International Journal of Humanities Social Sciences and Education (IJHSSE)
Volume 8, Issue 12, December 2021, PP 124-129
ISSN 2349-0373 (Print) & ISSN 2349-0381 (Online)
https://doi.org/10.20431/2349-0381.0812014
www.arcjournals.org

Research on the Types, Characteristics and Countermeasures of Telecom Fraud

Kezhong Liu

The Department of Investigation, Guangdong Police College, Guangzhou

Corresponding Author:** ***Kezhong Liu, *The Department of Investigation, Guangdong Police College, Guangzhou, China*

Abstract: *Nowadays, with the help of fixed telephone, mobile phone, network and other communication tools and modern online banking technology, the crime of Telecom fraud without direct contact presents a high incidence trend. In recent years, telecommunications fraud has become one of the fastest-growing criminal cases, which has a profound impact on the people's sense of social security and endangers social trust and social stability. It is urgent to actively carry out the fight and prevention work. In view of this situation, this paper summarizes the types, characteristics of some telecom fraud, and puts forward countermeasures to further strengthen the fight against Telecom fraud, so as to effectively curb the arrogance of Telecom fraud.*

Keywords: *Telecom fraud ; criminal offence; sense of security; social trust*

1. INTRODUCTION

Telecommunications fraud refers to a criminal act of fraud by making up or concealing the truth to defraud property with the help of telecommunications networks and other communication channels. Nowadays, with the help of fixed telephone, mobile phone, network and other communication tools and modern online banking technology, the crime of Telecom fraud without direct contact is also showing an increasingly high incidence.

2. MAIN TYPES OF TELECOM FRAUD

With the development of science and technology, the types of Telecom fraud crimes emerge one after another. Telecom fraud is no longer shown in the most basic and original appearance, but more varied and various types. The original fraud has not yet quit, but new fraud techniques have sprung up and developed.

2.1. Pseudo Base Station Fraud

The so-called pseudo base station fraud is to use the searched mobile phone card number to impersonate the operator for SMS fraud. It is different from the previous point-to-point way of using mobile phones to send information and make calls to deceive. The pseudo base station realizes the "one to many" information transmission mode, which can enable most mobile phone users within a certain range to receive fraud information with high degree of camouflage and easy to be confused, and these information has no specific calling number directivity. According to statistics, more than 70% of fraudulent text messages pretend to be operators to induce users to click malicious websites to achieve the purpose of fraud. For example, a considerable number of fraud criminals will falsely use public service numbers such as 10086 series or 955 series to induce users to click on malicious websites by notifying preferential activities, so as to steal the user's account and password related to property, or directly invade the user system to obtain personal private electronic information to commit fraud.

2.2. Fraud Committed by Posing as Medical Insurance, Social Security and Bank Personnel

This kind of fraud is also called "consumption overdraft" fraud. Due to the victim's poor safekeeping of personal information, the account information of we chat, QQ, microblog and other social software was stolen, and the relevant personal information bound to the account was known to the criminals.

When the criminals were familiar with the basic information of the victim, they pretended to be the identity of medical insurance, social security and bank personnel, used the pseudo base station to call or remind mobile phone users through mobile phone text messages, First disclose some basic personal information of the mobile phone user to win the trust of the victim, then say that the user's medical insurance card, social security card or bank card has just been stolen and swiped in a certain place, provide relevant telephone number transfer services, inform the user that the card carried by the user may be copied and stolen, and require the user to go to the bank ATM for the so-called operation of changing data information, Or strengthen the security and confidentiality of medical insurance card and social security card according to telephone instructions. In fact, when the victim provides personal information including ID number, various types of card number and SMS verification code, the criminals will transfer the funds in the victim's card to their prepared bank account.

2.3. Posing as Public Security Personnel for Fraud

Such fraud is also known as "suspected crime" fraud. In recent years, the criminal suspect has changed the number software on the Internet, and the case of posing fraud by the public security organs has been more and more rampant. Criminals often induce the victims to call the alarm number they provide on the grounds that the victims themselves or their relatives are suspected of participating in the crime or helping the crime, inform the victims that they or their relatives are suspected of committing a crime or are under investigation, and take advantage of the victims' eagerness to ensure their own and relatives' safety and prove their innocence, Promise that the victim can help him get rid of the crime or prove his innocence, so that the victim can listen to the arrangement and spend a little money to ensure safety and defraud funds. Because this kind of fraud is novel and clever, it often causes the victims to remit all the deposits in their accounts into the hands of criminals, often involving a large amount of money, and such cases directly challenge the public power organs. Many local public security organs, procuratorial organs and judicial organs are falsely used, so that it is very easy to damage the social credibility of the public power organs.

