



Telecommunication Fraud in China as Basis for an Enhanced Crime Prevention Strategy

Huang Guangshun^{1,2}, Ma. Xenia Z. Bitera^{3,4}

¹Student, College of Criminology and Criminal Justice, Lyceum of the Philippines University- Batangas,

²Huainan Normal University, Huainan City, Anhui Province, China, 232038

³ Faculty, College of Criminology and Criminal Justice, Lyceum of the Philippines University-Batangas,

⁴ Center Research and Innovation, Lyceum of the Philippines University-Batangas

ABSTRACT

The crime of telecommunications fraud brings serious difficulties to the investigation as this occurs through the internet which has strong concealment and anti-reconnaissance capabilities. Only by fully understanding the root causes of telecommunications fraud crimes can effective prevention strategies be developed. This descriptive correlational study aimed to determine telecommunication fraud in China as a basis for an enhanced crime prevention strategy. Specifically, this study aimed to determine the respondents' profile, factors supporting victimization of telecommunications fraud as to precipitating and attracting factors and impacts of telecommunications fraud. Moreover, it sought to test a significant difference in responses when grouped according to profile variables and test a significant relationship between factors supporting victimization and the impacts of telecommunications fraud. The respondents were 424 telecommunications fraud victims from Huainan City, Anhui Province. The results revealed that the majority of the respondents were female, 31 to 40 years old, with bachelor's degrees, personnel from private institutions, and had participated in online false shopping. Respondents agreed that factors supporting victimization of telecommunication fraud include precipitating factors like venturing on online high-profit capital and attracting factors like trans regional or transnational telecommunications fraud is difficult to detect. Moreover, telecommunication fraud had negative impacts like increasing litigation by the victims, psychosocial impact on the victims like feeling stupid about the action, and positive impacts like the increase in the lawful crackdown against telecommunication fraud. There were significant differences in occupational and victimizing styles between Precipitating Factors and Attracting Factors, but there was no significant difference in victimizing styles among Attracting Factors. There is a high correlation between the factors that support victimization and the impact of telecommunications fraud. Based on the results of this study, an enhanced crime prevention strategy was crafted.

Keywords: telecommunication fraud, precipitating factors, attracting factors, psychosocial impact, victimization

INTRODUCTION

Telecommunications fraud is a common and rampant crime in contemporary Chinese society, which involves various aspects of people's daily lives and is caused by many factors. According to Article 2 of the Anti-Telecommunications Network Fraud Law of the People's Republic of China, telecommunications network fraud refers to the act of fraudulently obtaining public or private property through remote or non-contact means using telecommunications network technology for illegal possession [1].

Criminals often use the victims' mentality of being eager to seek employment, take out loans, and seek cheap opportunities to induce fraud, using methods such as winning lottery fraud, training fraud, and impersonating public officials to commit fraud. Telecommunications network fraud groups have a certain level of organizational, collaborative, and teamwork spirit, making it difficult for people to identify telecommunications network fraud [2]. Currently, telecommunications fraud mainly consists of 50 types: phone impersonation as a leader, acquaintance fraud, ticket refund, visa change fraud, etc. Telecommunications fraud can be divided into four types: impersonation type, inducement type, threat type, and friendship type [3]. The crime of telecommunication fraud is characterized by the fact that the suspect does not make positive contact with the victim, the technological content and means are constantly updated, the gang crime is widespread, and the degree of organization is high [4].

The Public Security Department of China has carried out multiple network clearing and card interruption actions to combat telecommunications fraud crimes. Consequently, the "Anti-Telecommunications Network Fraud Law" was promulgated and implemented on December 1, 2022. One thousand two hundred seven (1207) suspects involved in fraud in northern Myanmar were successfully handed over to China, including 41 fugitives online, which is another major result of the crackdown after 269 suspects involved in fraud in northern Myanmar were captured earlier [5]. The long-term strict crackdown on telecommunications fraud crimes has achieved great results, but telecommunications fraud crimes in China are still frequent, and the fraud methods are iterative and upgraded. In 2019, China had a total of 620000 telecommunications fraud cases, involving a huge

amount of fraud, reaching 7.3 billion yuan. From this, telecommunications fraud has a significant impact on society, seriously hindering social stability and harmonious development [6].

