Journal of Sociology and Ethnology (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/jsoce.2023.050511
ISSN 2616-2318 Vol. 5 Num. 5

The Characteristics and Prevention Countermeasures of Telecom Network Fraud Crime under the Background of Big Data

Dong Anyang

People's Public Security University of China, Beijing, 100038, China

Keywords: Telecom network fraud, spatial and temporal distribution, social and demographic characteristics

Abstract: With the rapid development of internet technology and the arrival of the big data era, telecommunications network fraud has become a serious social problem with a growing number of cases in recent years. The victims and the amount of money lost are countless, making the prevention and crackdown of telecommunications network fraud a top priority for law enforcement agencies. This article explores the characteristics and prevention strategies of telecommunications network fraud in the context of big data. Starting from the spatiotemporal distribution and studying the social demographic characteristics, the characteristics of telecommunications network fraud are identified. Finally, the prevention strategies for telecommunications network fraud are summarized and analyzed, including strengthening the legal system, raising public awareness, and optimizing telecommunications network security technology. The aim is to provide effective reference and guidance for relevant departments and personnel, and to promote the prevention and crackdown of telecommunications network fraud.

1. Problem is Put Forward

Since the COVID-19 outbreak, crime rates have continued to rise worldwide, and the number of violent crimes has increased significantly. New York City officials said the outbreak led to a rise in 35 percent from a year earlier, while shootings increased by nearly 100 percent[1]. In contrast, China, with the continuous improvement and advancement of public security management, the traditional contact crime such as theft, robbery incidence decreased significantly, according to the national public security organ, in 2020 the national criminal case filing fell 1.8%, eight major criminal cases and investigate security cases for six years, the national residents of social security satisfaction is as high as 83.6%[2].

However, with the rapid development of Internet technology and the change of people's life style, the Internet has become a new platform for criminals to commit new crimes in the era of big data. For example, criminals will disguise themselves as legal institutions or posing as relatives and friends, so that the victim is not easy to detect. The epidemic of the frequent occurrence of contactless crimes such as telecom network fraud is the best proof. According to the statistics of procuratorial organs across the country, cybercrimes have climbed at an average annual rate of nearly 40 percent, reaching a peak of 54 percent in 2020. One third of all fraud crimes handled by procuratorial organs during the epidemic period were implemented through the Internet, much higher than in previous years[3]. As you can see, in recent years, the overall theft and robbery cases of the national public security organs, but the number of fraud cases has shown a steady upward trend, and the number of telecom network fraud cases is more obvious, which confirms that the phenomenon of social crime in our country has gradually undergone a huge structural change, and the non-contact crime represented by telecom network fraud may replace other property crimes in the future to become the most serious crime type in our country.

Under the background of all sectors of society and the broad masses of the people calling on the criminal judicial organs to strengthen the punishment of telecom network crimes, the cause of the "blowout" growth of the number of telecom network fraud crimes in China deserves the attention of the criminal circle. This paper will study the spatial and temporal distribution of telecom fraud, search for relevant cases, combine with the social and demographic characteristics, summarize the characteristics of telecom network fraud crime under the background of big data, and give some preventive countermeasures. The aim is to enhance the understanding of the law of the telecom network fraud crime, and to provide a reference for the prevention and control of the criminal judicial organs in China.

2. Current Situation and Characteristics Analysis of Telecom Network Fraud Crime under the Background of Big Data

2.1 Current Situation of Network Fraud Crime in the Era of Big Data

Telecom network fraud crime in criminal justice in a serious crime, according to the criminal law of the People's Republic of China, the crime belongs to "for the purpose of illegal possession, the use of computer information network fraud" category, if involving large amount or if the circumstances are particularly serious, can be sentenced to imprisonment of more than ten years or life imprisonment, fine or confiscation of property." Criminal law" in the telecom network fraud has not been included in the points, but the corresponding judicial interpretation, telecom fraud generally has two situations: one is to steal others communication lines or copy others telecom number to defraud others, the other is with their own communication equipment or number directly dial or camouflage dial by fraud to defraud others money[4]. After referring to the case, combined with this type of crime, it is concluded that telecom network fraud refers to the victim through the telephone, website, APP and other network channels, according to the victim's income ability or family situation, make use of their fear or profit psychology to fabricate false facts or conceal the truth. This non-contact telecom network fraud means, make the criminals finally defraud the victims and their relatives and friends of property, causing serious economic losses and social harm.

