Causes and Prevention of Telecommunication Network Fraud

Huang Zuhe [1, a]
[1]Post-Doctoral Research Center of CCISR, Haidian District, Beijing, China
[a]email：zuhe_2010@163.com

Key words: telecommunications network fraud; causes; prevention; international cooperation

Abstract: This paper mainly discusses the causes and prevention of telecommunications network fraud, and the international cooperation to jointly fight telecommunications network fraud crime. The formation of telecommunications network fraud crime is caused by the following reasons: the economic value is regarded as the standard of success in the social transformation , which leads to the moral deterioration of unit and individuals and the telecommunications network fraud crime for profit. In addition,the telecommunications companies, banks and other enterprises are lack of the sense of responsibility. The phenomenon of illegal trading of personal information is very common. People have no enough precautionary consciousness. Civil law is despised and criminal law is treasured in the telecommunications network fraud. In order to effectively combat and prevent fraud in the telecommunications network, we must strengthen the construction of spiritual civilization and the construction of social morality, make great efforts to protect personal information, increase supervision and responsibility of telecom operators, banks and other relevant departments, advocate the concept of “Attaching the same importance to the civil law and the criminal law”,set up national anti fraud telecommunications network center,make further cooperation with foreign police, and effectively fight the crime of fraud telecommunications network.

1. Overview of telecom network fraud

At all times and in all countries, fraudulent crime is an old and common crime. Therefore,we must seriously face the fraudulent crime which is a mirror of society.

In the history of criminal law, the crime of fraud has a long history. In the Sui Dynasty and Tang Dynasty, there were crimes of fraud such as making money by forging official documents or the treatment of disease. With the continuous development of economy and society, the means and objects of fraud are increasingly renovated with changing forms.

According to the 266th article of the Criminal Law of China,the crime of fraud refers to the act of cheating other people's property with a large amount for the purpose of illegal possession. In general, Ordinary crime of fraud will go through several stages of “ the offender conceals the truth of the fact or make fiction -- the victim has wrong understanding -the victim dispose of property based on wrong understanding--the victim has property losses -- the offender obtains property.”

In China, before telecommunications network fraud crime appeared in the Taiwan at the end of last century, ordinary fraud was generally implemented through the small area, which brought relatively small loss of money in scope and area for victims.

In the early 2000s, the telecommunications network fraud was spread from Taiwan to the mainland, and it spread rapidly in the mainland. People call it "Taiwan fraud", which caused serious harm to society and caused social panic. In cross-border large telecommunications network fraud cases, Taiwanese have rich experience of telecommunications network fraud, so it is usually the Taiwanese that writes the script of telecommunications network fraud and the mainland people make phone calls of fraud in accordance with the script.

As the mainland police strike telecommunications network fraud crime more seriously and mainland police made more cooperation with Taiwan police to strike telecommunications network fraud crime, the place of fraud crime is transferring from Taiwan area and mainland China to Southeast Asian countries and even African countries.The criminal in these areas make a huge fraud

against mainland China and Chinese Taiwan residents by using number changing software and setting up malicious links . In some individual cases, the amount of fraud is even millions of dollars. In the three cross-boarder telecommunications network fraud with national influence which were successfully dealt with by judicial apartment in 2010, there was a victim who was cheated more than 10 million yuan in each case including a victim who was cheated up to 23 million yuan. Due to the strike from mainland China and Taiwan police, the criminals have fewer opportunities to commit crime, they focus on foreign countries. Therefore, the criminal group is getting bigger, with more and more countries involved.In 2010, Chinese mainland judicial organs handled 4 representative cross-border telecommunications fraud cases involving Thailand, Kampuchea, Malaysia, Indonesia, Sri Lanka, Fiji and other 6 countries.