After suffering from telecommunications network fraud, victims fall into economic difficulties, losing funds from their savings, being forced to borrow or steal funds from their families by fraudsters, and loss of economic independence and autonomy [7]. Fraud crimes can also cause varying degrees of psychological damage to victims, with recent psychological damage manifested as irritable reactions such as anger, panic, shame, regret, and self-blame. Long-term psychological damage manifests as the imprint of being killed and the aftermath of being killed [8].

Based on the above premise, this study aims to gather data to better understand telecommunication fraud in China as a basis for an enhanced crime prevention strategy.

OBJECTIVES OF THE STUDY

This study aimed to describe telecommunication fraud in China as a basis for an enhanced crime prevention strategy. Specifically, this study aimed to present the profile of the respondent in terms of sex, gender, age, education attainment, occupation/employment, and methods of victimization of the telecommunication fraud experienced; to determine the factors supporting victimization of telecommunication fraud in terms of precipitating and attracting factors, and the impacts of telecommunication in terms of psychosocial, positive and negative legal/political impact.

METHODOLOGY

This research employed a quantitative descriptive research design in determining the telecommunication fraud in China. Descriptive research can explore multiple variables to describe people, events, or situations in their natural setting and it examines a population's characteristics, uncovers issues within a unit, organization, or population, and investigates differences in traits or practices between institutions [9].

There were 424 respondents through purposive sampling who were telecommunications fraud victims, residents of Huainan City, Anhui Province, China, and gave consent to answer the survey.

RESULTS AND DISCUSION

Table 1

Percentage Distribution of the Respondents Profile

Sex	Frequency	Percentage %
Male	149	35.1
Female	275	64.9
Age		
Under 18 years old	6	1.4
Age 18 to 30	166	39.2
Age 31 to 40	169	39.9
Age 41 to 50	75	17.7
Age 51 or older	8	1.9
Education Attainment		
Secondary (High School)	38	9.0
Bachelor Degree (undergraduate)	244	57.5
Master's degree	132	31.1
Doctoral degree or above	10	2.4
Occupation		
Student	36	8.5
Farmer	3	.7
Unemployed person	32	7.5
Professional	8	1.9
Personnel of public institutions	72	17.0
Personnel of private institutions	176	41.5
Government personnel	37	8.7
Enterprise workers	36	8.5
Individual business personnel	24	5.7
Method of Victimization of the Telecommunication Fraud Suffered		
Availed of fast loans online	44	10.4
Participated in an online false shopping	127	30.0
Participated in an online gambling	7	1.7
Participated in online investment	80	18.9
Made a friend online	18	4.2
Searched for a job online	31	7.3
Shop lottery online	10	2.4
Participating in online naked chat	2	.5
I was made to believe in a person who pretends to be my friend to borrow money	31	7.3
I was made to believe in a person who pretended to be a policeman	74	17.5

Table 1 presents the profile of respondents. In terms of sex, the number of female victims of telecommunications fraud is 275, accounting for 64.9% of the total, and the number of male victims of telecommunications fraud is 149, accounting for 35.1% of the total. When receiving fraudulent

information, the proportion of women who only recognize their identity is higher than that of men in terms of their recognition of the identity and expression of the information. Therefore, overall, women are more susceptible to telecommunications fraud [10]. The gender ratio in different types of telecommunications network fraud shows a selective characteristic. For example, men are the most deceived due to pornography and making friends. In pornographic scams, male victims account for 98%, while in dating scams, male victims account for 85%. The types of fraud with a higher number of female victims are often related to part-time jobs and promotional activities. For example, in part-time scams, female victims account for 69%, and in free delivery scams, female victims account for 56% [11].

In terms of age, the victims of telecommunications fraud show a trend of youthfulness. Data shows that there are 6 people under the age of 18, accounting for 1.4% of the total. Most of these people are in the student stage, and this group has weak security awareness, weak vigilance, immature mentality, and is more susceptible to scams such as phishing websites, Trojan horse links, and game equipment sales. There are 410 people aged between 18 and 50, accounting for 96.7% of the total, especially those aged between 18 and 40 who are the key targets of telecommunications fraud crimes. This group is currently in the stage of career selection, employment, and entrepreneurship, with both a demand for career choices and enormous pressure for employment, as well as a high passion for entrepreneurship, resulting in a large amount of funding and demand for career choices for this group. However, due to information inequality, personal information leakage, lack of social experience, bad habits, and blind choices, telecommunications fraud criminals engage in various forms of fraud against them. There are over 60 types of fraud, including investment and financial management, impersonation of public security personnel, online fraud, false recruitment, margin, and online loans (handling credit cards). There are a total of 8 victims over the age of 50, accounting for 1.9% of the total. This group of victims has a stable life, high financial freedom, and is more susceptible to financial and investment income fraud [12].

