Research on Methods and Legal Basis of Reconnoitring and Monitoring the Telecom Network Fraud Information

Liang Yuan[1]

[1] Border Management Brigade of Heihe Economic Cooperation Zone of Heilongjiang Province, Heihe, Heilongjiang, China

ABSTRACT

With the popularization and development of the Internet, the forms of network fraud have become increasingly diverse, from phishing emails, fake websites, to online shopping fraud, stock fraud, and so on, which are emerging endlessly. Network fraud has done great harm to people's lives and work, causing consequences such as property loss, privacy leakage, and credit bankruptcy. Starting from the methods and legal basis of telecom network fraud information reconnoitring and monitoring, the author analyzes and studies how to do a good job in network fraud, thereby enhancing people's understanding of network fraud, improving their legal awareness and prevention awareness of network fraud.

Keywords: *Reconnoitring and monitoring, Law, Basis.*

1. INTRODUCTION

Currently, various telecom network fraud cases are emerging one after another, with a variety of patterns. Fraudsters often engage in fraudulent activities against friends or acquaintances around them, especially by pretending to be family and friends. Some even use online channels and adopt information technology to carry out network fraud, which brings certain difficulties to police information reconnoitring and monitoring work.

Recently, network fraud mainly relies on phone calls, text messages, or email as the main means. By answering unknown phone calls, text messages, and claiming to be a staff member of a certain bank or government agency, the victim's trust is gained. Through these identities, important information such as personnel identity information, bank card passwords, credit card verification codes, and online banking passwords can be further obtained, and confidentiality will be required for various reasons, including not disclosing to family members, and even intimidating them by holding them jointly responsible. The author conducts an in-depth analysis of the current situation, means, approaches, methods, and legal basis of telecom network fraud information investigation and monitor, and studies countermeasures.

2. THE MAIN MEANS OF NETWORK FRAUD

Telecom network fraud is the act of using the internet to fabricate facts or conceal the truth for the purpose of illegal possession, in order to defraud a large amount of public and private property. By analyzing the investigation and control work of current telecommunications network fraud police, the following common network fraud situations are summarized.

2.1 Impersonating Government or Enterprise Personnel to Engage in Fraud

This kind of fraud is mostly based on pretending to be government staff, telecommunications staff, etc., informing the fraudster of mobile phone arrears, package loss, suspected violation of the law and other reasons, obtaining the bank account number, ID number, mobile phone verification code and other information of the fraudster, and charging fees for helping to handle and solve problems. The fee collection method is mostly bank transfer, where the amount of money is increased one by one and the transfer to the account is claimed to be a "secure account"; At the same time, by obtaining the SMS verification code of the fraudster, online lending services such as credit cards can be opened, and various cards of the victim can be directly opened for consumption, which can be directly transferred to the fraudster's account through borrowing and lending, thus committing fraud.

2.2 Obtaining Details of Daily Life to Commit Fraud

Fraudsters obtain basic information about the name, occupation, age, address, and phone number of the victim through illegal channels, as well as their daily life whereabouts. Then, through phone calls and other means, they use loans, car tax reductions, refunds, and other reasons to target the victim's daily experiences as a starting point. Victims are prone to trust and commit fraud; At the same time, they send discounted and tempting information such as low price shopping, internal shopping, prohibited items, and soliciting prostitutes to some users of certain account segments through mass messaging and spam messages, which can easily make the victim feel that they are getting cheap or affordable. Then, they confirm the transaction by paying a deposit and remit it to a designated account, but the amount of the deposit increases every time, until the victim no longer pays the deposit or discovers that they are scammers.

2.3 Using Communication Tools Such as WeChat to Commit Fraud

Fraudsters often use instant messaging tools such as WeChat and QQ as channels to post winning information, marriage information, and high salary recruitment information in the online space. Then, on the grounds of paying taxes or handling fees, they ask the fraudster to transfer the money to a designated account, and then engage in second or third fraudulent activities on the grounds of not receiving it, until their behavior is discovered. Moreover, fraudsters use network fraud to deceive them into remote areas in China or abroad, often using fraudulent methods such as working and obtaining high profits. They close them in their rooms and use intimidation or violent pressure to incite fraudulent behavior towards their family and friends around them, or use video chat tools such as QQ and WeChat to commit network fraud against family and friends.

