International Journal of Research Studies in Management
2024 Volume 12 Number 8, 205-218

Influencing factors, challenges, countermeasures on telecommunication fraud in Sichuan Province, China

Han, Chenglin ✉
Graduate School, Lyceum of the Philippines University - Batangas, Philippines (402372549@qq.com)

Received: 30 July 2024
Revised: 5 August 2024
Accepted: 8 August 2024
Available Online: 9 August 2024
DOI: 10.5861/ijrsm.2024.1216

ISSN: 2243-7770
Online ISSN: 2243-7789

OPEN ACCESS

Abstract

This study adopted a descriptive quantitative design to analyze telecom fraud in Sichuan Province, China, examining influencing factors, challenges, and countermeasures. It surveyed 405 randomly selected police officers to describe their demographic profiles and understand telecom fraud from their perspectives. Findings indicated that technological advancements, economic downturn, income disparity, and inadequate supervision created favorable conditions for telecom fraud. Challenges included legal lag, insufficient personal information protection laws, corporatization and high-tech nature of fraud organizations, difficulties in evidence collection, and rapid fund transfers. The study recommends improving legislation, enhancing crime-fighting efforts, strengthening industry supervision, and increasing social participation to effectively control telecom fraud, protect people's interests, and maintain social stability.

Keywords: telecommunications, fraud, influencing factors, challenges, countermeasures

Influencing factors, challenges, countermeasures on telecommunication fraud in Sichuan Province, China

1. Introduction

The concept of telecommunications fraud is defined as the use of telecommunications, the Internet, and other technical means to contact the victim for the purpose of illegal possession, and to deceive the victim by fabricating facts or concealing the truth, thereby infringing on public or private property(Zhang，2023). The crime of telecommunications fraud seriously infringes on the property interests of the people, and at the same time, the social harm caused by it is also becoming increasingly prominent, such as guiding young people's bad value orientation, triggering a crisis of social trust, affecting the credibility of government departments, breeding black and gray industrial chains, deriving upstream and downstream crimes, and a large amount of public and private property flowing abroad. Telecom network fraud has become the most harmful type of property infringement crime in society(Li,2023).

According to the 53rd Statistical Report on China's Internet Development released by the China Internet Network Information Center (CNNIC), as of December 2023, the number of Internet users in China reached 1.092 billion, and the Internet penetration rate reached 77.5%. The rapid development of telecommunication network technology has not only greatly facilitated people's communication and life, but also created space for telecommunication network crimes. As far as fraud crimes are concerned, since 1994, telecom fraud has surpassed traditional fraud, and the crime rate has remained high, and has become a serious tumor restricting economic and social development, seriously infringing on people's property security, undermining social stability, hindering economic development, causing economic losses of more than one trillion yuan per year (Sun, 2018), and even causing serious consequences such as suicide of many victims and corporate bankruptcy, such as the "Xu Yuyu incident" in 2016. Xu Yuyu, a prospective college student from a poor family, suffered cardiac arrest because she was defrauded of 9,000 yuan, and died after ineffective medical treatment (Procuratorate Daily, 2016).

Although the whole country and the province have concentrated their efforts on cracking down on telecom fraud and have achieved phased results, the current situation of prevention and control of telecom fraud is still grim, and telecom network fraud is still the type of crime with the largest number of cases, the fastest rising rate, and the widest coverage. According to data released by the Ministry of Public Security in 2024, from January to November 2023, public security organs across the country intercepted a total of 2.75 billion fraudulent phone calls and 2.28 billion text messages, disposed of 8.364 million fraudulent domain names and websites, and urgently intercepted 328.8 billion yuan of funds involved in the case. According to the 2024 report released by the Sichuan Provincial Public Security Department, in 2023, telecom fraud cases have accounted for 25% of the total number of criminal cases in Sichuan Province, 8,163 cases have been cracked, more than 18,000 criminal suspects have been arrested, 4.755 billion yuan of fraudulent funds have been frozen, and 1.43 million fraudulent Internet accounts have been cleaned up.

In view of the above situation, the researcher conducted a comprehensive investigation, analysis and research on the telecom fraud crime in Sichuan Province around the three variables of influencing factors, challenges and countermeasures, and put forward corresponding suggestions, to provide some valuable references for the theory and practice of telecom fraud prevention and control. Zhang (2021) defined Influencing factors as the direct and indirect factors that lead to the crime of telecommunications fraud. Relative to such, the primary factor is the progress of science and technology. The biggest difference between telecom network fraud and traditional fraud is that the criminal process relies on telecom technology, which is the product of the combination of traditional fraud and modern communication technology. The development of communication technology and the popularization of smart devices have objectively provided technical support for telecom

fraud (Ding, 2019).

The unbalanced economic development and the widening gap between the rich and the poor have prompted some poor people to engage in telecom fraud to obtain high returns. Some studies have shown that poverty-stricken areas are more likely to be areas with a high incidence of telecom fraud (Du, 2022). At the same time, with the development of the economy, social values are more diversified, and more and more people regard wealth as the highest standard of success. The idea of money worship and the concept of profit-seeking have led some people to ignore the law and embark on the criminal road of telecommunications fraud (Li, 2023). Another factor is due to the weak government supervision and lack of industry self-discipline in the communications, financial and banking industries, as well as related Internet enterprises, there has been a leakage of user information and lax account opening review. These regulatory loopholes not only facilitate telecom fraud, but also contribute to the black industry related to telecom fraud (Huang, 2021). Moreover, through the analysis of fraud cases, it can be found that due to the victims' weak awareness of prevention and weak prevention ability, some victims have the psychology of getting rich for nothing or overnight, and some victims are not familiar with financial transfer and telecommunication services, and lack basic legal knowledge, which provides a large number of opportunities and conditions for fraudsters (Xi, 2023).