In terms of the education level of the victim group, the majority have Bachelor's degree consisting

of 244 which is 57.5%. The group with low education level is deceived due to the difficulty in identifying and distinguishing fraud information from a large amount of information, especially for some consumer fraud cases where the victim needs to possess certain financial knowledge and strong complex computing ability and cannot accurately identify fraud information [13]. However, in recent years, with the popularization of higher education in China and the improvement of technical means for telecommunications fraud criminals, as well as the classification and implementation of telecommunications fraud, the number of higher education levels affected by telecommunications fraud has increased. The criminal classification is based on the dependence of the educated group on logic, guiding them to fall into traps and successfully implement fraud. When some highly educated individuals encounter fraud and are dissuaded by police or bank staff, they ignore it, have a strong speculative mentality, and have a relatively weak sense of prevention [14].

In terms of the occupation of telecommunications fraud victims, the majority were personnel of private institutions accounting for 176 (41.5%) individuals. There are 72 personnel in public institutions, accounting for 17.0% of the total.

The respondents are mainly distributed in professions with stable income, high income, and relatively free working hours. This is the main victim of telecommunications fraud, as these individuals have fast and sufficient capital flow, free financial decision-making power, and do not have too many constraints. They are also the group with the largest demand for funds, making them vulnerable to telecommunications fraud in investment and financial management, online loans, and other aspects.

In terms of the method of victimization of telecommunication fraud, the majority of the respondents were those who participated in online false shopping accounting for 127 (30.0%) respondents. In China, there are many communication and exchange apps, and the diversion of various apps can easily lead to the leakage of personal information. The entry requirements for online brushing work are very low, making it suitable for most people with leisure time. This also provides convenience for telecommunications fraud criminals to engage in fraud. The initial motives of victims of online fraud may vary. It is generally believed that victims of card fraud often have the motivation to be greedy and

take risks to "earn quick money", which leads to being deceived [15].

This is followed by those who participated in online investment accounting 80 (18.9%). In such cases, so-called "investment" group chats and dating platforms are used to deceive the victim's trust. Subsequently, fraudsters induce the victim to open an account on a false investment platform for investment and offer rebates for the victim's small investment in the early stage. Once the victim increases their investment, they may become unable to withdraw funds. False investment and financial management-related telecommunications network fraud have a high number of cases, a large amount of money involved, and difficulty in recovering stolen goods and losses, which is the key to governance of electronic fraud crimes. The extension of criminal time and space, collusion between domestic and foreign groups, illegal leakage of personal information, oversight of telecommunications network control, and unfavorable banking and financial supervision are all the crux of the rampant nature of such crimes [16].

Thirdly, were those made to believe in a person who pretended to be a policeman accounting for 74 (17.5%) individuals. This type of fraud mainly involves fraudsters impersonating national law enforcement and judicial officials such as public security, procuratorates, and courts, claiming that the victim's identity has been impersonated or suspected of various crimes, and then enticing the victim to transfer money to the account provided by the suspect. The process is divided into three stages: 1. contacting the victim, causing panic to the victim with suspected crimes or various reasons, and then seeking solutions from them. 2. Sending false documents to victims in various ways to gain their trust. 3. Criminals will take technical measures or virus links to initiate call forwarding on the victim's phone, guiding the victim to transfer money into the designated "secure account" of the criminal [17].