According to the latest statistics from the Ministry of Public Security, in 2021, the public security organs cracked more than 441,000 cases of telecom and network fraud cases, arrested more than 69 0,000 criminal suspects, destroyed 39,000 criminal gangs involved in "two cards", and recovered 12 billion yuan of defrauded funds to the people. At the end of 2020, in response to the rampant telecom and network fraud, the state set up the National Anti-fraud Center, a special agency to conduct early warning and monitoring. In 2021, the platform stopped more than 320 billion yuan of funds involved in the case, intercepted 1.55 billion fraudulent calls and defrauded 1.76 billion text messages, successfully avoiding more than 28 million people from being cheated.

The criminal means used by telecom network fraud crimes mainly include: publishing false information on Internet platforms, chatting and making friends on online social media platforms, making fraudulent phone calls, sending fraudulent text messages, etc. Among them, 71% of Internet platforms release false information and chat and make friends on online social media platforms account for them, which are common criminal means used by criminals. In addition, from the perspective of time series, the frequency of criminals using criminal means such as making fraudulent phone calls and sending fraudulent text messages is decreasing year by year, while the frequency of using Internet technology to commit crimes is increasing year by year.

Table 1: Detailed details of telecom network fraud[7]

Fraud method	frequency	percentage	Fraud method	frequency	percentage
Fake female identity to defraud finance	62	15.5	Fraud defraud advance payment of materials	7	1.8
False recruitment information	33	8.3	Gambling website	6	1.5
Promote the credit card processing	32	8	Fiction provides to do Taobao shop	6	1.5
Pretend to be a bank officer	29	7.2	False recruitment to defraud the training fee	6	1.5
Pretending to be a shopping website for customer service	23	5.8	Attract players to buy fake game items	6	1.5
Selling fake health care products	23	5.58	Use of money laundering through gambling platforms	5	1.3
Lottery game platform	17	4.3	Pretending to act as a company buyer	5	1.3
Mail card investment	12	3	Futures investment	5	1.3
Sell fake goods	11	2.8	Taobao franchise business	5	1.3
Fuel subsidy for car purchase	10	2.5	Loan capital verification	4	1
Pretending to be a public security organ staff member	10	2.5	Pretending to cash the prize personnel to defraud notary fees, handling fees	9	2.3
Pretend to be a company leader	9	2.3	Preposing as a court worker	8	2
Brush sheet rebate	8	2	Pretending to be an airline customer service officer	7	1.8

For the specific fraud methods, in the fraud methods, the fictitious female identity for the purpose of cheating property crime is the highest frequency. Specifically, these criminals usually look for potential victims in the name of dating social platforms. They use the prepared words to chat with the victim, develop feelings, and gain the trust of the victim. Once the victim is completely trapped in the false "love network", the criminals will ask for money on the grounds of medical expenses, travel expenses, gifts, or guide the victim into the gambling, investment platform to recharge. When the goal is achieved, the criminals will disappear. According to statistics from the China Xinyuan Communications Research Institute and other units, more than 260 new scams have emerged from January to October in 2020 alone[5], And the use of big data by criminals is the primary reason for the endless emergence of fraud techniques. Using the "black and gray industry" means, criminals obtain a large number of victims' accurate information and personal privacy data. The data are fed into AI systems for a lot of data training and deep learning, allowing computers to accurately judge a person's preferences, mental state, and even simulate human decisions. Based on these data, fraudsters can quickly produce a large number of customized scripts, using different ways of fraud according to the age, gender, occupation and other characteristics of the victims. In

February 2021, among the five telecom fraud gangs arrested by Guangzhou police, three had graduate degrees, all of which were related to computer information technology [6]. More and more highly educated people join the fraud gang, which is also one of the reasons why the telecom network fraud method is constantly updated and iterative. It can be seen that under the influence of the network media, the traditional fraud means have changed dramatically. In recent years, telecom network fraud methods have evolved from the traditional wide-net model to the era of customized scripts (see Table 1).