Sun (2020) defined challenges as mainly as the obstacles and dilemmas existing in the governance of telecom fraud crimes. Among these challenges is the conflict between the inherent limitations of the law and the variability of telecom fraud, so that the speed of updating laws and regulations cannot keep pace with the progress of criminal technology, in fact, some new types of fraud cannot be accurately convicted and sentenced. At the same time, China's laws and regulations on citizen information protection and electronic evidence identification are not perfect enough, and there is still a certain gap between China and developed countries in the West. Furthermore, telecommunications fraud is basically committed by gangs, and even adopts corporate operation, which has obvious characteristics of specialization, intelligence, trans-regional, and transnational characteristics, and the rapid renovation of fraud methods and the strict organizational structure have greatly increased the difficulty of cracking down (Li, 2018). Another challenge is in the process of investigating telecom fraud crimes, due to the limited police force and funds, coupled with the difficulty of obtaining evidence and relevant data involved in the case, the difficulty of preserving electronic evidence, the difficulty of sorting out the funds involved in the case and the rapid transfer, and the wide distribution of criminal suspects and even transferring abroad, the investigation of telecom fraud is complex and arduous (Zhang, 2021).

It is important to note too that the black industry is growing with the development of telecom fraud, forming a complete industrial chain and solid interest groups, such as encrypted communication tools, malware development, information trafficking, and money laundering. The participation of these illegal industries has greatly increased the concealment, complexity and transnational nature of telecom fraud, making it more challenging to combat and prevent telecom fraud (Du, 2018). Countermeasures mainly refer to the criminal and non-criminal measures taken to prevent and control the crime of telecommunications fraud. Song (2021) suggested to improve legislation, that is, improve the current legal system, update the law to cover new types of telecommunications fraud, and clearly stipulate the legal responsibilities and penalties for different types of fraud, so as to enhance the pertinence and operability of the law. At the same time, it is necessary to strengthen legislation on citizen information and electronic evidence, further consolidate the government's responsibility for industry supervision, reduce the possibility of telecom fraud from the source, and improve the ability of judicial organs to combat telecom fraud (Cheng, 2021).

Liu (2022) on the other hand, stressed that it is necessary to strengthen the crackdown on criminal crimes, by increasing investment in technology and resources, strengthening international cooperation, innovating case-handling models, and strengthening cooperation between the police and the Internet, telecommunications, financial enterprises, and other government departments, so as to form a joint force in the fight against fraud and build a more efficient crackdown system. Teng (2022) resolves to strengthen industry supervision, promote self-discipline and cooperate in related industries such as communications, banking and the Internet through

government supervision and industry self-discipline, establish intra-industry and cross-industry risk prevention and control mechanisms, upgrade technology, share information, and coordinate to combat telecom fraud. In addition, it is imperative too to expand social participation, give full play to the role of schools, media, and communities in publicity and education, strengthen public anti-fraud education, and improve public awareness and skills for prevention (Song, 2020).

In summary, this study used literature research, questionnaire survey, interviews and case studies to investigate and describe the telecom fraud crime in Sichuan Province, focusing on the analysis of the influencing factors, challenges and countermeasures, hoping to be helpful to judicial theory and practice.

Objectives of the study - This study analyzed the influencing factors, challenges, and countermeasures of telecommunications fraud crimes in Sichuan Province, with the goal of enriching and improving existing academic research and providing valuable references for judicial practice. Specifically, this study identified the influencing factors of telecommunications fraud crimes in terms of technological, economic, regulatory and defensive factors. It also determined the challenges in combating telecommunications fraud from the perspectives of top-level design, criminal organizations, criminal investigation, and the illegal industry. It also discussed the countermeasures to the challenges as to improving legislation, strengthening fight on crime and industry regulation, and expanding social participation. In addition, the study tested the relationships among influencing factors and challenges, influencing factors and countermeasures, and challenges and countermeasures. Furthermore, from the perspectives of improving legislation, increasing crackdowns, strengthening industry supervision, and expanding social participation, this study proposed an improvement plan to combat telecommunications fraud crimes.

2. Methods

Research Design - A descriptive and quantitative study design was used in this study. Descriptive research is a method of collecting materials, analyzing them, describing the laws, characteristics, and development of things in order to obtain the final descriptive results. Descriptive quantitative research designs are suitable for measuring variables or establishing relationships between variables. Therefore, this study collects the data of survey respondents and performs data analysis to describe and interpret the influencing factors, challenges and countermeasures of telecom fraud crime in Sichuan Province, China, and their relationships. The questionnaire includes descriptive items to investigate participants' attitudes towards the three variables and the relationship between the three variables.

Participants - The police are a professional group directly responsible for the investigation of telecommunications fraud crimes, and can directly face criminal suspects, victims, and relevant individuals and enterprises, have rich experience in handling cases and a high level of law, have mastered a large number of telecommunication fraud case information and typical cases, and at the same time, through investigation practice, can put forward targeted and effective legal and policy suggestions. Therefore，in this study, police officers from Chengdu, Guangyuan, Ya'an, Nanchong, Aba and other cities and prefectures in Sichuan Province were selected as the research objects. The origins of these police officers cover the capital cities of Sichuan Province, ordinary cities, ethnic minority areas, and remote areas, and the level of these police officers covers the three levels of province, city and county. The study used a random sampling method, with a minimum indicator of 385 respondents at a 95% confidence level and a 5% difference limit according to the Raosoft sample calculator. To broaden the scope of the study, the sample was later expanded to 405 people.