Table 2
Factor Supporting Victimization of Telecommunication Fraud
in terms of Precipitating Factors

Indicators	Weighted Mean	Verbal Interpretation	Rank
1. Handling personal loans through the network.	3.07	Agree	5
2. Believing in positive reviews made by the sellers themselves.	3.07	Agree	4
3. Participating in online gambling.	3.06	Agree	6.5
4. Venturing online high-profit capital.	3.22	Agree	1
5. Making friends or dating on the Internet	3.21	Agree	2
6. Finding high-paying jobs on not legit websites.	2.92	Agree	9
7. Shopping on informal not legit websites or telephone.	3.10	Agree	3
8. Borrowing of property without verification of legal information.	2.94	Agree	8
9. Paying of property without verification of legal information.	3.06	Agree	6.5
10. Accepting cash returned from unverified shopping or winning.	2.67	Agree	10
Composite Mean	3.03	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 presents the factors supporting victimization of telecommunication fraud as to precipitating factors which were agreed by the respondents with a composite mean of 3.03. Among the indicators, venturing online high-profile capital has the highest average score of 3.22, ranked 1st. Making friends or dating on the internet has a comprehensive rating of 3.21, ranked 2nd.

People with stable incomes and a certain amount of wealth accumulation, always hope that their assets can increase in value, so they have the desire to invest and manage finances. There is another situation where victims blindly follow, which is their tendency to show off their wealth and prowess daily. When their circle of friends makes so-called investments, not participating in the investment appears to be inconsistent with their usual identity [18]. Fraud crimes have taken advantage of the development of information technology. Under the catalysis of the Internet, online fraud has not only become the main manifestation of fraud crimes but also constantly innovating under the natural barrier of the Internet. Among them, telecommunications fraud through online dating or dating, also known as pig-

killing online fraud, is a new form of online fraud that has emerged in recent years. Unlike traditional online fraud, the pig-killing plate online fraud has a strong gang nature, a long duration, and a large amount of financial fraud. While trampling on the victim's emotions, it also causes damage to the victim's property rights and seriously disrupts social security and order [19]. Online shopping fraud has maintained a high proportion among the types of online fraud suffered by netizens. From the current criminal situation, online shopping fraud crimes have characteristics such as relying on precise citizen information, relying on phishing websites or links, younger victim groups, regional professional crimes, specialization of criminal division of labor, and industrialization of criminal chains [20]. The victims of online loan fraud are mainly young and middle-aged men aged 18-40. Under fraudulent information such as low interest, high credit limit, and no guarantee, victims are generally highly motivated and have a clear tendency to seek profits. Under this psychological influence, victims' awareness of prevention decreases, not only neglecting to identify fake loan apps or websites but also quickly obtaining funds, victims will meet unreasonable requirements such as verification of repayment ability proposed by fraudsters, which leads to being deceived [21]. Commonly known as online fraud, it has become the most common form of telecommunications fraud. In terms of objective characteristics, the victims are mainly women, mostly housewives, unemployed groups, and student groups.

In addition, in terms of their environment, rural women are more likely to be deceived, and due to their possession of a large amount of family property, they may suffer significant losses once deceived. Therefore, public security organizations should strengthen their focus on promoting and educating high-risk groups in rural areas [22].

Table 3
Factor Supporting Victimization of Telecommunication Fraud
in terms of Attracting Factors

Indicators	Weighted Mean	Verbal Interpretation	Rank
1. The ways of telecommunication fraud are updated quickly.	2.61	Agree	6.5
2. There are various means of telecommunication fraud.	2.61	Agree	6.5
3. Telecommunication fraud is tightly organized and difficult to detect.	2.76	Agree	3
4. Telecommunication fraud is a low-cost and high-return crime.	2.42	Disagree	10
5. The method of Telecommunication fraud is very simple and easy to spread.	2.71	Agree	4
6. Advanced network communication technology provides convenience for telecommunication fraud.	2.63	Agree	5
7. Transregional or transnational telecommunications fraud is difficult to detect.	2.82	Agree	1
8. Anonymous and non-contact telecommunications fraud is more difficult to detect.	2.78	Agree	2
9. Inadequate protection of citizens' personal information leading to the occurrence of telecommunications fraud.	2.52	Agree	9
10. Inadequate cooperation of the telecommunications and financial sectors in the occurrence of telecommunications fraud.	2.55	Agree	8
Composite Mean	2.64	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 presents the factors supporting victimization of telecommunication fraud as to attracting factors which were agreed by the respondents with a composite mean of 2.64. The indicator 'Trans regional or transactional telecommunications fraud is difficult to detect', with an average score of 2.82, ranked 1st. Cross-regional or international telecommunications fraud is the focus and difficulty of case investigation. Therefore, establishing cross-regional, departmental, and national linkage to solve telecommunications fraud cases is an important way to effectively solve them. China has always strived to coordinate and carry out international cooperation to jointly combat telecommunications fraud.

