Internet giants Google and Facebook also suffered many phishing scams and lost more than 100 million dollars.

3. Measures to prevent and control telecommunication fraud

3.1 Vigorously publicize the social harmfulness of telecom fraud and further improve the public's awareness

Although the means of telecommunication fraud will change with the development of the times, it usually does not change much in terms of the same type of fraud. Public security organs and government propaganda departments should focus on publicizing the dangers of telecom fraud, and can conduct in-depth analysis of various types of telecom fraud cases through community bulletin boards, WeChat public accounts, leaflets, and the Internet. For example, by analyzing the criminal characteristics and methods of criminals, as many people as possible are familiar with the fraud process of various telecom frauds, so as to improve people's awareness of prevention and thus reduce the occurrence of crimes.

3.2 Strengthen supervision and eliminate management loopholes

(1) To supervise network operators more comprehensively. Network operators are required to implement the real-name system of mobile phones in strict accordance with laws and regulations, strictly stipulate various sales channels

of mobile phone cards, and make the sales channels standardized and transparent. It is also necessary to prohibit network operators from using the "transparent transmission" function of VOIP network phones, and increase the crackdown on illegal production and sales of "arbitrary number" software, so that it is difficult for criminals to implement telecommunication fraud crimes.

(2) To strengthen the management of various base stations, resolutely crack down on the illegal production and sale of forged base stations, and cut off the channels for fraudsters to cheat. At the same time, all departments and units of public security organs should strengthen communication and cooperation with network operators, closely monitor the signals sent by pseudo base stations, and strike a strong blow in time.

(3) The public security organs must strengthen cooperation with the relevant regulatory authorities of the Internet. They should delete illegal "phishing websites" and Trojan virus links hidden on web pages, and remove illegal websites, thus breaking the channels for criminals to obtain information such as the victim's bank account number through their illegal means. At present, the Ministry of Industry and Information Technology, public security organs, banks and many other departments have set up the "12321" network spam report acceptance mechanism, and the broad masses of the people should take active actions to report bad web pages in time.

(4) The public security organs must resolutely crack down on and sanction the criminal acts that violate citizens' basic personal information. In the specific fraud process, the first step of telecom fraudsters is to obtain a large amount of basic personal information of citizens by illegal means. Some units or other staff members who have mastered a large amount of citizen information sell the basic information of these citizens to others to obtain high profits, which provides a channel for criminals to choose fraud targets. In order to reduce telecommunication fraud from the source, it is necessary to crack down on the criminal acts of infringing citizens' basic personal information.

(5) To strengthen the supervision and management of bank cards, and strictly implement the real-name ID card authentication system[3]. It is necessary for the bank staff to strictly check the identity information of customers when dealing with bank card business to prevent fraudulent use of other people's ID cards. The banking industry may consider implementing a personal lifetime unique account system. The unique identity account is uniformly provided by the People's Bank of China, which can be set up with multiple bank accounts in numerous commercial banks and can transfer money between different banks. It is relatively independent and each bank card is associated with an ID card, which can eliminate the random use of bank cards. Meanwhile, the relevant departments should also monitor the large cash withdrawal and transfer business, and fully implement the newly introduced 24-hour transfer system. Leaving electronic traces in the process of transferring money can increase the difficulty for criminals to commit crimes and prolong the time for committing crimes, which will be beneficial for the investigation department to investigate and collect evidence and clues about telecom fraud, so as to solve fraud cases.

3.3 Strengthen the intensity of criminal strikes

(1) In order to crack down on telecommunication fraud, relevant departments urgently need to formulate strict criminal justice policies. In recent years, telecommunication fraud has been rampant with a dramatically increasing number. It is in urgent need to formulate stricter laws and policies, improve the judicial system of examining evidence, and make judgments fair. In addition, it is also necessary to break the conventional thinking and take the criminal methods and means of telecommunication fraud as the incriminating standard, so as to make up for the shortcomings of telecommunication fraud in investigation and evidence collection.

(2) To establish a special department to combat telecommunication fraud and establish and improve relevant supporting mechanisms. At present, China has carried out reforms and practices in many aspects, and at the same time, it has established the Work Department of Combating and Governing Telecommunication Network Crimes under the State Council. Good results have been achieved now. The local people's governments at or above the county level should also set up special departments to crack down on telecommunication fraud crimes, and work together to strengthen the crackdown on telecommunication network crimes.

(3) To continuously realize the scientific and intelligent network survey technology. The main crime form of tele-

communication fraud is to defraud the bank account provided by the victim to transfer funds through network communication technology and electronic payment technology. With the continuous progress of science and technology and the continuous improvement of fraud methods, the public security organs must continue to strengthen the combination of scientific and technical personnel and modern equipment.

(4) To actively work with other countries to establish a working mechanism and extradition system to fight against network fraud. Nowadays, telecom fraud is widely distributed all over the world. The ringleaders of large telecom fraud criminal gangs and members of other important organizations are hidden abroad, and most of the network servers are located abroad. All these factors bring great difficulties to the detection of telecom fraud crimes. China should actively communicate and cooperate with other governments and Interpol. A platform should be jointly established to combat transnational telecommunication crimes, so that telecommunication fraud criminals have nowhere to escape.

(5) To improve relevant laws. In the construction of laws, it is necessary to learn more from the advanced legal concepts of western developed countries, and understand the laws of intensive credit card bookkeeping and electronic fund transfer issued by the United States and other developed countries against telecom fraud. By introduce and improving the relevant provisions on conviction and sentencing of telecommunication fraud crimes, paying more attention to telecommunication fraud crimes, and dealing with endless telecommunication fraud crimes in a timely and effective manner, people's interests and social security and stability can be safeguarded.

4. Conclusion

Telecommunication fraud is a new type of high-tech crime since the new era, the method of which breaks the traditional criminal form. Criminals have made full use of many new tools, such as telephone and Internet, fabricated all kinds of false information, lied that the victim or related personnel closely related to him had some urgent situation, and used the victim's fear psychology to swindle the victim for money. Telecommunication fraud has become a huge hidden danger in present society, a "cancer" threatening social security, people's property safety, social harmony and stability. In order to effectively prevent telecommunication fraud from further endangering public order and people's happy life, relevant departments must increase the investigation and research on telecommunication fraud, and formulate corresponding preventive measures according to the actual situation. At the same time, they should crack down and deal with various telecommunication fraud cases in a timely and effective manner.

References

1. Zou D, Lu Q, Pang Y. Analysis on the prevention of telecommunication network fraud crime (in Chinese). Journal of Huainan Vocational and Technical College 2019; 19(2): 118-119.
2. Zhang M. Research on prevention and control of cyber fraud in big data era (in Chinese). Computer Enthusiasm 2018; (25): 146.
3. Wen L. Regulation dilemma and optimization path of data cybercrime (in Chinese). Journal of Chongqing University of Posts and Telecommunications (Social Science Edition) 2018; 30(5): 46-53.
4. Ye B, Chen J. Accurate telecom fraud analysis based on big data (in Chinese). Communication and Information Technology 2017; (2): 56-57.