Instrument - On the basis of relevant literature research, three variables were identified: influencing factors, challenges and countermeasures. The questionnaire is divided into four parts. The first part consists of demographic information, including five pieces of information: gender, age, years of work, education, and major. The second part includes 4 dimensions of influencing factors, with a total of 20 questions. The third part consists of 4 dimensions of the challenge with a total of 22 questions. The fourth part includes 4 dimensions of

countermeasures, with a total of 20 questions. The specific sources of the questionnaire are as follows. Based on the literature "Research on the Dilemma and Countermeasures of Telecom Network Fraud Governance" written by Zhang Yang (2021) and "Research on the Regulatory Problems and Countermeasures of Telecom Fraud in Sichuan Province from the Perspective of Platform" written by Xu Yongmei (2022), the influencing factor questionnaire was compiled. The questionnaire consists of 4 subscales and 20 questions. The subscales include technological factors, economic factors, regulatory factors, and defensive factors.

Based on the literature "Research on Telecom Fraud Crime and Its Governance" written by Sun Shaoshi (2018) and "Research on the Current Situation and Countermeasures of Telecom Network Fraud" written by Sun Gaofeng (2020), the challenge questionnaire was compiled. The questionnaire consists of 4 subscales and 20 questions. The subscales include top-level design challenges, criminal organization challenges, criminal investigation challenges, and illegal industry challenges. Based on the literature such as "Methodology for the Investigation of Telecom Network Fraud" written by Fang Kanglan (2022) and "Research on the Optimization of Anti-telecom Fraud Network Propaganda Path from the Perspective of Media Space" written by Yang Xin (2023), a countermeasure questionnaire was compiled. The questionnaire consists of 4 subscales and 20 questions. The subscales include improving legislation, strengthening the fight against crime, strengthening industry regulation, and expanding social participation. After determining the questionnaire information, the researcher randomly selected 30 police officers for reliability and validity testing. After collecting 30 questionnaires, the researcher sent the questionnaires and data to data analysts for reliability and validity testing. The specific results are as follows:

Table 1

Reliability Test

Indicators	Cronbach Alpha	Remarks
Technological factors	0.928	Excellent
Economic factors	0.820	Good
Regulatory factors	0.940	Excellent
Defensing factors	0.914	Excellent
Top-level design challenges	0.808	Good
Challenges of criminal organizations	0.982	Excellent
Challenges in criminal investigations	0.931	Excellent
Challenges of the illicit industry	0.924	Excellent
Improve legislation	0.883	Good
Strengthen criminal crackdowns	0.979	Excellent
Strengthen industry supervision	0.985	Excellent
Expand social participation	0.984	Excellent

The reliability coefficient is an important metric to measure a test or scale, with a coefficient value between 0 and 1. There are many kinds of reliability coefficients, and the one with a higher rating rate is the α reliability coefficient. When the α reliability coefficient is greater than 0.9, it indicates that the results are excellent, and when it is greater than 0.8, the results are good. As shown in Table 1, the test results for each dimension are all above 0.8. The highest score was for "Strengthen industry supervision" (0.985), followed by "Expand social participation" (0.984) and "Challenges of criminal organizations" (0.979). Therefore, the questionnaire demonstrates good reliability. After completing the pilot test and obtaining the consent of the mentor, the researcher began distributing questionnaires to 405 respondents to collect a larger range of data for analysis.

Data Gathering Procedure - After obtaining the consent of the supervisor, the researcher translated all questions into Chinese and English. By informing and explaining the purpose of the survey, and after the confidentiality review, the questionnaire was imported into the "Questionnaire Star" Mini Program for distribution. The researcher exported the collected data in Excel format through the "Questionnaire Star" applet, and used SPSS software for reliability testing and data analysis.

Data Analysis - Once the data was collected, the data analyst used the SPSS 28 statistical analysis tool for processing. According to the results of the study, the researcher used difference analysis, correlation analysis and

other methods to explain and test the attributes of each variable and the correlation between the three variables. The analysis focused on determining the extent to which the participant disagreed or consented from the questionnaire data to determine the participant's attitude towards the three variables and the relationship between the three variables.

Ethical Considerations - The survey was conducted with the consent of the participants. For ethical reasons and confidentiality reasons, the questionnaire does not ask for the names of the participants, under no circumstances will the information of the respondents be disclosed, and the questionnaire does not involve any case information, personal privacy and other information and data that needs to be kept confidential. In addition, the purpose of the study is fully explained at the beginning of the questionnaire, and the results are used for academic research only.

3. Results & discussion

Table 2

Summary Table on Influencing Factors

Indicators	Weighted Mean	Verbal Interpretation	Rank
Technological factors	3.38	Agree	4
Economic factors	3.59	Strongly Agree	1.5
Regulatory factors	3.59	Strongly Agree	1.5
Defensing factors	3.57	Strongly Agree	3
Composite Mean	3.53	Strongly Agree	

Legend: 3.50 – 4.00 = Strongly Agree; 2.50 – 3.49= Agree; 1.50 – 2.49 = Disagree; 1.00 – 1.49 = Strongly Disagree

Table 2 summarizes the four major factors influencing telecom fraud: technical, economic, regulatory, and defensive, with an overall average score of 3.53, indicating that these factors were generally considered to be strongly agreed which significantly influence the occurrence of telecom fraud. Ranked first was economic factors (weighted average score of 3.59). This suggests that economic factors become one of the most important factors. Studies have shown that economic downturn, income inequality and high unemployment have a significant negative impact on crime rates, and that the impact of the market economy will increase the motivation to commit crimes, which in turn will lead to higher crime rates.