2.4. Fraud by Posing as an Acquaintance

Such fraud generally includes "guess who I am" type telephone fraud and contactless network communication fraud. In the "guess who I am" type of fraud, criminals usually dial the victim's mobile phone number one-on-one. Once someone answers, they will ask, "guess who I am". Because of the victim's preconceived ideas, he will begin to think about his familiar relatives, friends and colleagues. Criminals take this opportunity to pretend to be people familiar with the victim, and follow the clues, making up various reasons based on the established impression of acquaintances in the victim's mind, pretending to encounter difficulties or poor life, and need the victim's temporary assistance or support. Once the victim determines that the criminal is an acquaintance, he will reduce his defense and automatically transfer to the criminal's designated bank account, resulting in the loss of money. The non-contact network communication fraud is similar to the "guess who I am" type of fraud. Criminals steal the password of relevant communication software accounts of the victim's acquaintances, such as QQ and we chat, "put on" the "clothes" of the victim's acquaintances, have a non-face indirect dialogue with the victim, and even use video to "prove" that they are the victim's friends or relatives, After gaining trust, they began to implement fraud and requested the victim to remit money for some less visible reasons, such as being arrested for whoring, entering the hospital for treatment and surgery.

2.5. Fraud with Winning as Bait

This kind of fraud is one of the most common types of fraud in the early stage, also known as "winning the prize and paying tax" fraud. Criminals use mobile phones to send mass text messages or call mobile phones. In the name of the interactive lottery of various TV programs, they notify the victims of winning the cash prize. Taking advantage of the victims' greedy attitude of joy and excitement and thinking they are lucky, they ask the victims to verify their identity. Once the victims reply, they further defraud the victims of paying risk deposit, handling fee Individual income tax, postage and other expenses shall be collected less and more times, gradually accumulate fraud funds, and implement telecommunications fraud to defraud the victims' property.

2.6. Using QR code Scanning for Fraud

This kind of fraud is one of the most popular and rapidly developing fraud types in the near future, also known as "sweeping" fraud. Recently, the online payment system is becoming more and more

mature and developed, and QR code is widely used by businesses with its advantages of large information capacity, strong confidentiality and anti-counterfeiting, reliable decoding and so on. Because the QR code can give consumers the convenience of using handheld payment, criminals also take the opportunity to replace the merchant's QR code with their own QR code. When consumers pay, if the merchant does not pay attention to updating their account information, it is easy to directly transfer the consumption money to the criminal's account, which is easy to transfer flowers and trees.

3. CHARACTERISTICS OF TELECOM FRAUD

In recent years, with the rapid development of Finance and communication industries, telecom fraud has also developed and spread wantonly. Although the forms of Telecom fraud cases are diverse and different, most Telecom fraud cases have certain commonalities and similar characteristics.

3.1. Low Cost, High Output and Great Temptation

The crime of Telecom fraud does not need to contact the parties at all. It is a prominent type of non-contact fraud. The criminals of fraud fake their identity, fabricate facts and have strong concealment. They can commit fraud at low cost, high frequency and large span, face unspecified people, and defraud the funds on the victim's bank card. Most of the suspect who commit SMS fraud will operate on the computer platform by sending text messages, and mass SMS will be used to carry out fraud. The tools required are mainly mobile phone cards, SMS mass senders, computers and mobile phones. There are not too many expensive tools and do not require too high technical level. The more common SMS group sender on the market is generally only a few hundred yuan. Once connected to the mobile phone, you can identify the mobile phone number segment still in use, and then send messages directly to achieve a large-scale "bombing". In addition, criminals do not need to buy the victim's personal information and other data, but directly set a certain number segment on the computer for mass distribution. Therefore, as long as there is the Internet and SMS group sender, the fraud information can be sent to the whole of China in half an hour, and the identity of the victims is also more complex, including workers, farmers, students, intellectuals and even cadres of state organs. The characteristics of low cost, high profit and low threshold lead to criminals flocking to SMS fraud. Even if only one in ten thousand people are cheated, it can bring great benefits to criminals. Therefore, telecom fraud has a specific temptation, and criminal cases are increasing day by day.