2.2 Analysis of the Characteristics of Telecom and Network Fraud Crimes

2.2.1 The Overall Distribution Characteristics of Network Fraud Cases

Adopt from the China Judicial Documents website (https: / / wenshu.court.gov. According to cn /), the website has published the effective judgment documents of courts at all levels across the country, with a total number of more than 100 million documents, covering criminal, civil, administrative and other cases. Based on the database of judicial documents, the judgment date is set from January 1, 2019 to January 1, 2023, the cause of action is set as "crime of fraud" and the document grade is set as "judgment". Through full-text search and screening of cases with online fraud circumstances, a total of 126,813 judgments on online fraud from 2019 to 2022, including 49,008 in 2019,53,102 in 2020 2,21,287 in 2021 and 3,416 in 2022.

Figure 1 shows the change trend of the number of online fraud in all provinces in China from 2019 to 2022. It is not difficult to see from the figure that the number of telecom fraud crimes in each province reached the highest in 2020, and all showed a downward trend. Combined with the spatial distribution of online fraud cases, it can be found that the number of online fraud in coastal developed areas such as Zhejiang, Jiangsu, Guangdong, Fujian and populous provinces Henan is significantly higher than other provinces. Fraud cases are concentrated in coastal areas and scattered in central and western Henan, Hunan and Chongqing provinces (cities). During the study period, more than 75 percent of the 50 districts and counties with the largest number of online fraud were concentrated in five provinces: Zhejiang, Jiangsu, Guangdong, Fujian and Henan.

2.2.2 Social and Demographic Characteristics of Network Fraud Cases

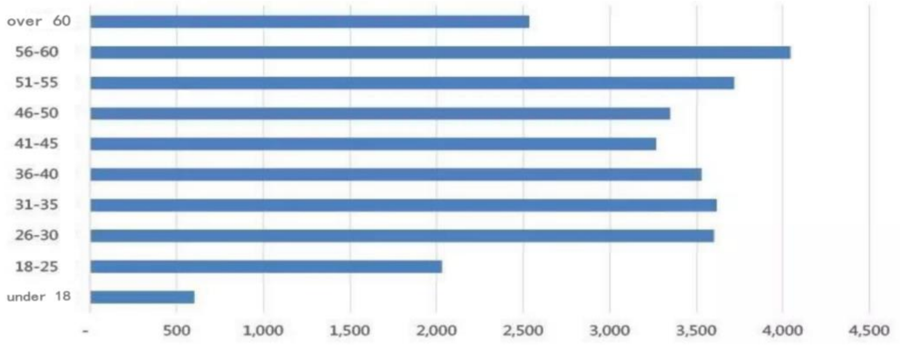

Figure 1: The distribution of the average self-impaired age of the deceived population

19 years old is the peak of fraud, 18-25 years old accounted for 52.4% of the overall fraud, followed by 26-30 years old, accounting for 21.4% of the total. However, the elderly are still the group with the largest damage amount of communication network fraud, among which the elderly aged 56 to 60 have the highest average amount of fraud. These single cases involve tens of thousands of yuan, more than hundreds of thousands of yuan or even millions of yuan. In

communication network fraud, the degree of capital loss is positively correlated with the age of the victim, and the older the age, the greater the amount of capital loss, as shown in Figure 1.