Another factor ranked first was the regulatory factor (weighted average score of 3.59). This shows that the loopholes in government and industry regulation are an important factor in the generation and development of telecom fraud. Due to the lack of a solid concept of security development, telecommunications, communications, banks and other relevant industry entities closely related to telecommunications fraud focus too much on economic benefits, ignore social responsibilities, and are not strict and inadequate in implementing national policies and regulations. For example, problems such as illegal card issuance by communication operators and illegal handling of non-real-name bank cards by banks are still prominent. All of this is an important tool for fraudsters to carry out fraudulent activities and successfully transfer funds. (China Academy of Information and Communications Technology, 2018) Of course, the implementation of policies and regulations in these industries is not in place, which itself also exposes the weaknesses of the relevant government authorities in consolidating the regulatory responsibilities of industry entities (Ke, 2020).

Ranked third was the defensive factor (weighted average score of 3.57), which indicates that the lack of public awareness and ability to prevent it is also one of the key factors in telecom fraud. Telecom fraud is not a crime that fraudsters can complete unilaterally, and requires the "cooperation" of the victim. However, due to the lack of necessary legal, financial and other common sense, or out of the psychology of greed for cheapness, the victim did not identify and prevent the fraudulent information, which led to the success of the fraudster. The main reason is that the public's awareness of prevention is relatively weak, and many victims are blindly confident and always think that they will not be deceived, so that their prevention is lax, which has become an important reason for the repeated success of fraud (Cao, 2022).

Ranked fourth was the technical factor (weighted average score = 3.38), which, although in the "agree" range, also indicates that the role of technical factors in telecom fraud is also widely recognized. This is basically consistent with the basic principle of Marxism, that is, the material base determines the superstructure. Specifically, without telecommunications, there would be no telecommunications fraud. At present, strong technology is a prominent feature of telecom fraud. Fraudsters commit fraud through contactless means, relying on basic technologies such as notification SMS technology, cross-border data communication technology, short URL service technology, online social software technology, etc., and even cutting-edge technologies such as big data technology and artificial intelligence technology (Zhang, 2022). These technological advances, on the one hand, reduce the cost of violating the law, reduce the technical requirements for practitioners, and on the other hand, also improve the accuracy and success rate of fraud.

Table 3

Summary Table on Challenges

Indicators	Weighted Mean	Verbal Interpretation	Rank
1. Top-level design challenges	3.60	Strongly Agree	2
2. Challenges of criminal organizations	3.61	Strongly Agree	1
3. Challenges in criminal investigations	3.56	Strongly Agree	4
4. Challenges of the illicit industry	3.58	Strongly Agree	3
Composite Mean	3.59	Strongly Agree	

Legend: 3.50 – 4.00 = Strongly Agree; 2.50 – 3.49= Agree; 1.50 – 2.49 = Disagree; 1.00 – 1.49 = Strongly Disagree

Table 3 shows that all four challenges to telecom fraud governance were highly recognized as "strongly agree" levels (3.50 – 4.00). The overall average was 3.59, indicating that respondents generally believed that these challenges were significant in the governance of telecom fraud.

At the top of the list was challenges of criminal organizations (weighted average score of 3.61). This indicates that respondents agreed that criminal organizations posed the greatest challenge to tackling telecom fraud. In the game of fraud and anti-fraud, fraud organizations show the characteristics of professionalism, corporatization, specialization, etc., the internal division of labor is becoming more and more clear and refined, the technology and equipment used are becoming more and more advanced, the degree of intelligence of crime methods is getting higher and higher, and the forms of fraud are becoming more and more diverse, and the speed of update and change is extremely fast. The dens and ringleaders of fraud organizations are hiding abroad, and cross-border fraud has become a mainstream trend. All these have brought great difficulties to cracking down on telecommunications fraud (Dong, 2023).

Ranked second was Top-level design challenges (weighted average score of 3.60). This indicates that respondents strongly agreed that the imperfection of legislation seriously restricts the effective governance of telecom fraud. In China's current criminal law system, the crime of telecom fraud is still treated as an ordinary crime of fraud, and there is no separate provision for the crime of telecom fraud, and there is no refinement of the crime of telecom fraud. In contrast, special frauds such as contract fraud and fund-raising fraud have been separated from ordinary frauds and provided for separately, reflecting the importance and improvement of legislation. Obviously, the legal provisions cannot meet the needs of preventing and combating telecommunication fraud, and cannot achieve the desired results, which also leads to the situation that in judicial practice, judicial organs have different judgments due to different understandings of such crimes (Liu, 2023).

At the same time, China does not currently have a unified electronic evidence law. The existing law focuses too much on the collection of electronic evidence and ignores the admissibility of evidence, resulting in a lot of evidence that cannot be used as the basis for conviction (Zhang, 2018). Although the promulgation of the Personal Information Protection Law provides an important guarantee for the security of personal information, there are still some gaps. For example, the personal information protection law does not clearly state the principles of personal information processing, which gives information processors more room for interpretation. To a certain extent, this leads to the possibility that information processors may abuse the right of interpretation and infringe on user privacy (Cao, 2022).