2.4 Using Web Pages and Other Means to Provide False and Tempting Information for Fraud

Fraudsters use websites and other channels to disclose false internal information, such as lottery winning numbers, stock potential stocks, and other information as trading bait. Through the victims' weaknesses such as wanting to win or become rich, the fraudsters layout and set up scams, sending verification codes to mobile users in the form of text messages or posting fake shopping, ticketing, and other websites to lure victims to share personal information online, Especially, important information such as bank card numbers will be provided to the fraudster, and the funds will be transferred to the fraudster's bank account.

3. METHODS OF NETWORK FRAUD RECONNOITRING AND MONITORING

Due to the characteristics of strong concealment and wide coverage of network fraud crimes, as well as difficulties in obtaining evidence and determining jurisdiction in reconnoitring and monitoring, some are difficult to adapt to the reality of network fraud crime reconnoitring and monitoring. The ways and means of reconnoitring and monitoring mainly refer to the ways and means of finding case clues, mainly including mass reporting, network services and regulatory agencies reporting, reconnoitring and monitoring organs finding clues by themselves and suspect. In the reconnoitring and monitoring of network fraud, in terms of obtaining new clues, the reconnoitring and monitoring authorities can use relevant technical reconnoitring and monitoring means at this time, such as extracting and saving relevant data, conducting targeted tracking of the suspect's IP address, and monitoring the suspect's account number.

3.1 Starting from False Information for Reconnoitring and monitoring

In network fraud, suspect first need to attract victims with false information. In order to make false information spread faster and more widely, suspect often set up websites, publish messages in game platforms, and publish advertisements through websites.

3.2 *Starting from the Flow of Funds Involved in the Case to Carry out Reconnoitring and monitoring*

The crime of network fraud inevitably involves transaction funds. The motive of the crime of network fraud is money. The suspect will eventually remit the stolen money obtained from the fraud into his/her account, which makes it possible to investigate and monitor the crime of network fraud from the flow of transaction funds.

3.3 *Starting with the Victim for Reconnoitring and monitoring*

In the network fraud crime, the victim has a long contact time with the suspect. Therefore, the victim has more information about the suspect. In order to increase the success rate of fraud, suspect will also design corresponding fraud schemes according to the characteristics of victims or such people.

3.4 *Reconnoitring and monitoring of Information Left Behind by Suspects*

The suspect must go through the network when committing network fraud, that is to say, the suspect must have a device that can access the Internet, and through the server provided by the network operator, the police can start with the Internet information left by the suspect and organize the police to carry out reconnoitring and monitoring.

4. LEGAL BASIS FOR NETWORK FRAUD

The People's Courts, People's Procuratorates, and Public Security Organs, in response to the characteristics of telecommunications network fraud and other criminal activities, adhere to the full chain and comprehensive crackdown, adhere to strict and prompt punishment in accordance with the law, and resolutely curb telecommunications network fraud and other criminal activities. Based on the relevant legal basis for handling telecommunications fraud and other forms of cases, the legal basis for telecom network fraud is summarized as follows:

4.1 *The Electronic Information Network Law Involved in Civil and Commercial Law*

Civil and commercial law involves electronic information network law in the network environment, mainly through effective expansion of its principles. Mainly reflected in intellectual property, network contracts, and other aspects, the management of online payment and other platform transactions through relevant network regulations is carried out, especially for regulating and constraining information security issues such as disputes and information leakage, and effectively regulating electronic invoices and other materials.

4.2 *Administrative Law and Electronic Information Network Law*

The main department of administrative law is the competent department for effectively managing network security issues. According to regulations, social organizations and individuals responsible for electronic information network security are the primary responsible persons for network transactions, use, and management, and bear legal responsibility for any violations or illegal activities that occur during the use of the network.

4.3 *Relevant Substantive Law and Electronic Information Network Law*

This mainly includes the issuance, use, and management of electronic bills, such as electronic network transaction records, transaction vouchers, transaction data, and other verifiable electronic evidence generated, signing and preserving digital signatures, as well as criminal electronic evidence rules.