With the continuous development of telecommunications network technology and personal information infringed, the way that the criminals commit telecommunications network fraud is becoming more hidden and more “realistic”. Among the seven areas where the first batch of occupational fraud crimes were classified as the source of the crime of fraud by the Ministry of public security, there were differences in the ways of fraud. In Guangdong Dianbai District Maoming City,the criminals make fraud by passing off acquaintances and leaders; in Danzhou City of Hainan province, the criminals make fraud by changing flight; in Yuqian County of Jiangxi province, the criminals make fraud by praying for a son with a huge sum of money; in binyang County of Guangxi province, the criminals make fraud by passing off the friend of QQ;in Shuangfeng County of Huanan province, the criminals make fraud by PS; in Fengning county of Hebei province, the criminals make fraud by passing off gangland; in Xinluo District, Longyan City, Fujian province, the criminals make fraud by online shopping. In addition, a more widespread telecommunications network fraud is passing off public security, the placement of test, score modification, entertainment winning fraud, subsidies and aid scholarship fraud, medical insurance and social security fraud, fraud website, tickets booking fraud, and loan fraud etc.

2. Causes of telecom network fraud crime

With the continuous development of telecom network technology and the disclosure of citizens' personal information, the crime of telecommunications network fraud has caused more and more harm to the whole world. According to the telecommunications Fraud Control Association (2007), the global average annual economic losses due to telecommunications fraud crime reached 550-600 billion dollars. According to the Report on the Protection of Internet users' Rights and Interests in China 2016 by China Internet Association,in the nearly a year, the amount of economic loss of 688 million internet users caused by spam, fraud information and personal information disclosure is 91.5 billion yuan. The way of telecommunications network fraud crime renovates unceasingly, with more and more covert implementation of fraud. Some criminals commit "precision fraud”crime successfully again and again, leading to more harm to the victims. The main reasons are as follows:

2.1 Social values distorted in the period of social transformation

After nearly forty years of reform and opening, there is a great achievement and change in economy and society. People's living standard is getting higher and higher and the social values are also diversified.Some values occupy the main values in the social transformation period, and they may bring some negative effects. For example, since the reform and opening up, people become more active in thinking with a big wish to increase economic income and live a happy life. Therefore, the "money oriented" value firmly occupies the minds of the people.

Therefore, to "get rich" whether through legal means or illegal means to some extent has become an important standard to determine success in social transition period.

In other words, in the social transition,to "get rich" regardless of whether it is through the legal way or the illegal way has become a value to judge “success”, which will lead to cyber crime, including Telecom crime.

In many areas of China, there are some counties,towns and villages specializing in telecommunications fraud such as the above-mentioned areas such as Maoming Dianbai District,

Binyang County of Guangxi, Shuangfeng County of Hunan, Fengning county of Hebei and Xinluo district of Longyan in Fujian. Some scholars mentioned some deception by the whole village in Fujian Province.The scholar thinks that the whole village fraud was founded out due to the case of telecommunications fraud which caused the suicide of Xu Yuyu, a college student in Shandong, and thinks that this kind of fraud by the whole village cannot be explained by the utilitarianism from the perspective economics. "The whole village fraud" stems from the stable equilibrium of evolution of the closed ethnic group in the competition of biological adaptation.This balance has a serious conflict with the universal will of the state and the modern morality of society in the open society.

2.2 Serious violation of personal information

Telecommunications network fraud was initially implemented by SMS to take the bait such as inducing the victim by entertainment winning and false official website. For example,fraudsters induce the victims with the prize such as car,cash and laptop as the bait and charge the personal income tax by the name of entertainment TV programs such as "very 6+1", "lucky 52", "The Voice of China" and so on. With the publicity of telecommunications network fraud by public security organs and the relevant departments,the public pay attention to such telecommunications network fraud crime with precaution.So this kind of telecommunications network fraud has been very difficult. Therefore, telecommunications network deceivers begin to search for or buy more detailed personal information such as house information, investment information, citizen identity card number, bank card account and the phone number left in bank, so as to more accurate way to confuse the victims. This kind of telecommunications network fraud is becoming more and more successful with greater infringement of property .Because personal information can bring great benefits , illegal activities such as stealing personal information and buying or selling personal information are also very popular. For example, in the death case of Xu Yuyu in Shangdong caused by telecommunications network fraud , Du Tianyu attack the 2016 Shandong college entrance examination online registration information system by technology and implanted trojan virus. Chen Wenhui purchased 1800 pieces of information of high school graduates at the price of 0.5 yuan for each piece from Du Tianyu. Bu using these detailed personal information, Chen Wenhui get an understanding of Xu Yuyu and her family background, and hired Zheng Xiancong and Huang Jinchun to call Xu Yuyu. Zheng Xiancong told Xu Yuyu that she had 2680 RMB scholarship waiting to be declared and “today”(the phone call day) was the last day if she wanted to get it. He asked Xu yuyu to contact Chen Wenhui, a staff in the County Finance Bureau .