Ranked third was Challenges of the illicit industry (weighted average score of 3.58). This indicates that respondents strongly agreed that the illicit industry had become a significant challenge to the governance of telecom fraud. In general, telecom fraud involves multiple steps and requires multiple resources to be successfully implemented, and it is difficult for a single person to complete all the criminal steps. As telecom fraud becomes more and more specialized, and criminal income becomes more and more stable, a series of related illegal and criminal activities (such as money laundering, information trafficking, etc.) actively participate in it and develop and grow, and finally form a large-scale industrial chain. Based on the relationship between supply and demand, these black industries provide a variety of information, technology and other services for telecom fraud, which further enhances the degree of specialization of telecom fraud and makes it more difficult to combat and prevent telecom fraud (Huang, 2021).

Ranked fourth was Challenges in criminal investigations (weighted average score of 3.56). This indicates that the respondents strongly a that the agreed difficulties faced by criminal investigation activities themselves seriously restricted the effectiveness of telecom fraud governance. From the perspective of security, the public security organs themselves have limited police force, there is a shortage of professional personnel, and the financial guarantee is not sufficient when investigating and prosecuting major telecommunications fraud criminal activities, all of which limit the intensity of the public security organs' crackdown. From the perspective of investigation, the crime of telecommunications fraud is a kind of well-organized and large number of gang crimes, fraud activities have the characteristics of concealment, cross-border and high-tech, the collection and fixation of electronic evidence involved in the case has high requirements, and it is very easy to tamper with and destroy, which makes it difficult to carry out the investigation work such as arrest and evidence collection, so that the incidence rate of telecommunication fraud is very high, but the detection rate is very low (Liu, 2022).

Table 4

Summary Table on Countermeasures

Indicators	Weighted Mean	Verbal Interpretation	Rank
1. Improve legislation	3.60	Strongly Agree	3
2. Strengthen criminal crackdowns	3.60	Strongly Agree	3
3. Strengthen industry supervision	3.64	Strongly Agree	1
4. Expand social participation	3.60	Strongly Agree	3
Composite Mean	3.61	Strongly Agree	

Legend: 3.50 – 4.00 = Strongly Agree; 2.50 – 3.49 = Agree; 1.50 – 2.49 = Disagree; 1.00 - 1.49 = Strongly Disagree

Table 4 shows that the four countermeasures for the prevention and control of telecom fraud crimes are highly recognized as "strongly agree" levels (3.50 – 4.00). The overall average was 3.61, indicating that respondents generally believed that these countermeasures were necessary and effective in tackling telecom fraud. At the top of the list was strengthen industry supervision (weighted average score of 3.64). This indicates that strengthening industry supervision is essential for the prevention and control of telecom fraud crimes.

If the industry does not strictly implement the real-name system and other requirements, although it can achieve short-term prosperity, in the long run, as telecom fraud and other cybercrimes become more and more rampant, it will inevitably affect the development of the entire economy and society, and ultimately endanger the security and development of the industry itself. Therefore, the communications, finance and Internet industries should strengthen supervision and put the control of telecom fraud and enterprise development in an equal position (Li, 2023).

The prevention and control of telecom fraud is a complex and long-term task, and it depends on the cooperation and linkage between the public security organs and the communications, finance and Internet industries to integrate resources more scientifically and rationally and fight crime more effectively. At present, the criminal acts of telecommunication fraud are mainly communicated through the communication industry or the Internet, and the use of banking services and financial institutions to achieve the transfer of funds. Therefore, on the one hand, these industries should strengthen cooperation with the public security organs, cooperate with the investigation and evidence collection, and open data to the greatest extent. On the other hand, it is necessary

to strictly implement the responsibility of industry governance, strictly implement the real-name registration system, closely monitor abnormal mobile phone cards, bank cards and online accounts, and at the same time strengthen technical investment, upgrade interception, shielding and other security prevention technologies, and resolutely safeguard the property interests of customers, so as to block the flow of funds and information for telecommunications fraud, so as to effectively crack down on money laundering, information trafficking and other illegal industries, and eradicate the breeding ground for telecommunications fraud (Xu, 2022).

Ranked third were the remaining three strategies: Improve legislation, Strengthen criminal crackdowns, and Expand social participation (Weighted average score of 3.60). This indicates that enhancing legislation, intensifying criminal enforcement, and broadening social involvement are indispensable for combating telecommunications fraud.

In terms of improving legislation, in order to deal with the high crime rate and serious harm of telecom fraud, it is necessary to treat telecom fraud as a separate crime according to the uniqueness of telecom fraud, and at the same time issue relevant judicial interpretations, which will become the most powerful and authoritative tool for punishing telecom fraud. At the same time, in the criminal law, it is necessary to increase the degree of punishment for the upstream crimes and downstream crimes of telecommunications fraud, so as to facilitate the full-chain crackdown on telecommunications fraud crimes and related crimes (Song, 2021).

As far as the strengthening of criminal crackdowns is concerned, it is necessary to enhance the technical capacity of investigation, and comprehensively improve the personnel, equipment, and legal capabilities of investigative organs through such means as professional training, equipment upgrades, technological updates, and strengthened assessments (Wang, 2023). Public security organs must adhere to the idea of coordinated governance, establish cross-regional and cross-border coordination mechanisms, strengthen cooperation with other government departments and relevant enterprises, innovate case-handling models, and coordinate different types of police, so as to more effectively combat crime, increase the risk and cost of telecommunication fraud, so as to collect evidence more efficiently, arrest criminals, form a strong deterrent effect, and enhance the public's sense of security and satisfaction (Wang, 2023).