3. Preventive Countermeasures of Telecom Network Fraud in the Era of Big Data

3.1 Adopt a Criminal Policy of Emphasizing the Law and Controlling Chaos

Professor Bai Jianjun once pointed out that if the scale, level, quantity, structure and development of a certain type of crime break through the tolerable limits of the subject of criminal policy, the country will adopt a more stringent criminal response[8]. Based on the conclusion of the above criminal data, it is obvious that the characteristics of the organizational degree, crime ability and criminal benefits have already gone beyond the scope of the current criminal policy, which is also one of the reasons for accelerating the drafting of the Anti-Telecom Network Fraud Law of the People's Republic of China. Therefore, China is in urgent need to adopt the criminal policy of emphasizing the law and controlling the chaos, strengthen the crackdown on "black and gray industry" and related crimes, and give play to the deterrent role of the Criminal Law of the People's Republic of China. From the legislative level, telecom network fraud should be independent of crime, therefore, telecom network fraud is different from traditional fraud. Concealing the truth of fictional facts and "undermining information network security behavior" are clearly stipulated from three perspectives: criminal means, victims and infringement of legal interests. At the judicial level, it is necessary to strictly implement the Opinions on Several Issues concerning the Application of the Law in Handling Criminal Cases of Telecom and Network Fraud, and other judicial interpretations on the severe punishment of telecom and network fraud crimes, related crimes, evidence collection and review and judgment, the handling of property involved and other content provisions. Secondly, in addition to taking the amount of fraud as the basic sentencing basis for such crimes, the number of information browsing, the object of fraud, fraud means and other contents should also be taken as the basis for the aggravating circumstances, so as to comprehensively improve the judgment rate of fine and fixed-term imprisonment.

3.2 Make Full Use of the Advantages of Big Data to Create Wide Clues Sources

In the investigation practice, when the public security organs handle the telecom and network fraud cases, the clues obtained from the victim's report are relatively simple, and the access channels for obtaining other clues are relatively scarce. In order to make the possibility of obtaining clues ahead, the public security organs should dig deep and expand channels, make full use of the advantages of big data to dig case clues from massive information, and change the situation of passively obtaining clues in the past. On the one hand, the public security organs should enhance the investigation awareness of actively obtaining clues, determine the suspects from the starting point of research and judging personal information and transaction information as the starting point, and use the information obtained from the rectification of "black and gray industry" to carry out data collision and lock the suspicious personnel. Investigation department, on the other hand, can control on the "black ash industry" network control to dig related crime clues, and to buy and sell personal information network to determine the key suspects, using the seized equipment information and the number involved, network location data matching, timely monitoring card treasure "black ash industry" tools calling number and called number, dig out the personal information of criminal suspects.

3.3 Promoting Social Co-Governance to Form Synergy

The high incidence of telecom network fraud is also inseparable from the support of the large-scale "black and gray industry" group. Due to the non-standard supervision of dating, chat software and other platforms, fraudsters can purchase a large amount of personal privacy data from the "black and gray industry", while the "black and gray industry" group makes profits from the cooperation with criminals, and many have formed a relatively fixed criminal network, which further improves the upper limit of criminals' fraud ability. It can be seen from this that today's telecom network fraud is no longer confined to the circle of the public security organs, but a comprehensive disease that needs to be prevented and treated by the society. It not only needs the precise attack of the responsible organs in the key links, but also needs to promote social co-governance to form a joint force. On the one hand, we should strengthen the top-level design, and build a whole-chain three-dimensional comprehensive governance system with the deep cooperative participation of the Internet, public security, finance and other related industries. For financial institutions and Internet enterprises, they should rely on their own security technology and timely provide criminal clues to the public security organs. On the other hand, for the public security organs, they should further strengthen the linkage between the police and enterprises to fully share information resources. In recent years, around the public security department have set up the fraud center, further cooperation with Internet companies, effectively cut off fraud chain, the 32 provincial anti-fraud center and ali security fraud early warning system establish linkage mechanism, push more than 5000 warning information, the public security organ successfully intercept more than 2270 cases, save the loss of more than 4200 ten thousand yuan[5]. It is not difficult to find that only by coordinating the social forces can the possibility of public online fraud be minimized.