The development of society, especially the application of artificial intelligence technology, it has brought serious challenges to the fight against telecommunications fraud. At the same time, there will be more new attracting factors that can lead to people being deceived and suffering property damage.

The crackdown on and governance of telecommunications fraud is mainly led by public security and related departments, and comprehensive governance of telecommunications fraud crimes is carried out by the law and regulations. By deploying elite police forces such as criminal police, intelligence agencies, cybersecurity, legal systems, and economic investigations, a special task force is formed to initiate joint combat mechanisms and achieve close cooperation [23]. The openness and remoteness of telecommunications fraud have built a natural protective wall for criminals, posing great obstacles to the investigation work of public security organs [24].

The indicator 'Anonymous and non-contact telecommunications fraud is more difficult to detect', with an average score of 2.78, ranked 2nd. Non-contact also brings many difficulties to the collection of criminal evidence, and the criminal evidence left behind by telecommunications fraud is generally electronic evidence, which has timeliness, limited retention time, and easy modification, all of which bring great difficulties to the investigation of cases. Some advanced devices such as synthetic voice, number changing software, big data analysis software, and artificial intelligence devices have been applied to telecommunications fraud, which has led to the increasingly intelligent and professional fraud methods of criminals, and the concealment has gradually improved [25]. On May 22, 2023, the police in Baotou City, China released a report on scammers using AI face-changing technology to commit telecommunications fraud, defrauding 4.3 million within 10 minutes.

All types of telecommunications fraud crimes have the characteristics of low capital investment, a much lower probability of being caught and dealt with than other types of criminal crimes, and huge criminal profits [26].

Table 4
Summary of Factors Supporting Victimization
of Telecommunication Fraud

Indicators	Weighted Mean	Verbal Interpretation	Rank
1. Precipitating Factors	3.03	Agree	1
2. Attracting Factors	2.64	Agree	2
Composite Mean	2.84	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

Table 4 presents the summary table of factors supporting the victimization of telecommunication fraud. The Precipitating Factors, ranked 1st, were agreed by the respondents with a weighted mean of 3.03. On the other hand, Attracting Factors, ranked 2nd, were agreed by the respondents with a weighted mean of 2.64, and a composite mean of 2.84.

Comparing these two, it can be seen that respondents have a slightly easier perception and grasp of the former, while the latter belongs to a deeper level of problem. Attracting Factors refer to the fact that victims are victims of fraud because their factors play a decisive role. There are many types of factors, and the occurrence of an event is not determined by a single factor. It is often the result of a combination of multiple factors. However, in summary, victims mainly suffer property losses due to greed for small profits and insufficient information confirmation. From the perspective of the victim, the main issue is that the victim lacks awareness of self-protection and fraud prevention.

Precipitating factors are the result of the comprehensive effects of various environmental factors in which the victim is located. If the legal system is not sound, telecommunications fraud crimes have low costs, high profits, and are easy to replicate. Compared with contract fraud, financial fraud, etc., telecommunications fraud has simple methods, a wide range of targets, and a high success rate. Once someone is deceived, the profits range from a few hundred to ten million yuan, luring many people who want to be once and for all and have weak legal awareness of the path of crime. The existing legal framework also does not clearly define the legal responsibilities that banks and telecommunications

operators should bear, resulting in weak self-discipline and weak supervision in related industries [27]. In addition, telecommunications operators, commercial banks, and other related industries are diverse and have poor communication, and a single department cannot effectively curb telecommunications fraud activities. Due to the additional benefits brought by telecommunications fraud, it is difficult for telecommunications operators commercial banks, and other related industries to choose between individual and collective conflicts of interest, and it is impossible to truly achieve linkage between all parties.