At the same time, in view of the fact that telecommunication network fraud has formed a black industry chain that covers a wide range, involves many subjects, and has a close relationship between upstream and downstream crimes, the public security organs should also strengthen the criminal crackdown on information trafficking, money laundering and other related crimes (Yao, 2019).

As far as expanding social participation is concerned, it is necessary to build an anti-fraud alliance with the participation of multiple entities such as communities, banks, telecommunications companies, law enforcement departments, schools, etc., establish a joint prevention and control security mechanism, formulate a work plan for preventing fraud, widely carry out anti-fraud propaganda through one-on-one propaganda and poster posting, and call on community residents to report to the public security organs in a timely manner when they encounter suspicious calls and information (Shen, 2023).

The government should take anti-fraud propaganda as the key work of preventing telecommunication fraud, and widely mobilize public security organs, propaganda departments, anti-money laundering departments, education departments, communities, as well as communications, banks, Internet and other enterprises to participate in anti-fraud propaganda. The elderly, corporate accountants and other vulnerable groups have carried out targeted publicity and prevention work, continuously improving the coverage and pertinence of the content of publicity, and continuously improving the public's awareness of prevention and the ability to identify telecommunications fraud crimes (Du, 2022).

Strengthening industry supervision is essential for the prevention and control of telecom fraud crimes. Strengthening industry supervision and strengthening enterprise self-discipline is an effective measure to deal with telecom fraud. The financial industry should strengthen the review of customer information, and carry out

the normalization of monitoring of abnormal accounts and suspicious transactions. In the event of an abnormality, the payment stop and emergency freezing procedures shall be initiated in a timely manner, and the funds shall be unfrozen and returned in a timely manner after the risk is removed. The internet industry should regulate the products and services it provides, employing technical means to block and block communication between fraudsters and victims, and actively creating a healthy internet ecosystem (Li, 2023).

In addition to implementing the real-name system and identity verification as required, communication operators should also give full play to their strong data advantages, upgrade security prevention technology, focus on intercepting cross-border calls and text messages suspected of fraud, and improve their anti-fraud capabilities (Wang, 2021).

Table 5

Relationship Between the Influencing Factors and Challenges

Technological Factors	r-value	p-value	Interpretation
Top-level design challenges	.113*	0.023	Significant
Challenges of criminal organizations	.199**	0.000	Highly Significant
Challenges in criminal investigations	.156**	0.002	Significant
Challenges of the illicit industry	.229**	0.000	Highly Significant
Economic Factors			
Top-level design challenges	.316**	0.000	Highly Significant
Challenges of criminal organizations	.387**	0.000	Highly Significant
Challenges in criminal investigations	.359**	0.000	Highly Significant
Challenges of the illicit industry	.389**	0.000	Highly Significant
Regulatory Factors			
Top-level design challenges	.318**	0.000	Highly Significant
Challenges of criminal organizations	.375**	0.000	Highly Significant
Challenges in criminal investigations	.361**	0.000	Highly Significant
Challenges of the illicit industry	.346**	0.000	Highly Significant
Defencing Factors			
Top-level design challenges	.278**	0.000	Highly Significant
Challenges of criminal organizations	.304**	0.000	Highly Significant
Challenges in criminal investigations	.389**	0.000	Highly Significant
Challenges of the illicit industry	.318**	0.000	Highly Significant

Legend: Significant at p-value < 0.01

Table 5 shows the association between Influencing Factors and Challenges. The computed r-values indicates a moderate direct correlation and the resulted p-values were less than the alpha level. This means that there was significant relationship exists and implies that the better is the influencing factors, the more challenges experienced. Any crime is the result of a number of factors, and similarly, the intensification of any one factor will affect the crime. In the crime of telecommunications fraud, due to the progress of science and technology, the existence of loopholes in industry supervision, the lack of awareness of prevention by victims, and the influence of incorrect values, the incidence rate of telecommunication fraud is high and the amount of fraud is large. With the development of telecom fraud crimes, criminal gangs have shown obvious trends such as intelligence, specialization, and cross-border, and the fraud methods have changed rapidly, which has amplified the shortcomings of legislation and criminal crackdown, and derived illegal industries, which have further brought severe challenges to the fight against and control of telecom fraud (Zhang, 2021).

Table 6 displays the association between Influencing Factors and Countermeasures. The computed r-values indicates a moderate direct correlation and the resulted p-values were less than the alpha level. This means that there was significant relationship exists and implies that the better is the influencing factors, the greater countermeasures experienced. Any measure must be targeted in order to achieve the desired effect. In the management of telecom fraud, only by analyzing each influencing factor one by one, formulating special prevention, crackdown and control strategies, and carrying out targeted governance work, can we achieve good governance results as a whole (Wang, 2023). Taking industry supervision as an example, it is through the analysis and finding out the performance and reasons of poor supervision of communication operators that we can put forward measures such as building a new regulatory model, strengthening the construction of technical

means, and deepening police-enterprise cooperation, so as to ensure that these measures can achieve due results in actual implementation and prevent and control telecom fraud activities from the source (Shi, 2021).

