Research on improving the quality and efficiency of interrogation in telecommunication network fraud cases

Xingyuan Du

People's Public Security University of China, Beijing, 100038, China
wumingxingqing@163.com

Abstract: *With the advancement of science and technology, telecommunication network fraud crime constantly updates the means of operation, completing the transformation of intelligence, syndication, and specialization, and has become the most prominent crime with the highest incidence, the largest losses, and the strongest public repercussions. The interrogation of such cases in practice suffers from a lack of professionals, takes a long time, is inefficient, and has other problems, but currently there is less research on it in China. By summarizing the differences between telecommunication network fraud cases and other ordinary cases and the special psychology of criminal suspects, combined with the actual interrogation, problems in the interrogation reality are found, and reasonable countermeasures to improve the quality and efficiency of interrogation are proposed with reference to the practice of telecommunication network fraud investigation.*

Keywords: *Telecommunications Network Fraud, Investigative Interrogation, Improved Quality Effect*

1. Research Background and Current Situation

As of June 2022, the number of Internet users in China was 1.051 billion, and the proportion of those using cell phones to access the Internet reached 99.6%. The rapid development of the Internet and its comprehensive integration into people's lives necessitate the traditional crime type of "fraud" from contact and the "individual warfare" mode of operation to complete the intelligent, group, and professional transformation, and the modus operandi is constantly updated as technology progresses and develops. As of November 2021, the national public security authorities have investigated and handled more than 370,000 cases of telecom network fraud, arrested more than 549,000 suspects, and intercepted up to 326.5 billion yuan of funds involved in emergency cases. Telecommunication network fraud crimes have become prominent crimes with the highest incidence, the largest losses, and the strongest reactions from the public, and the interrogation of suspects in telecommunication network fraud cases has become a systematic task with a high volume and difficulty in the interrogation of these cases[1].

The national public security authorities have taken a series of crackdown measures against telecommunication network fraud and its upstream and downstream associated crimes and have achieved fruitful results. Under the high-intensity situation of the crackdown, the number of telecommunication network fraud crimes decreased year-on-year for six consecutive months from June to November 2021, and the prolific trend was further controlled. As of December 30, 2021, the "card-breaking" and "flow-breaking" operations have eliminated nearly 50,000 "two-card" gangs and illegal exit gangs and arrested more than 460,000 suspects. More than 460,000 people have been arrested.

Interrogation is an essential and crucial part of case solving, and its quality and effect directly affect the determination of the results. Various problems are the key to improving the quality and efficiency of interrogation. The interrogation of such cases is more complicated than the interrogation of ordinary cases due to the special nature of the case itself and the special psychological characteristics of the suspects. Therefore, in order to improve the quality of interrogation, we should first start with the special characteristics of the case, looking for its differences with ordinary cases, and the existing problems of interrogation work to analyze, and then find the right remedy and put forward effective problem-solving strategies, so as to provide a reference for practical work.

2. The special nature of interrogation in telecommunications network fraud cases

2.1 Characteristics of telecommunication network fraud cases

Unlike traditional fraud and other common contact crimes, telecom network fraud is characterized by its technical, gang, and cross-regional nature. In terms of modus operandi, traditional fraud cases require contact between perpetrators and victims, with backward means and a single crime scene, while telecom network fraud perpetrators use VOIP, GOIP, dynamic QR codes, new cloud control systems, and other sophisticated technical means to defraud across borders through electronic device platforms, with complex and stealthy means and constantly updated fraud techniques. In terms of the main perpetrators, the perpetrators of telecom network fraud rarely work "alone" and often appear in the form of a gang. Gang members often have a common goal and a clear division of responsibilities, forming a complex and complete chain of interests from the provision of tools to the implementation of fraud to money laundering. In terms of operational efficiency, telecom network fraud is low-cost and high-return; using technical software and network platforms, perpetrators only need to "move their hands" and "move their mouths" in front of the computer or telephone to transfer a large amount of the victim's property to their designated account in a short period of time and successfully obtain high illegal benefits.