3.2. Gang Crime, Fine Division of Labor

With the continuous upgrading of telecommunications fraud means, the gang characteristics of this kind of crime are becoming increasingly prominent. Criminals should try every means to master the psychology of potential victims, fabricate attractive and novel information, and carefully prepare and plan any procedure and step in the crime. Generally speaking, most telecommunication fraud criminal gangs have a "family contract system" model, which is closely related. They commit crimes on a family basis, have high trust and strict internal organization. Most gangs adopt an enterprise operation mode with fine work arrangement. Some personnel are responsible for collecting victim information and some personnel are responsible for opening the victim's account, There are also groups that specialize in making phone calls or mass texting, and departments that are specifically responsible for online banking transfer. Some gangs even have principal criminals who implement remote command. Because there is no cross situation in each process, there is little contact with each other, the process is relatively independent, and each department has its own duties in process operation.

3.3. Technical Operation and Intelligent Crime

In recent years, the crime means and tools of Telecom fraud have been continuously upgraded, which also shows its intelligence. It is not necessary to be limited to a certain district or county or a fixed physical area like traditional fraud. Criminals use high-tech fraud tools such as Internet phone, arbitrary number display software and voice group transmitter, which not only confuse the victims, but also increase the possibility of evading the attack. The network telephone digitizes the voice signal, compresses, encodes and packs it, transmits it through the network, and then decodes the compressed package to re convert the digital signal into sound, so that both parties can communicate freely. Due to the emergence of arbitrary number display software and the lax supervision of telecom operators and other departments, the reversible addressing of network telephone is confused, which greatly improves the security index of this kind of criminals, and it is difficult to find a breakthrough.

3.4. Various Types, Keeping up with the Trend

Telecom fraud is bound to breed with the progress of the times. With the development of science and technology and the increasing progress of communication tools, the types of Telecom fraud are wave after wave, from the traditional SMS notification winning fraud to the emerging P2P credit, wechat red envelope fraud, and even the two-dimensional code scanning jump type. Various scams closely follow the trend of social development. The traditional fraud has not completely withdrawn from the stage, but the new fraud is slowly rising, which can be described as "a hundred flowers bloom" Type fraud, criminals take advantage of the asymmetry and opacity of various information to seize the victim's impatience, luck, greed and other psychology, so as to mobilize the people's curiosity and curiosity, so as to take advantage of the opportunity and make it impossible to prevent.

3.5. The Victims are Extensive and the Investigation is Difficult

The "shotgun" crime mode of Telecom fraud can almost involve all financial business points, resulting in a high dispersion of the victims. The victims report to the local public security organ. The case acceptance is easy to be isolated from each other, resulting in adverse information sharing and poor serial and parallel channels. Random crimes lead to great difficulty in merging. The clues left by criminals are generally not the telephone number and bank card number opened by themselves. Once the investigation work is started, it needs cross regional operations and a lot of human and financial resources. For the grass-roots teams of county-level public security organs, the investigation ability is limited, and sometimes they can only be forced to give up tracking. Traceless crime makes tracking difficult. Telecommunications fraud has strong concealment. The arrest requires the coordinated operation of network investigation, technical investigation and other departments, with high technical requirements. In practical work, although the public security organs work hard, they usually only catch the relevant personnel of downstream crimes. Because of the characteristics of fine division of labor and unilateral contact in criminal gangs, the principal criminals generally escape and are difficult to catch. In addition, the current phenomenon of transnational crime is not optimistic. There are overseas accomplices among the people who implement Telecom fraud in China. They command, plan and participate in crime through single line contact. At present, China has basically cracked down on criminals who withdraw money in China. It is difficult to crack down on overseas crimes from the root and recover stolen money.

4. Countermeasures of Telecom Fraud

4.1. Prevention Strategies of Telecom Fraud

4.1.1. Do a Good Job in Publicity, Establish a Three-dimensional Prevention System

Make corresponding publicity work according to various aspects that may be involved in Telecom fraud. Do a good job in community safety education, and formulate posters and leaflets for people at different levels to prevent fraud; Irregularly carry out education and publicity lectures on fraud prevention, and timely inform the masses of deceptive and new fraud means; Make relevant video clips to prevent fraud, and use the method of telling stories to teach in fun; Make mobile publicity vehicles and other platforms to carry out preventive publicity work anytime and anywhere; Make use of newspapers, television, Internet and other media with large audiences and wide coverage to widely spread the knowledge of preventing fraud among the people, so as to maximize the number of audience groups; Make full use of the anti fraud propaganda position of the Internet platform to open up anti Telecom fraud websites and columns; Make public service advertisements to publicize and prevent fraud, and strive to broadcast some promotional films to prevent Telecom fraud in prime time of major TV stations around the country. The prevention of Telecom fraud cases is not based on one point and one aspect. An effective prevention system should be established, based on the whole city and the whole country, so as to realize the three-dimensional, long-term and efficient prevention and control, so as to improve the people's awareness and ability to identify scams and prevent being cheated.