4.4 *Procedural Law Related to Electronic Information Network Law*

The procedural law mainly involves the jurisdiction of electronic information networks, criminal investigation, and monitoring principles in the reconnoitring and monitoring of online crimes. In terms of network use, management, and other aspects, there are criminal activities such as evidence collection and investigation.

5. COUNTERMEASURES FOR PREVENTING NETWORK FRAUD

The telecom network fraud criminal activities carried out through communication methods such as mobile text messages, phone calls, and the internet are very prominent. The criminal methods are technologically advanced, and the fraud methods are constantly being renovated. Once they enter the trap of scammers, they will inevitably bring economic losses. Through research on the ways and methods of investigating and controlling telecom network fraud information, the author has summarized the fraud prevention measures to effectively reduce and prevent the occurrence of fraud cases.

5.1 Improving the Reconnoitring and monitoring Organizations

The competent departments in charge of network fraud must attach great importance to cracking down on and governing telecom network fraud crimes, strengthen organizational leadership, play the role of "leading geese", form a "wild goose formation effect", and achieve a good pattern of leaders in charge taking the lead and leading teams in charge of the front line; they should also regularly conduct in-depth analysis of new situations, new means, and new methods of electronic fraud crimes, research targeted measures and operational tactics, conduct pressure layer by layer, implement responsibilities layer by layer, and research and develop relevant rigid measures to combat and govern telecom network fraud crimes, as well as normative documents such as nationwide anti-fraud prevention propaganda, to provide institutional guarantees for the orderly implementation of various work; There is a must to firmly establish the concept of "one game of chess" and carry out the reconnoitring and monitoring of network fraud. It is also a must to personally deploy and promote, organize research and judgment, and lead teams to deploy and monitor the work. The entire police force has concentrated and launched a cluster attack, quickly forming a high-pressure situation to crack down on the crime of electronic fraud. The plan to integrate the crackdown on telecom network fraud into the social governance system should be promoted synchronously, and a dedicated person responsibility system should be established. A system of "daily reminder, weekly report, and monthly dispatch" needs to be established to tighten and compact the responsibility of local entities.

5.2 Building a Strong Professional Reconnoitring and monitoring Team

Establishing a professional reconnoitring and monitoring team is conducive to improving the level of case reconnoitring and monitoring, improving case handling efficiency. Through the accumulated experience of professional reconnoitring and monitoring teams, an effective continuation can be formed, which helps to overcome difficulties such as long cycle of network fraud. The establishment of a professional team for cross regional crimes of network fraud is a characteristic. Compared to traditional cases, it requires reconnoitring and monitoring personnel to possess professional network technology capabilities and comprehensive abilities such as relevant data analysis and judgment. Only when a specialized team possesses a certain level of professional knowledge can the process of investigating cases be ensured to be smoother, without the need to coordinate the support and assistance of relevant technical personnel. It plays a certain role in the confidentiality of cases and effectively improves the effectiveness of online anti-fraud work.

5.3 Establishing a Collaborative and Coordinated Combat Mode

In response to the complexity of network fraud cases, it is necessary to highlight the four elements of "cracking down, prevention, management, and monitoring" to ensure fast investigation, fast handling, and thorough investigation of electronic fraud crimes. It is necessary to adhere to the synchronous filing of cases by multiple departments, strengthen clue verification, analysis and judgment, and on-site investigation to ensure that the crackdown is in place; It is also necessary to quickly verify mobile phone clues, timely landing and landing of people through WeChat and QQ clues, increase the number of cooperation results, leverage the deployment warning model, timely identify high-risk individuals, and push warning information. There is a must to strengthen deep docking, close collaboration, and joint strikes, optimize and integrate research and judgment capabilities, fully leverage the data resources and information advantages of communication and financial departments, and collaborate to build research and judgment control models. There is also a must to carry out targeted dissuasion work for relevant pushed early warning information by grading, classifying, and targeting. For high-risk information, there will be a necessity to assign dedicated personnel to carry out precise dissuasion point-to-point and face-to-face, continuously improving our ability to crack down on governance.