Zheng Xiancong also asked the family background of Xu Yuyu in details.Xu Yuyu had a bank card with money given by her father as tuition. Chen Wenhui asked Xu Yuyu to go to the bank and check the subsidy. Then Xu Yuyu came to the bank on a rainy day. Chen Wenhui called called her and said the card need to be activated with a deposit machine. He asked her to withdrawal all the tuition in the card, save it to his designated account of student subsidies for activation, and then stole all her money. Then Chen Wenhui called his partner Zheng Jinfen who was in in Quanzhou to let Xiong Chao withdrawal all the money to divide the spoils.

In the case of Xu Yuyu, Du Tianyu stole the detailed information of 2016 entrance examination students in Shandong by embedding Trojan virus and illegally sold it to Chen Wenhui so that Chen Wenhui committed "precision telecommunications fraud" crime successfully. In this case, the illegal sale of personal information has become one of the most critical factors for the successful implementation of "precision telecommunications fraud" by Chen Wenhui and his partners.

With rapid developing market economy today, many units need to fill in personal information in applying for the so-called "discount card" , such as ID number, home address, and even bank card password, etc. Some enterprises illegally sell customers’ information to make profit, thus providing fertile breeding soil for telecommunications network fraud crime.

Chen Huang and other scholars believe that disclosure of personal information of citizens has become a "multiplier" of telecommunications network fraud crime at this stage. Once the personal information is used by the criminals of telecommunications network fraud , the crime will become

more accurate and real-time with sudden attack , so that the masses are impossible to guard against it.

Because of this, more and more people with high intelligence or high social status have been "targeted" and successfully cheated by the telecommunications network fraud criminals.For example, the reason why a professor of Tsinghua University and a film star Tang Wei were successfully cheated by telecommunications network fraud is mostly because the criminals have accurate grasp of personal information. So it is the same with many transnational telecommunications fraud crimes.

It is understood that in "hurricane No. 3" to strike transnational telecommunications network fraud crime in 2016, the modus operandi of the telecommunications network fraud Gang is as follows: the telephone caller posing as staff of domestic commercial banks and telecom operators obtain the information of ID, phone number, bank card number of victims in an illegal way and defraud the trust of the victims with the excuses that the identity information of victim's mobile phone cards, telephone or bank credit cards were stolen and result in high charges or consumption fees. Then the second group of phone callers posing as personnel of public security department gradually induce the payment information and bank card password of the victim. Finally,the cash in card are transferred out of the victim in online way.

Therefore,the fact that the citizens' personal information has been illegally infringed and used by telecommunications network fraudsters has become one of the main reasons for the crimes successfully committed by telecom network fraud criminals

2.3 The low responsibility of Telecom and banks

There are two current patterns of telecommunications network fraud crime:the first is the fraud through telecommunications network, namely making fraud phone calls by telephone or mobile phone, or inducting victims to click the faked website link with Trojan horse virus so as to steal bank account, password; The second is the transfer of balance in the bank through bank account or clicking the faked website link with Trojan horse virus. Therefore, the Telecom network fraud crime fact crime has two indispensable factors. One is the telephone services and other equipment of the telecommunications network ; the other is the bank transfer or cash withdrawal of the bank card or online bank. If telecom operators take effective measures in the supervision of telecommunications products and services or the real name and quick payment stop of the bank card, it will increase the difficulty of telecommunications network fraud crime and the ratio of clearing up a criminal case by public security investigation organ.

Judging from the current cases of attacking telecom network fraud crime, it is very difficult for public security organs to clear up the telecom network fraud case. The main reason is that telecom operators have enough effective supervision of the communication product and communication service. Telecom network fraud depends largely on the support of communication information products and services, such as website registration, the purchase of mobile phone card , SMS sending device and so on. For a long time, there is large degree of regulatory loopholes in the registration of the communication tools and website domain name .For example, the real name is not needed to buy mobile phone card or register domain name. Or the audit of the identity information provided by applicants is not strict, which results in the non audit real name registration and the sales of mass texting card and bearer card to make illegal profits.