Table 5
Impacts of telecommunications fraud in terms of Psychosocial Impact to the Victims

Indicators	Weighted Mean	Verbal Interpretation	Rank
1. I experienced mental torture.	2.70	Agree	8
2. I experienced extreme disappointment with the slow processing of telecommunications fraud.	2.68	Agree	9
3. I experienced helplessness in the absence of the true information of the criminal.	2.98	Agree	2
4. I was angry with the people who did this to me.	2.92	Agree	4
5. I lost hope in recovering the virtual property.	2.88	Agree	6
6. I felt guilty for causing a financial disaster for my family.	2.90	Agree	5
7. I felt stupid for my actions.	3.01	Agree	1
8. I developed trust issues in online transactions.	2.93	Agree	3
9. I felt embarrassed by others' opinions.	2.74	Agree	7
10. I encountered personal problems due to property loss.	2.54	Agree	10
Composite Mean	2.83	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 5 mainly presents the impact and psychological activities of telecommunications fraud on victims. The composite mean of 2.83 indicates that the respondents agree with the above indicators. Among the listed projects, the overall effective indicator for "I felt stupid of the actions" ranked 1st with an average score of 3.01. This reflects the victim's sense of self-blame and guilt when

telecommunications fraud occurs. After encountering telecommunications fraud, most victims will experience the following psychological states: high internal panic, high psychological pressure, strong emotional reactions, and so on. The emotions of regret and self-blame, even not wanting to be known by others, make them ashamed to report the case, which will only make the criminals go unpunished. If the amount of money cheated is large, some victims can't bear the huge psychological pressure and even choose to commit suicide [28].

“I experienced helplessness in the absence of the true information of the criminal.” with an average score of 2.98, ranked 2nd. Non-contact is a fundamental feature of telecommunications fraud, and it is also the fundamental difficulty and inability to eradicate telecommunications fraud cases. There is no necessary causal relationship or actual contact between the criminal gangs of telecommunications fraud and the victims, and the investigation authorities are unable to determine the scope of investigation through conventional causal relationships, resulting in weak directional and targeted investigation. This is not conducive to the investigation authorities discovering clues from the social and interpersonal relationships of the victims, It is also not conducive to relatively accurate identification of the interests between criminal gangs and victims [29].

Telecommunication fraud crimes have caused a significant decrease in social trust and a lack of trust between individuals. It devours social integrity and increases the cost of social operation. The national image has been tarnished by telecommunication scammers, which has also raised doubts among Chinese and foreign citizens about the government's governance capabilities. The national image and government credibility have been questioned [30].

The impact of telecommunications fraud on victims is multifaceted, not only limited to economic losses, but also includes psychological, social, and security threats. Therefore, we should be vigilant, protect our private information, not easily trust strangers' words, and avoid being deceived.

Table 6
Impacts of telecommunications fraud in terms of Positive Impact

Indicators	Weighted Mean	Verbal Interpretation	Rank
1. Rigid government regulation by amending or enacting new laws or regulations.	2.79	Agree	2
2. Increase the crackdown against telecommunications fraud according to law.	2.83	Agree	1
3. Multi sectoral cooperation fight through joint action of public security departments, telecommunications companies and financial departments.	2.77	Agree	3
4. International cooperation through international joint action of many countries against fraud.	2.64	Agree	5
5. Increase awareness of prevention since the government carries out publicity activities on the public's awareness of security against telecommunications fraud through various channels	2.68	Agree	4
Composite Mean	2.74	Agree	

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

In terms of criminal policy, there are still many shortcomings in the crackdown on telecommunications fraud, and there is no effective containment of telecommunications fraud, mainly due to inadequate administrative supervision, inadequate legal environment, and increasingly severe information leakage [31]. To address the root cause of telecommunications network fraud, it is necessary to rely on a social governance system composed of administrative supervision mechanisms, a sound legal system, the cultivation of civic values, and a moral quality culture to formulate prevention regulations for telecommunications fraud [32].

To some extent, increasing the legal punishment for telecom fraud criminals is a strong guarantee to curb the current surge in the number of telecom fraud cases. Only by increasing the legal punishment for telecom fraud criminals and maximizing their criminal costs can we more effectively combat and punish telecommunication fraud criminals [33].

To enhance the collaborative governance capability of telecommunications fraud, it is necessary to maximize the standards and effectiveness of telecommunications fraud governance through communication, coordination, cooperation, sharing, and other means. It is necessary to clarify the relationships between government departments, enterprises and institutions, social organizations, and the public [34]. Due to the continuous strengthening of domestic crackdown efforts, telecommunications network fraud dens have shown a trend of transferring to foreign countries, especially Southeast Asian countries such as Myanmar and Laos, which have become the hardest hit areas for telecommunications network fraud dens. Faced with such a criminal situation, it is inevitable for China to cooperate fully with foreign countries.