4.1.2. Clarify the Legislative Conviction Standards and Strengthen the Punishment

Laws and regulations are not only an effective weapon to crack down on Telecom fraud, but also the basis and criterion for public security organs to crack down on Telecom fraud. At present, the formulation of laws and regulations does not make telecommunications fraud impossible to rely on,

but most laws and regulations are only related and involved, without clear rules. Therefore, the current legislative suggestions strengthen the punishment of Telecom fraud by reducing the filing standard and increasing the penalty range.

4.2. Strategies to Crack Down on Telecom Fraud

4.2.1. Form a Binding Mechanism for Relevant Police Types to Encourage Normalized Cooperation

Since the traditional single police investigation mode has been difficult to adapt to the comprehensive attack on this kind of crime, we should boldly implement the binding mechanism of relevant police types such as criminal investigation, technical investigation and network investigation, conduct joint operations, make use of the different advantages and advantages of various police types, and in the early investigation process, mainly focus on network investigation and criminal investigation, and adopt the mode of large Corps operation to fully combine network investigation and criminal investigation, This makes the investigation and evidence collection more perfect and thorough, and timely and comprehensively fixes the relevant electronic evidence, which lays the foundation for the follow-up arrest work; And when we need to find out the suspect's dens and the outside tracks, we will give priority to criminal investigation and technical investigation, and provide clues for criminal investigation, and provide technical support for technical investigation. In terms of the binding mechanism of relevant police types, if it is necessary to realize the normalization of cooperation, relevant police types need to actively intervene to investigate and provide technical support for cases in different stages of case investigation, so as to effectively curb the rampancy of Telecom fraud gangs.

4.2.2. Build an Effective Sub Application Cooperation Platform to Realize Resource Sharing

Due to the cross regional characteristics of Telecom fraud cases, it is very important for public security organs to cooperate across regions in order to detect such cases quickly and efficiently. Therefore, we should implement the developed cross regional cooperation platform, make good use of the information of different regions on the platform, effectively string and analyze cases to verify the victims, assist in querying and retrieving the telephone list and the list of account numbers involved, and understand the occurrence of Telecom fraud cases.

4.2.3. Close Contact with Telecommunications and Financial Institutions to find a Breakthrough in Investigation

The information provided by the telecom fraud case to the public security organs is mainly fraudulent, involved in bank accounts and telephone calls. It is a long process to use these simple information to verify the suspect and detect the case. This requires the cooperation of financial institutions and Telecommunications institutions. The telecommunications department assists in providing personal information about the location of the telephone number and the number owner, as well as relevant communication records and recordings, while the financial institutions can provide account opening information, account opening transaction flow records, customer service telephone, SMS service opening, online bank transfer IP address, withdrawal and withdrawal address, etc, Provide clues for investigation work and find effective investigation breakthrough, so as to speed up the investigation process.

REFERENCES

[1] Ma Fengshi Research on Telecom fraud and its prevention [n] Journal of Yellow River University of science and technology, 2016 (032)

[2] Wang Feifei Telecom fraud put on QR code "vest" [n] Economic information daily, 2017 (024)

[3] Xiao Qinghua Analysis of Telecom fraud mechanism and prevention and control measures [J] Mobile communication, 2016 (19): 27-29

[4] Ming Yu On the investigation difficulties and Countermeasures of Telecom fraud cases [J] Journal of Yunnan Police Academy, 2011 (1): 104-107

[5] Guo Yunhong Psychological prevention of Telecom fraud [J] Legal system and society, 2016 (7): 70-71

[6] Jiang Li Research on prevention and control of Telecom fraud [D] Changsha: Hunan University, 2014

[7] Fang bin Evidence application in criminal trial: from obtaining confession to collecting information [J] Evidence science, 2020,28 (06): 684-703

[8] Zhang Linyan Research on the pressure control of investigation and interrogation [J] Journal of Liaoning Public Security judicial management cadre college, 2020 (04): 39-44

[9] Yan Xiafei, Fu Zhenzhen Research on the amendment of nine step interrogation method under "evidence centralism" [J] Journal of Jiangxi Electric Power Vocational and technical college, 2020,33 (04): 135-138

[10] Liang Jialong Research on evidence use technology in interrogation [D] People's Public Security University of China, 2019

Citation: *Kezhong Liu. "Research on the Types, Characteristics and Countermeasures of Telecom Fraud" International Journal of Humanities Social Sciences and Education (IJHSSE), vol 8, no. 12, 2021, pp. 124-129. doi: https://doi.org/10.20431/2349- 0381.0812014.*

Copyright: *© 2021 Authors. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.*