The smart phones such as Yihaotong and "400" which are developed by communication enterprises have the functions of call, answer, reception transfer, bundle multiple phones and hidden calling number.People can buy them from communication enterprises or online without issued documents. In the communication service supervision, some communication operators have many illegal operation, such as loss of supervision and management in the marketing process of various network telephone resources. Through the VoIP technology, the suspect can easily dial any numbers using automatic dialing service and make calls posing as telecommunications, banks or even government departments. For example,in the telecommunications network fraud case which was cleared up by Zhejiang Ningbo city public security department, the criminals made online phone

calls from Taiwan province of China and foreign countries and made faked numbers of public security organs in Beijing, Shanghai and Jiangsu, Fujian, Guangdong.Then they use these numbers to cheat Chinese citizens.

The special investigation team had preliminary investigation on the three cases in Beijing, Fujian and Zhejiang. A total of more than 200 people were cheated at the amount of up to 13.31 million RMB. In the actual operation, operators have taken a laissez faire attitude towards this kind of behavior of criminals. For their own benefit, some operators in some places even turn a blind eye to the large-scale sending of fraudulent SMS or even bit dialing and abnormal traffic flow. For example, one of the victims received a fraud call from a faked 10086 customer service staff. They he reported the fraud to the Telecom customer service to check whether the verification code is sent from the China Mobile platform. At first, the Mobile Corporation only asked the victim to properly keep the verification code information and did not explicitly answer whether the verification code is issued from the Mobile Corporation platform. Later, the user repeatedly insisted asking the Mobile Corporation to reply whether the fraud verification code was issued by China Mobile. Finally, China Mobile made a clear recognition:The message filled with verification code which was sent by the fake mobile staff was from the mobile platform and claimed that it was caused by the non-standard operation of the cooperative operators. The author once bought travel insurance in Ping An insurance company of China. The insurance company may disclose the author's personal information so that the someone posed as the staff of Ping An insurance company of China with the hot line “075595511”. If you don't pay attention, you'll be deceived . These telecommunications network fraudsters use arbitrary display numbers posing as the customer service of China Ping An insurance company . Obviously, it is the result of lax supervision or even indulgence of telecom operators for the interests of enterprises.

In terms of bank and other financial institutions, there is lack of supervision in the real name system of bank cards. For example, in the process of applying for bank cards, the absence of real name bank accounts and savings supervision in China is the booster of successful telecommunications fraud. As everyone knows, the transaction only recognize the password instead of personal signature. There is lax supervision of opening account and make deposit with fake ID card. To some extent, the real- name saving is useless for some people who have an ulterior motive. According to relevant statistics of investigation department, when the public security organs combat telecommunications network fraud crime,they confiscated 20000 bank cards including major commercial banks, of which the accounts were open with false identity information. Many criminals buy identity information from migrant workers and students to deal with the relevant business, which has laid a great hidden danger for the telecommunications network fraud crime. Although the bank has quick freezing and emergency stoppage,the requirements and procedures of business application are too complicated to provide quick and convenient emergency stoppage service for victims. There is absence of supervision in bank transfer business. Online banking provides customers with fast and convenient services, but it also has its own great security risks and regulatory loopholes. Because criminals can make bank transfers and diversion of funds without time limit and amount limit, so that the fraud criminals can transfer the money easily after getting the money from victim.

The bank inquiry system is also quite lagging behind. The science and technology of the Telecommunications network fraud make more accounts cheated in wider areas. Some of the crime of fraud involve hundreds of accounts and dozens of areas, so the manual service is not available in a short time due to the low efficient bank customer service and inquiry system. Even the manual service is available, the enquiry person is required to go to the opening bank with original account documents. It not only waste the time of victim, but also restricts the time to solve the case by the public security investigation organ.

In a word, there is vacancy of the main regulatory responsibility of telecom operators and financial services, which provides enough time for the criminals to successfully commit the crime. It also makes the public security organs more difficult to effectively crackdown to crime, so that the victims suffer more and more loss which is more difficult to recover. Some victims even die or

commit suicide because of too much grief, which is a great tragedy.