Table 7
Impacts of telecommunications fraud in terms of Negative Impact

Indicators	Weighted Mean	Verbal Interpretation	Rank
1. Spike in crime rate as telecommunication fraud can be used to fund other criminal activities	3.04	Agree	3
2. Loss of public trust as telecommunication fraud can erode trust in government and institutions.	3.00	Agree	4
3. Increasing litigation by victims due to the belief that there is negligence by the telecommunications company.	3.18	Agree	1
4. Intensified government requirements for telecommunications companies for security management measures.	3.08	Agree	2
5. Damage the reputation of the Telecommunications companies who became victims of fraud.	2.92	Agree	5
Composite Mean	3.04	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 7 shows the impact of telecommunications fraud from a negative perspective, composite mean of 3.04. Among the listed projects, the indicator of "Increasing literacy by victims to the belief that there is diversity by the telecommunications company" ranked 1st with an evaluation score of 3.18. It can be seen that the occurrence of telecommunications fraud cases is closely related to the management issues of telecommunications operating companies. Therefore, great criticism has been

raised regarding their management level and attitude, and certain management constraints have been required. The mobile phone business has become a big cake for telecom operators, and multiple operators have spared no effort to develop their business and seize the market. However, due to poor management of their own business, a large number of phone cards have circulated in the market without real-name registration, leading to frequent telecom fraud cases. Law enforcement agencies, due to unclear attribution of mobile phone numbers suspected of committing crimes and inability to fully access the phone list of these numbers, have no authority to deal with them such as blocking, stopping, or canceling numbers, and are unable to effectively combat crime [35].

The indicator "Intensify the requirements for telecommunications companies for security management measures." ranked 2nd with an evaluation score of 3.08. This indicates that although telecommunication companies, banks, and other financial institutions are profitable entities, they also need to bear a certain degree of social responsibility and undertake relevant assistance obligations. In terms of lack of prevention and control in the telecommunications sector, they spare no effort to develop their business and seize the market for their interests but have not managed their SMS business well, resulting in a large number of phone cards circulating in the market without real-name registration. Moreover, fraudulent phone calls and SMS are constantly taking advantage of the prevention and control loopholes in the telecommunications department to commit crimes [36]. They must have supporting supervision and law enforcement agencies to intervene in order to force enterprises to comply with the law. As a competent authority, the government should assume supervisory responsibilities, improve accountability mechanisms, and promptly punish any illegal or irregular behavior, regardless of whether it has adverse consequences [37].

The indicator of a spike in prime rate communication fraud can be used to fund other critical activities, ranked 3rd with an evaluation score of 3.04. This indicates that the spillover of telecommunications fraud crimes has led to the emergence of other forms of crime. With the continuous iteration of the telecommunications fraud crime model, the relevant industry chain has become more refined, and the division of labor between upstream and downstream-related crimes has become more

professional, giving rise to professional money laundering groups that wash away the proceeds of fraud.

There has also been a clear division of labor within the groups, each performing its duties and being closely connected [38]. The upstream of telecommunications fraud, it involves multiple illegal and criminal activities such as falsifying identity documents, illegally infringing on others' privacy, illegally obtaining personal information of citizens, and using illegal channels to purchase mobile phone cards and bank cards in bulk. In the downstream of telecommunications fraud, it is also necessary to hire personnel to withdraw and transfer funds, which may involve concealing criminal proceeds or money laundering crimes.

Table 8
Summary Table on Impacts of Telecommunications Fraud

Indicators	Weighted Mean	Verbal Interpretation	Rank
1. Psychosocial Impact to the Victims	2.83	Agree	2
2. Positive Impact	2.74	Agree	3
3. Negative Impact	3.04	Agree	1
Composite Mean	2.87	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 8 examines the impact of telecommunications fraud on both victims and society. A comprehensive average score of 2.87 indicates that the respondents agree with the above indicators.