Table 6

Relationship Between the Influencing Factors and Countermeasures

Technological Factors	r-value	p-value	Interpretation
Improve legislation	0.093	0.062	Not Significant
Strengthen criminal crackdowns	.284**	0.000	Highly Significant
Strengthen industry supervision	.193**	0.000	Highly Significant
Expand social participation	.150**	0.002	Significant
Economic Factors			
Improve legislation	.360**	0.000	Highly Significant
Strengthen criminal crackdowns	.413**	0.000	Highly Significant
Strengthen industry supervision	.289**	0.000	Highly Significant
Expand social participation	.294**	0.000	Highly Significant
Regulatory Factors			
Improve legislation	.326**	0.000	Highly Significant
Strengthen criminal crackdowns	.427**	0.000	Highly Significant
Strengthen industry supervision	.354**	0.000	Highly Significant
Expand social participation	.227**	0.000	Highly Significant
Defensing Factors			
Improve legislation	.322**	0.000	Highly Significant
Strengthen criminal crackdowns	.368**	0.000	Highly Significant
Strengthen industry supervision	.335**	0.000	Highly Significant
Expand social participation	.254**	0.000	Highly Significant

Legend: Significant at p-value < 0.01

Table 7

Relationship Between the Challenges and Countermeasures

Top-level design challenges	r-value	p-value	Interpretation
Improve legislation	.340**	0.000	Highly Significant
Strengthen criminal crackdowns	.321**	0.000	Highly Significant
Strengthen industry supervision	.254**	0.000	Highly Significant
Expand social participation	.228**	0.000	Highly Significant
Challenges of Criminal Organizations			
Improve legislation	.404**	0.000	Highly Significant
Strengthen criminal crackdowns	.371**	0.000	Highly Significant
Strengthen industry supervision	.281**	0.000	Highly Significant
Expand social participation	.213**	0.000	Highly Significant
Challenges of Criminal Investigations			
Improve legislation	.453**	0.000	Highly Significant
Strengthen criminal crackdowns	.414**	0.000	Highly Significant
Strengthen industry supervision	.327**	0.000	Highly Significant
Expand social participation	.251**	0.000	Highly Significant
Challenges of the Illicit Industry			
Improve legislation	.360**	0.000	Highly Significant
Strengthen criminal crackdowns	.445**	0.000	Highly Significant
Strengthen industry supervision	.292**	0.000	Highly Significant
Expand social participation	.319**	0.000	Highly Significant

Legend: Significant at p-value < 0.01

Table 7 shows the association between challenges and Countermeasures. The computed r-values indicates a moderate direct correlation and the resulted p-values were less than the alpha level. This means that there was a significant relationship and implies that the greater the challenges encountered, the greater countermeasures experienced. In the fight against crime, we the challenges had to be faced head-on and had to work to overcome them. Whether it is a criminal crackdown or a comprehensive approach, they must be dealt rationally with the difficulties and challenges faced by crimes. In recent years, telecom fraud has spread rapidly and social harm has been intensifying, which has brought severe challenges to the governance of telecom fraud. In order to effectively deal with the crime of telecommunications fraud, it is necessary to adopt a practical and effective approach to address the challenges. For example, due to the challenges posed by cross-border fraud by fraud gangs, international police cooperation must be strengthened to deal with them. Another example is the

challenges brought about by the information trafficking industry, which must be targeted in terms of intelligence sharing, joint arrest, remote evidence collection, etc. Only in this way can we curb the spread of telecommunications fraud and safeguard citizens' property rights and interests and a safe and stable social environment (Ding, 2019).

4. Conclusion and recommendations

In general, the prevalence of telecommunication fraud in Sichuan Province was notably shaped by various factors including technological, economic, regulatory, and defensive elements. While economic and regulatory factors were the most influential in the context of telecom fraud, defensive and technological aspects also significantly contributed to the dynamics of such crimes. The governance of telecom fraud in Sichuan Province faced significant hurdles across various domains, including criminal organizations, top-level design, the illicit industry, and criminal investigations. While criminal organizations presented the most significant challenge, top-level design issues, the illicit industry, and difficulties in criminal investigations also played critical roles in the governance of telecom fraud in Sichuan Province. The evaluation of countermeasures for addressing telecom fraud in Sichuan Province reflected a broad consensus on the importance of several strategic approaches. There was a clear pattern where improvements or increases in influencing factors correlate with greater challenges and necessitated more robust countermeasures. Conversely, as challenges became more pronounced, the intensity and range of countermeasures also increased. This reinforced the dynamic nature of telecom fraud management, where evolving factors and emerging challenges required adaptive and effective responses to maintain control and mitigate the impacts of telecom fraud. Based on the results of the study, an improvement plan for the management of telecommunication fraud crimes was formulated.

The national legislature may devise the crime of telecommunications fraud a separate crime through legislation, draft a unified electronic evidence law, strengthen the protection of citizens' personal information, and strengthen the regulatory responsibilities of the government and industry. At the same time, the national judicial organs have promptly formulated and issued judicial interpretations based on the needs of judicial practice, providing all-round legal support for the governance of telecommunications fraud crimes. Public security organs may strengthen multi-police cooperation through innovative case-handling models, strengthen police-enterprise cooperation, international cooperation, and the extent of business enhancement and safeguards, increase investigative capacity, and further increase the force of criminal crackdowns on telecommunications fraud and related crimes. All levels of government and industry self-regulatory organizations may strengthen regulation to promote the implementation of entity responsibility for governance of telecommunications fraud by enterprises such as telecommunications, banks, and the internet, strictly implementing the real-name system, and using advanced technology to normalize efforts such as identifying, monitoring, intercepting, early warning, and freezing funds for information and transactions suspected of fraud, to continuously compress and eliminate the space for telecommunications fraud to grow. All levels of government may strengthen anti-fraud propaganda through extensive mobilization of government departments, schools, media, communities, and relevant enterprises, forming joint prevention and management work mechanisms, unblocking channels for reporting and handling, increasing the general public's awareness and ability to prevent fraud, and creating a strong anti-fraud atmosphere throughout society. The proposed governance plan based on the results of this study may be studied, implemented, and evaluated after implementation to assess its effectiveness and make any necessary adjustments. Future researchers may further study the influencing factors, challenges and countermeasures, and other variables and their relationships by expanding the sample size and adjusting the research methodology.