2.4 People's awareness of prevention is generally weak

As is known to all,"The heavens don't drop the pie." However,people have weak awareness of prevention due to seeking for small profits,poor vigilance and poor common sense. According to the recent analysis on social security card and the low price goods,it is mainly because the victims are greedy. The telecommunications network fraud criminals take the advantage of the victims. In addition, through the analysis of some influential telecommunications network fraud case,either the Xu Yuyu case or any other case, we can find that the victims have weak awareness of prevention and are easy to believe the fake banks, telecommunications and even state organs or relatives, so as to get cheated. For some people engaged in closed work for a long time, such as scientific research workers who are easy to be cheated because of the less contact with the outside world.For example, a professor of Tsinghua University was cheated about ten million yuan by telecommunications network fraud because he has too little contact with the outside world and has poor social common sense.

2.5 Publicity of relevant departments is not efficient

In the current grim situation of telecommunications network fraud, the legal propaganda for the prevention of telecommunications network fraud is still not in place. At present, with the popularity of money worship and taking economic benefits as the measure of success in life, the criminals still make fraud by all means regardless of the pain of the victim, which caused enormous harm to social security and stability. Especially those cases posing as national authorities not only caused tremendous damage and suffering to the victims of the masses,but also caused tensions between cadres and masses and even mass incidents because the majority of victims vent the anger on state organs . However, the current legal publicity campaign to prevent fraud is still not thorough and impractical. The propaganda methods are still the theoretical discussion combined with few academic actual cases, so that publicity is not deep and the people cannot truly understand the nature of the telecommunications network fraud. Therefore, it is useless for public to have fraud prevention. People are easy to get cheated due to poor common sense and greed for petty gains .

2.6 Severe punishment to the people

For the criminals of telecommunications network fraud, they should be severely punished because they bring great social harm. However, if the heavy penalty is applied blindly without solution, the criminal policy may play a serious role in stopping the crime of telecommunications network fraud.The punishment may push telecom network fraud criminals to the opposite side of society , so that they become more cunning and more hatred to society.They will take more vicious and effective means of anti crime investigation, which is not good for the unity of this group of people and the detection of cases. The victims did not receive much compensation. It may lead to the formation of a social "evil flow" in the telecommunications network fraud crime, thereby continuing to endanger society.

3. Effective response to telecom network fraud

According to the causes of telecommunications network fraud crime, we can see that we should deal with the telecommunications network fraud crime from the following aspects:

3.1 Strengthening the construction of citizens' moral rule of law in the period of social transformation

With the deepening of reform and opening up, the formation of pluralistic social concepts and moral values, especially mainstream value of economic values,is a normal phenomenon in the social transition period. This "money-oriented" value has considerable adverse effects.It makes people take all illegal ways to become rich overnight such as getting rich by telecommunications fraud .Some places even the whole village commit fraud telecommunications network crime.They

are proud of making money by telecommunications fraud and are shamed of the failure of making money by telecommunications fraud. The economic entities, such as enterprises, groups and individuals, are willing to buy and sell personal information illegally for profit, so that some people use these personal information to commit telecommunications fraud crime.

In order to obtain more profits in the fierce competition, some telecom operators and banks and other financial institutions do not take supervisory responsibility for the illegal use of telecom network products and services and the act of opening accounts through false identity information, and some even indulge this behavior with "one eye open and one eye closed" when knowingly and understanding the behavior of telecommunications network fraud

3.2 Increase the protection of personal information

we must increase the protection of personal information since the illegal acquisition of personal information is becoming more hidden and the telecommunications network fraud is becoming more and more successful. From the law point of view, we should increase the punishment for illegal infringement of personal information. At the same time, we should introduce more applicable judicial interpretations to the applicable standard of the crime of illegally infringing personal information in one of the 253rd article of the criminal law.

We must increase the punishment to the act of intentionally disclosing or illegally selling personal information and other criminal acts. For example, for the illegal infringement of personal information, the principle of punitive damages can be applied. At the same time, the main person in charge of the enterprise shall be strictly investigated of the responsibility. If there is any serious consequences, we can investigate the relevant enterprises for criminal responsibility. We should also strengthen the publicity of personal information protection, so that the whole society can form a good atmosphere to protect personal information,and we can avoid the criminals to make precise fraud with detailed personal information .