5.4 Establishing a Three-dimensional Propaganda and Prevention System Architecture

It is of great significance to grasp the two methods of online and offline promotion and theme activity promotion, expand the publicity area, expand the scope, and improve the publicity effect, and effectively create a strong atmosphere of public security cracking down and the whole people taking precautions seriously. There will be a must to fully leverage the power of traditional and online media to publish anti-fraud videos, tips, and tips on anti-fraud in radio, television, newspapers, and online media, and use information platforms such as outdoor LED screens in street shops to scroll and broadcast anti-fraud information. It is necessary to make full use of social platform resources to carry out propaganda, including express delivery, universities and other enterprises as members of the Anti-Electronic Fraud Public Welfare Alliance, and promote relevant departments to incorporate anti-fraud propaganda into legal publicity and public welfare propaganda, to prevent the advance and shift the focus forward. It will be a must to push and download anti-fraud and other software to the public, use radio, ringtone, graphic and text promotion, and send flyers to carry out fraud propaganda work. Grid personnel must explain the current methods of electronic fraud crime, teach methods to prevent telecommunications fraud crime, and mobilize them to popularize electronic fraud knowledge to family and friends, with small to large and point to area, effectively improving the overall society's awareness and ability to prevent fraud.

6. CONCLUSION

In summary, the current situation of online fraud in China is relatively difficult in terms of investigation and evidence collection, as well as difficulty in fund recovery. In addition, network fraud has the characteristics of intelligence and concealment, which requires people to comprehensively and meticulously carry out case registration work, timely and quickly strengthen contact with communication departments, and improve the ability level of relevant personnel to investigate and solve cases. It is a must to take national laws, government policies and regulations as the basis, and adopt multiple measures from different entry points to provide legal basis for network fraud, enhance the legal binding force on network fraud. Only in this way can people usher in a safe and trustworthy online environment, allowing people to enjoy a happy life in a safe and convenient online environment.

REFERENCES

[1] Chen Wei, Research on Network Fraud and Countermeasures for Detection [J]. Public Security Journal, 2008, 35(5). (in Chinese)

[2] Cui Hao, Legal Reflection on Electronic Evidence in Cybercrime [DB]. Criminal Research, 2007. (in Chinese)

[3] Liu Youhua, Wang Sheng, On Network Fraud and Its Preventive Measures [J]. Netinfo Security, 2008, 36(6). (in Chinese)

[4] Li Shan, Analysis of the Current Situation and Countermeasures of the Development of Online Criminal Law [J]. Journal of Chifeng University, 2012, 10(9). (in Chinese)

[5] Liu Shoufen, Shen Liuhua, Research on the Regulation and Application of Criminal Law on New Issues of Cybercrime [J]. Criminal Science, 2007, 15(4). (in Chinese)

[6] Liu Yingze, Zhang Yuxia, Wang Xuemei, Investigation into the Problems of Cyber Crime Legislation in China [J]. Hebei Normal University of Science & Technology, 2010, 14(3). (in Chinese)

[7] Zhang Hui, Exploring the Crime of Online Fraud [J]. Science & Technology Information, 2008,5(6). (in Chinese)

[8] Guo Xiaobin, chiefly ed., Strategy and Measures for Criminal Investigation [M]. Law Press, 2001. (in Chinese)

[9] Li Xincheng, Fan Wang, Li Donghai, Contemporary Crime and Criminal Investigation Guidelines (Volume 2) [M]. Mass Publishing House, 2003. (in Chinese)

[10] Luo Bingsen, Mo Guanyao, A Course in Investigating Economic Crime Cases [M]. Police Education Press, 2000. (in Chinese)

[11] Wang Guomin, Li Shuangqi, Investigation Science [M]. Chinese People's Public Security University Press, 2007. (in Chinese)

[12] Wang Chen, Research on Fraud Crime [M]. Courtbook Press, 2003. (in Chinese)

[13] Xiao Guibin, Economic Fraud and Prevention [M]. Chinese Worker's Press, 2003. (in Chinese)

[14] Zhang Yuxiang, Wen Shengtang, chiefly ed., Contemporary Investigation Studies [M]. China Procuratorial Press, 2001. (in Chinese)

[15] Shi Yu, Research on the Crime of Online Fraud and Its Reconnoitring and monitoring Measures [E]. Thesis, 2011. (in Chinese)