5. References

Cao, Y. (2022). Research on the governance of telecom network fraud crimes: A case study of city A (Master's thesis, Gansu University of Political Science and Law).

Cheng, Y. (2021). Research on issues related to telecom network fraud crimes (Master's thesis, Heilongjiang University).

Ding, C. (2019). Research on Cross-border Cooperation in the Investigation of Telecom Network Fraud Cases (Master's thesis, Chinese People's Public Security University).

Dong, H. (2023). Research on the problems and countermeasures of anti-telecom network fraud by Dalian public security organs (Master's thesis, Dalian Maritime University).

Du, S. (2022). Research on collaborative governance of telecom network fraud: A case study of province Z (Master's thesis, Party School of the CPC Zhejiang Provincial Committee).

Du, Y. (2018). Research on the industrial chain of black and gray internet production (Master's thesis, Zhejiang University).

Fang, K. (2022). Research on Investigation Methodology of Telecom Network Fraud Crimes (Doctoral dissertation, Zhongnan University of Economics and Law).

Huang, H. (2021). Research on the Industry Chain of Telecom Network Fraud Crimes and Countermeasures (Master's thesis, Chinese People's Public Security University).

Huang, X. (2023). Research on collaborative governance of telecom network fraud in Sichuan Province from a platform perspective (Master's thesis, University of Electronic Science and Technology of China).

Ke, M. (2020). Research on government regulation of telecom network fraud behavior: A case study of banks in Guangdong Province (Master's thesis, South China University of Technology).

Li, C. (2023). Criminal law evaluation of aiding telecom fraud cash withdrawals (Master's thesis, Liaoning University).

Li, J. (2023). Research on telecommunications industry governance for combating telecom network fraud in Shanxi Province (Master's thesis, Shanxi University).

Li, Y. (2018). Research on Investigation and Governance of New Types of Telecom Network Fraud Crimes. Chinese People's Public Security University Press.

Liu, J. (2022). Research on the Prevention and Control of Telecom Fraud Crimes by Public Security Organs in Z District (Master's thesis, Shandong University of Finance and Economics).

Liu, X. (2023). Research on Online Aiding and Abetting (Doctoral dissertation, Chinese People's Public Security University).

Shen, L. (2023). Research on the path of risk governance for community telecom network fraud: A case study of community H in Chengdu (Master's thesis, Southwestern University of Finance and Economics).

Shi, Y. (2021). Research on the dilemmas and countermeasures of telecom network fraud supervision by the communication department in H province (Master's thesis, Hunan University).

Song, G. (2020). Research on investigation countermeasures of telecom network fraud crimes: Focused on Dezhou City (Master's thesis, People's Public Security University of China).

Song, W. (2021). Research on Enhancing the Governance Capacity of Telecom Network Fraud in G City (Master's thesis, Northwest University).

Sun, G. (2020). Research on the Current Situation and Countermeasures of Telecom Network Fraud Crimes: A Case Study of Y City Public Security Organs (Master's thesis, Hebei University).

Sun, S. (2018). Research on Telecom Fraud Crimes and Their Governance (Doctoral dissertation, Zhongnan University of Economics and Law).

Teng, Y. (2022). Research on Problems and Countermeasures in the Governance of Telecom Network Fraud in the Province (Master's thesis, Jilin University).

Wang, H. (2021). Study on the effectiveness of commitment under mistaken motivation. Journal of the National Procuratorate Academy, 6.

Wang, X. (2023). Research on the dilemmas and countermeasures of grassroots public security organs in investigating telecom network fraud cases: A case study of the Z district branch of the J City Public Security Bureau (Master's thesis, Shandong Normal University).

Wang, Z. (2023). Research on the governance of cross-border telecom network fraud crimes (Master's thesis, Yunnan University of Finance and Economics).

Xi, M. (2023). Research on the risk management of QH Rural Commercial Bank accounts under the background of deregulation (Master's thesis, Shandong University of Finance and Economics).

Xu, X. (2022). Research on the problems and countermeasures of telecom fraud prevention and control by public

security organs in Quanzhou's Quangang District (Master’s thesis, Huaqiao University).

Xu, Y. (2022). Research on the regulatory issues and countermeasures of telecom fraud in Sichuan Province from a platform perspective (Master’s thesis, University of Electronic Science and Technology of China).

Yao, Y. (2023). Research on the Collaborative Governance of Black and Grey Industries Related to Telecom Network Fraud in Zhejiang Province (Master's thesis, East China University of Political Science and Law).

Zhang, Y. (2021). Research on Countermeasures for Preventing and Controlling Telecom Network Fraud in Daqing City (Master's thesis, Heilongjiang Bayi Agricultural University).

Zhang, Y. (2023). Research on the Prevention and Control of "Pig Butchering Plate" Telecom Network Fraud Crimes (Master's thesis, Zhejiang Gongshang University).