2.2 Psychological characteristics of suspects in telecommunications network fraud cases during interrogation

Since telecom network fraud cases and the psychology of the perpetrators are inseparable, investigators should look for interrogation breakthroughs based on their psychological characteristics and quickly break through their psychological defenses so as to obtain the suspect's confession. The psychological characteristics of the suspects in telecommunications network fraud cases are the following: 1) conceited psychology. Because of the high level of technology used in telecom network fraud, certain barriers are formed, so the suspects consider themselves to be highly intelligent and technical and look down on the suspects in other cases, thinking that their modus operandi is not "advanced" enough, so they feel resistant to their status as suspects and disdainful of police interrogations. 2) Vanity psychology The reason why the suspects choose this means of committing telecommunication network fraud is, on the one hand, because they are not willing to exchange their hard work for payment, and this crime model is in line with the criminal psychology of lazy people who pay less and get more in return, and on the other hand, because they can obtain high illegal benefits in a short period of time and, by squandering the illegal gains, they can make people around them recognize themselves[2]. 3) the psychology of fear of crime. The fear of guilt is a state of mind in which the suspect is afraid of being exposed and punished for his crime. Most of the perpetrators have a clear understanding of their criminal behavior and choose to commit online crimes like telecom network fraud in order to minimize the chance of exposure and thus reduce the probability of being caught. The perpetrators move to other provinces or even foreign countries to make themselves as safe as possible through the spatial and judicial inconveniences between regions and even countries. 4) Fluke psychology A "fluke mentality" is a state of mind in which the suspect believes that he can escape culpability. This mentality comes from the suspect's blind confidence in his counter-interrogation ability, contempt for the public security authorities, and his belief that he is experienced and capable of dealing with the investigators' interrogation offensive; on the other hand, the suspect is confident that he is technologically advanced and will not leave traces with the help of Internet tools, so he is gullible that the investigators will not obtain conclusive evidence. 5) the psychology of conspiracy to confess. Telecommunication network fraud is almost always a gang crime; the members have relative stability; large-scale, organized criminal groups will be established at the beginning of the establishment of the offensive and defensive alliances; the members have agreed to "not betray associates"; there has been training and brainwashing of members of the organization; there is a unified anti-interrogation caliber; so in the early stages of interrogation, the refusal to confess attitude is more obvious; with the prior fictitious circumstances to cover up the gang's criminal behavior, the answer is not the question; trying to conceal the sea

3. Current problems in the interrogation of telecommunications network fraud cases

3.1 The lack of professional interrogation personnel affects the efficiency of handling cases

The investigation and interrogation of telecom network fraud cases not only require mastery of the organization of various cases, process methods, technical means, etc., but also the experience of handling

new cases. However, there is no strict training and guidance for interrogation personnel, resulting in a lack of interrogation expertise and investigators' habits of interrogation that make it difficult to prescribe the right medicine to work quickly and effectively, thus affecting the efficiency of telecommunications network fraud cases.

3.2 The suspect's refusal to testify is tough and difficult to respond to effectively

Refusal to confess refers to the suspect's denial of the crime or refusal to answer questions during interrogation. Because of the hidden nature of telecommunication network fraud and the existence of the suspect's ego, fluke, fear of crime, and other special psychological factors, it is easier to form a psychological attitude of refusal to confess. The psychological attitude of refusing to confess is reflected in soft and hard behaviors, recklessly contradictory behavior, prevarication, not saying anything, and so on. In a stable gang criminal structure like telecom network fraud, the choice of interrogation breakthrough is more difficult.

3.3 The suspect's ability to counter-interrogate leads to slow progress of case interrogation

Due to the instinctive reaction of the suspect to avoid harm and the existence of the psychology of fluke, most telecommunications network fraud suspects will take certain counter-interrogation tactics in an attempt to muddle through and escape the law, specifically to test the bottom: denying, silent refusal to confess, active strategy counterattack, false confessions, false innocence, false accusations, changing the subject, throwing small concealment, and other behaviors. These behaviors not only increase the difficulty of handling the case, hindering the smooth conduct of interrogation, but also have a psychological and emotional impact on the investigators, disrupting the original interrogation plan and rhythm.

3.4 The criminal group is well organized and it is difficult to grasp the whole picture of the case

Telecommunication network fraud crimes are mostly committed by gangs and gradually form the characteristics of syndication and specialization, which are well organized, clearly divided, independent of each other, and have their own duties. The organization's management system has a pyramid-shaped structure, with top-level decision makers, middle-level technical preparers, and bottom-level fraud launderers. Such a mode of operation brings a complicated workload and great challenges to investigators. In such a context, it is difficult to grasp the whole picture of the case if the main lines of the case and the main personnel cannot be accurately grasped, with the interference of the suspects' counter-interrogation.

4. Measures to improve the quality and efficiency of interrogation in telecommunications network fraud cases

4.1 Careful selection of interrogators and improve professional interrogation skills

Interrogation work is an important part of the investigation procedure and the main way to expose crime because of the strong professionalism of telecommunication network fraud, so the requirements for investigative interrogators are high, not only to be proficient in the relevant legal knowledge system and familiar with the investigation of the various procedures but also to have a certain understanding or even mastery of telecommunications network technology, criminal psychological analysis methods, money analysis methods, fraudulent means, and other areas of knowledge. Therefore, in order to better achieve the purpose of interrogation work to expose crimes and identify facts, it is necessary to carefully select civilian police officers with suitable work levels and professional abilities for interrogation and also to use them as a standing professional force for the investigation of telecommunication network fraud cases[3]. Public security colleges and front-line units should also pay attention to cultivating the professional ability of interrogators and broadening the scope of learning in the process of education so as to provide talent support for conducting telecommunications network fraud crime investigation and interrogation operations.