3.4 Innovate Publicity Methods and Enhance the Public's Awareness of Fraud Prevention

The three-dimensional and manipulation characteristics of telecom network fraud crime determine that its prevention means should be different from other traditional crimes, so it is particularly important to do a good job of publicity and early warning and victim prevention. On the one hand, the relevant subject should expand propaganda ideas, according to the new characteristics of telecom network fraud, new technique, organized by the government enterprises, industry research institutions, etc., make full use of WeChat, weibo, short video APP and other channels to distribute the latest telecom network fraud risk tips and countermeasures, and timely release to the public. On the other hand, the organization and promoted local industry authorities to carry out publicity activities to prevent telecom and network fraud in schools, villages and communities, and carry out face-to-face publicity work for the elderly, teenagers and other key groups. Considering that the victim groups in different regions are different, the relevant publicity departments of each region should closely combine the local reality, enrich the means and methods of anti-fraud propaganda, so as to enhance the anti-fraud awareness of the people everywhere. As a new type of crime of invading property, telecom network fraud not only causes huge property losses to the public, but also disturbs the stability of the network social order. On this basis, the present situation and characteristics of penalty are systematically analyzed

The core influencing factors confirm the compatibility and applicability of technology-driven crime theory in China, and these findings provide a practical basis for the governance path of criminal judicial organs for such crimes in China. It needs to be pointed out that because did not consider the criminal psychological level of cognitive, emotional factors, thus makes this study has certain limitations, the future academia can try to use quantitative analysis and qualitative interview combining the defendant mixed design mode, so as to achieve comprehensive telecom network fraud crime attribution mechanism, operation mode and development situation, realize the overall national security concept view for such crime in the final destination of social comprehensive governance.

4. Conclusion

In general, telecom network fraud, unlike traditional crimes, breaks the limits of time and space and can be implemented without contacting the victims. In addition, the lack of relevant legislation and interest drive and other factors also make the telecom network fraud rampant, to the public security organs to crack down on the difficulties. To control the crime of telecom network fraud, it is necessary to combat and recover funds, but fundamentally governance, prevention is the key. Enhance the immunity of all sectors of society to telecom fraud crimes, which can naturally prevent the occurrence of such crimes. Therefore, we need to combine the characteristics of telecom network fraud, build a perfect legal system, strengthen the responsibility of data supervision, enhance the ability of the masses to prevent, in order to completely eradicate the crime of telecom fraud.

References

[1] Longitudinal news. Crime and COVID-19 rates surge, 30 0,000 New York "great escape" [EB/OL]. (2020 -11 -19)[2021 -11 -05].https://baijiahao.baidu.com/s?id=1683769696518269251&wfr=spider&for=pc.

[2] 2021-04-15 Central radio network. The Ministry of Public Security notified the public security organs across the country to safeguard national security and overall social stability [EB / OL] () [2021-11-05]. https/ /baijiahao. baidu. com/ s?id=1697108624504540522&wfr=spider&for=pc.

[3] Wang Dong. The Supreme People's Court: More than 30% of the fraud cases handled by prosecutors during the epidemic period are cybercrimes [EB / OL] (.2021-01-25) [2021-11-08]. https: // www. spp. gov. cn/ zdgz/ 202101/ t20210125_507512.shtml.

[4] Southern Metropolis Daily. National provincial police recovered more than 42 million losses in a month, cloud anti-fraud matrix accurate early warning telecom network fraud case [EB / OL] (.2018-12-21) [2021-11-11]. https: // www.sohu.com/a/283503145_161795.

[5] Ganzi Express. Telecom fraud, you are more likely to trap than the elderly [EB / OL]. (2021 -10 -11)[2021 -11 -09].https://www.163.com/dy/article/GM1VSFH0053410HV.html.

[6] People's information. Being blinded by the temptation of getting rich, knowing that the law but difficult to extricate themselves[EB/OL](.2021-07-27)[2021-11-09]https//baijiahao.baidu.com/s?id=1706386335001649679&wfr=spider&for=pc.

[7] Tang He. The quantitative characteristics and governance path of telecom network fraud crime in China under the perspective of big data [J]. Journal of Guangxi Police College, 2022 (02): 85.

[8] Bai Jianjun. The law of criminal policy [J]. Chinese and Foreign Law, 2004 (5): 513-532.