3.3 Increasing supervision responsibility of financial institutions such as telecom operators and banks

At present, there is lack of responsibility for telecom operators and banks and other financial institutions. Therefore, it is necessary to strengthen the supervision responsibility and necessary social responsibility of the telecom operators and the banking financial institutions from the law and the industrial management. The telecom operators must implement the real name system for mobile phone.The telecom operators with no real name system will have administrative or economic punishment by the relevant Administrative supervision department (Ministry of industry and information). In addition, telecom operators must also increase technical investment and transformation, improve telecom technical specifications and interception. In the aspect of strengthening the specification and interception of Telecom technology, scholars abroad have put forward feasible interception technology through technical research. As a public service department with rich social resources , China's telecom operator should take responsibility of rectifying and standardizing key telecom services and having strict regulation of network. In rectifying and standardizing the key telecom business,operators should carryout a comprehensive self-examination to clean up the stock of the user,including voice special line, “400”, “Yihaotong”, “business operator” and other key business of the basic telecom enterprises. If there is any problem, the user will be urged to rectify it in a limited time. If there is any serious problem and the user refuse to rectify or does not to rectify in accordance with requirements, it function shall be banned according to law. In foreign countries, such as India, New Delhi scholars Daya Gupta and other scholars make an analysis on fraud telephone signal by telecommunications interception technology such as abnormal detection of telecommunication signals. If it is a fraud phone, it will be intercepted, so as to achieve the purpose of preventing telecommunications fraud.

In terms of the main responsibility of banks and other financial institutions,Banks should strictly enforce the real name system of bank cards. The bank must require the applicant to present his identity document for verification, and register the name and number of the identity document. Banks should make full use of the Internet verification system,ID card anti fake identification

instrument and other means to improve the ability to identify the authenticity of residents' identity cards. In addition, according to the relevant regulations, since 2017, the banking financial institutions and non bank payment institutions have new policy for units and individuals and related organizers who rent, lend, sell, purchase bank accounts (cards) or payment accounts recognized by the public security organs at or above the city level. Units and individuals who open bank accounts (cards) or payment accounts for with another person's identity information or fictitious agency relationship shall be forbidden to apply for non counter services and payment service of bank account (card) within 5 years, and no account shall be opened within 3 years.At the same time, the bank should strictly manage and eliminate the unlimited amount of bank cards, legally punish illegal activities to steal bank card information, make delayed payment system, further improve the bank's emergency stop payment system, strictly implement the business records system of banking system, strictly enforce the potential risk reminding system of bank remittance, and actively cooperate with public security departments to recover the money.

3.4 Raise public awareness of fraud prevention and strengthen propaganda

The successful telecommunications network fraud is most because of the weak public awareness of fraud prevention of the victims who are easy to be cheated. Therefore, we should vigorously improve people's awareness of fraud prevention and educate people not to covet little advantages and get without any labor. We should educate the masses to avoid money issues, which will greatly reduce or avoid the telecommunications fraud. At the same time, the state propaganda department should increase publicity and vigilance. For example, the state propaganda department should have effective publicity for the public awareness of fraud prevention by public movies or meetings. By improving the masses' awareness of prevention and increasing publicity, we will stop telecommunications fraud in a fundamental way.

3.5 Equal emphasis on Civil and criminal law

Although the telecommunications network fraud crime is a serious infringement of the masses of the crime, but only the penalty is not enough. As in the process of combat telecommunications fraud network crime, too much dependence on the effect of penalty will cause great tension of penalty resource. Moreover, because of the extremely low detection rate of telecommunications network fraud crimes, the probability of victims to recover money through public security organs is also very low. So we must pay attention to investigating the civil liability. For example, we can bring civil compensation suit to the court for the reasons of telecom operators or the bank, so that the victims can get different degrees of compensation.

Of course, in the telecommunications network fraud, in order to make fraud criminals quickly get forgiveness and support from victims,if the criminals and victims agree to settle the issue through criminal reconciliation,they can make criminal reconciliation, which can not only recover the cheated money for victims but also repair their relationship .