4.2 Comprehensive mobilization of resources from all sides to strengthen the ability to obtain evidence and fix evidence

The wide range of telecommunication network fraud cases makes the grassroots public security

organs handle such cases with certain limitations in terms of investigative resources, technical platforms, and police security, so the investigative departments of public security organs should effectively use resources from all aspects and fully mobilize the advantageous resources of intelligence, public security, economic crime investigation, network technology and security, technical investigation, the legal system, and other departments and police types internally[4]. Externally, we should actively seek the strength and resources of all walks of life, strengthen communication and collaboration with banks, Internet companies, information and communication companies, financial institutions, and other departments to collect, summarize, and fix the evidence and case-related materials in a timely manner, including electronic data, communication records, conversation scripts, and other information flow evidence, but also transfer records, capital flows, and other capital flow evidence with behind-the-scenes "the gold master," personnel background, role division, and other personnel flow evidence, for the telecommunications network fraud crime, fraud, crime, interrogation, and other investigative procedures, to provide direction and evidence to support the suspect and to reduce the possibility of retracted confessions.

4.3 Advance mastery of case materials and detailed interrogation plans

Because of the complexity of telecommunications network fraud cases, the interrogators must summarize and master the various materials and information collected at the current stage of the case in advance, conduct a comprehensive analysis of the development process of the case, summarize the basic information on the network communication technology and software used by criminal gangs, including telephone numbers, bank accounts, etc., to summarize their modus operandi and crime patterns, and provide the next interrogation with convincing information support for the next interrogation. After mastering the case materials, it should be based on the relevant evidence collected combined with the psychological situation of the suspect to develop a more detailed interrogation plan, including the order of interrogation, evidence production time, and other content, with a clear direction of investigative interrogation and an interrogation process focused on the issue, to be prepared to improve the efficiency of pretrial work.

4.4 Based on the psychological characteristics of suspects, accurate implementation of interrogation breakthrough

Telecom network fraud suspects have a strong anti-interrogation ability and a more determined attitude to refuse to confess, so investigators should develop targeted interrogation strategies to more effectively break through their psychological defenses based on the psychological behavior characteristics of different telecom network fraud suspects at different stages of interrogation, combined with the actual situation. For suspects with a more prominent ego psychology, you can let the investigators with a higher level of cultural knowledge talk with them, and in the course of the conversation, a series of explanations and rebuttals to the suspect's proud knowledge and technology can make a positive breakthrough in the suspect's self-esteem and reduce his ego psychology. For the more obvious vanity of the suspect, it can be stated and interpreted as the "momentary pleasure" and the "bitter fruit" of the relationship between the stakes, to retain their "face," or to positively point out that the weak side is broken. For suspects with a prominent fear of crime, the combination of the plea system and emotional probation can be used to break through the psychological weakness of the confession[5]. For suspects with a more prominent fluke mentality, the use of evidence should be combined with the use of evidence in an appropriate manner, and the evidence in hand should be released to them at the right time to eliminate their fluke mentality. For the more stable criminal groups, timely use of the group of low-ranking members paying more in return for less and high-ranking members paying less in return for more contradictions and conflicts, combined with the implementation of the plea system of leniency, will help divide and dismantle.

4.5 Do a good job in the remaining crimes to dig deeper and expand the results of the investigation and interrogation

Telecommunications network fraud in the form of gangs, and frequently for multiple consecutive crimes, professionalism, high level of professionalism, the case is often detected only part of the criminal facts and some of the suspects; many cases are not mastered by the investigators, digging deeper to expand the value of the line; as a result, interrogation should accurately grasp the main line and the main members of the criminal gang on the basis of all-out efforts to uncover the main line and the main members of the criminal gang.

5. Conclusion

The interrogation of telecommunications network fraud suspects is different from ordinary criminal suspects, which is mainly reflected in the significant characteristics of telecommunications network fraud itself, such as the large number of cases, the large amount of funds involved, the criminalization of criminal gangs, and the technicalization of crime, as well as the suspects' self-conceit, weakness, fear of crime, luck, collusion, and other mentalities, which bring great challenges to the interrogation work and also reflect some problems in practice. In view of these problems, effective countermeasures should be put forward from the aspects of personnel training, making plans, psychological breakthroughs, and digging deep into residual crimes so as to greatly improve the quality and efficiency of interrogation of such cases and achieve the macro-purpose of curbing the high incidence of telecommunications network fraud crimes.

References

[1] Zhang Xiaona. The 50th Statistical Report on the Development of China's Internet Released [N]. Democracy and Legal Times, 2022-09-02(001).
[2] He Jinchao. Research on interrogation countermeasures of telecommunication network fraud cases based on the psychological characteristics of criminal suspects [J]. Forest Public Security, 2022(01): 7-12.
[3] Liu Shenshi. Research on interrogation countermeasures for suspects in telecommunication fraud cases [J]. Law and Society, 2017(11):210-211.
[4] Song Ping. Research on the current situation of interrogation work of telecommunication network fraud investigation and its countermeasures [J]. Journal of Zhejiang Police Academy, 2022(02):41-47.
[5] Leng Bing. Analysis of psychological characteristics of telecommunication fraud suspects and interrogation countermeasures [J]. Western Journal,2022(18):69-73.