3.6 Strengthen the cooperation with the international community

Since the telecommunications network fraud is transnational, it is necessary to strengthen the cooperation with foreign police.It will become difficult for Chinese police to investigate the fraud since the criminal commit network fraud abroad, so we should strengthen the cooperation with foreign police. According to the related statics, most recent crimes committed by telecommunications network fraud criminals, which were detected by Chines police, were from

Kampuchea, Laos, Burma, Thailand, Malaysia and other ASEAN countries and even Kenya with lax supervision. The criminals in these countries have masses of fraud crimes in china. In these cases of cross regional telecommunications fraud crime,the differences in jurisdiction and the law will affect the judicial organs of China to combat telecommunications network fraud crimes.

For example, according to Taiwan criminal law, the most serious punishment for internet fraud crime is a sentence of 5 years, and China has the most serious punishment for internet fraud crime with a sentence of life imprisonment and a fine or confiscation of property.

Therefore, it makes the cost of telecommunications fraud committed by Taiwanese very low,

which is also the cause of rampant telecommunications fraud in Taiwan. Nevertheless, since the signature of Joint crime fighting and mutual aid agreement between the two sides of the Taiwan Straits, the mainland police have had close cooperation with the Taiwan police to arrest 7700 telecommunications network fraud suspects including more than 4600 Taiwan suspects,destroyed more than 500 overseas crime places, and cleared up over 10000 network fraud crimes. By increasing cooperation with foreign and overseas police,the network fraud crime will be hindered or reduced by continuously crackdown of the fraud.

In addition, in terms of the whole country,each region and each department fight separately, which is not good for the joint crackdown of the network fraud crimes. Telecommunications network fraud crimes happen in many places and there is no national anti telecommunications network fraud organization, so the department with jurisdiction in each place has their own action. Without the sharing of information, the investigation resources are greatly wasted and the efficiency of investigation is reduced. Moreover, because the public security organs, telecom operators and financial institutions belong to different departments, so they may have different rules in during fraud crackdown, thus hindering the operation.

4. conclusion

In the society with telecommunications network fraud with greater and greater social influence , some private hospitals make false medical advertisements through the Internet, such as Baidu or a private hospital official website, claim that the victim is ill, and cheat money from victims through treatment. Is this kind of case a network fraud crime? There are more and more cases like this, how can we deal with it? According to the above discussion, the author thinks the telecommunications network fraud refers to the fraud crime that the criminals trap (steal) the victim's funds into his bank account by sending text messages, making phone calls, embedding Trojan horses with communication, Internet and other technologies and tools. For the above mentioned situation, the author believes that this behavior of the hospital should belong to the defrauding of the victim's money through the Internet, and it is the crime of fraud caused by telecommunications network.If the doctor is not qualified, it also constitute the crime of illegal medical treatment.If the victim is injured in this case, the doctor shall be punished with the principle of "a heavy penalty".

The reason for recommending this paper :
This paper is of great innovation and social practical significance: at present, China and even the international community are suffering the rampant telecommunications network fraud, which bring great social harm to society and individuals. Therefore, it is very urgent to crackdown and prevent telecom network fraud. This paper is written under this background.

Reference：

[1] Zhang Mingkai: Fraud Crime and financial Fraud Crime, *Tsinghua University press*, 2006.

[2] Research Institute of information industry development strategy of Nanjing University of Posts and Telecommunications: China Anti telecom network fraud Blue Book, *Posts and Telecommunications Press* , 1st ed, 2017

[3] Liu Tong: " Discussion on Legal Problems of cross-border telecommunications fraud--taking two large Taiwa cross-border telecommunications fraud case in 2006 as example. Shandong Youth Political College 3st ed, 2016

[4] Bi Mingxiong and Zhang Qi: closed equilibrium and social morality: conflict between tradition and Modernity -- Thinking and governance of "whole village fraud", *Tianfu New Theory* 1st ed, 2017.

[5] Li Fucheng: Guidance on the investigation and litigation of telecommunications fraud, China Procuratorial Publishing House, 1st ed, 2017

[6] Pang Jinfeng: analysis of the difficulties and Countermeasures of Telecom fraud investigation from Xu Yuyu case, *Journal of Hubei Institute of Science and Technology*, 1st, 2017.

[7] Daya Gupta,Paval Pahwa,Rajiv Arora: An Analysis of Telecommunication fraud using Outlier Detection Model based on similar Coefficient Sum, *International Journal of Soft Computing and Engineering(UCCE),ISSN:2231~2307，Volume-4,* March 2014.