Among the listed projects, the negative evaluation score for telecommunications fraud is 3.04, ranking first. This indicates that telecommunications fraud has a significant negative impact on people, mainly manifested in a decrease in people's trust in society, the breeding of other crimes, and the serious mental and financial impact on victims. For example, the main problems in the banking industry include inconvenient access to bank information, idle bank account monitoring functions, lack of access to bank card number and branch code information, bank restrictions on machine withdrawals only, and lax management of debit card issuance, which provide convenience for telecommunications fraud crimes and are difficult to crack [39]. The catalyst for the generation of fraud crime ecology is constantly iterating, and the black and gray industry has spawned a large number of black and gray industries in five key stages: promotion, information material supply, tool material supply, technical support, and fund

settlement, forming a complex network crime ecosystem [40].

The psychological impact evaluation score of telecommunications fraud on victims is 2.83, ranking second, indicating that the impact of telecommunications fraud on victims is enormous. Telecom fraud seriously affects the legitimate rights and interests of the people, not only causing property damage to people, but also affecting their physical and mental health. A survey conducted by the European Union found that 24% of victims suffer economic losses, and 79% of telecommunications fraud victims suffer emotional pain [41].

The evaluation of the positive effect of telecommunications fraud on social management is 2.74 points, ranking third. This is a passive change, but the effectiveness has limitations, resulting in a lower ranking.

CONCLUSION

1. The key distribution groups of telecommunications fraud victims are women, those aged 31 to 40, those with bachelor's degrees, and individuals from private institutions.
2. The main ways in which victims suffer from telecommunications fraud include participating in fake online shopping, participating in online investments, and impersonating police officers.
3. From the perspective of Precipitating factors, the main factors that victims of telecommunications fraud suffer from fraud are investing in high profit online capital and making friends or dates online.
4. From the perspective of attractive factors, the main factors that victims of telecommunications fraud suffer from fraud are cross-border and domestic telecommunications fraud, as well as anonymous and non-contact telecommunications fraud.
5. The psychological impact of telecommunications fraud on victims mainly includes victims feeling foolish and blaming themselves, feeling frustrated, and feeling helpless due to a lack of true information about criminals.
6. From the perspective of positive impact, the main impact of telecommunications fraud is the

revision or promulgation of more comprehensive laws or regulations, the strengthening of government

supervision, and the increase of crackdown on telecommunications fraud in accordance with the law.

7. From the perspective of negative impacts, the main impact of telecommunications fraud is due to negligence in the management of telecommunications companies, with an increasing number of victims and lawsuits being filed. The demand for government security management measures for telecommunications companies is increasing.

RECOMMENDATIONS

Based on the conclusions, the following recommendations are offered:

1. Increase the promotion of public anti fraud knowledge and identification skills, strive to form a nationwide anti telecommunications fraud campaign, ensure that everyone is vigilant and has anti fraud awareness, and strengthen the promotion of anti fraud campaigns for women, stable and high-income individuals aged 31 to 40, and private enterprise personnel who are vulnerable to fraud. For example, the prevention of telecommunications fraud knowledge competition and the promotion of telecommunications fraud prevention into communities, schools, and other means of publicity.
2. The government, functional departments, and communities should combine real cases to understand various forms of telecommunications fraud, improve their ability to identify telecommunications fraud, and strengthen the prevention of telecommunications fraud.
3. The government and various departments of society should guide people to have a correct concept of consumption and investment in financial management, avoid the mentality of speculation and small profit taking in consumption and financial management, strengthen the promotion of online consumption and financial management traps against telecommunications fraud, and severely crack down on telecommunications network fraud such as online investment, online dating, and making friends.
4. Strengthen deep cooperation between international and domestic regions and departments, establish information collaboration platforms, achieve real-time information sharing, jointly combat telecommunications fraud crimes, and make every effort to recover the property losses of victims.
5. Utilize existing mature network communication technology to develop powerful criminal tracking and

positioning systems and fraudulent fund flow tracking systems, while strengthening the acquisition and fixation of electronic evidence, and increasing efforts to solve cases and recover fraudulent funds. Enhance the identification and interception of fraudulent information dissemination, and reduce the spread of fraudulent information.

6. While cracking down on telecommunications fraud and recovering fraudulent funds, the government and functional institutions should also provide psychological rehabilitation assistance to victims, as well as policy and economic relief, to help victims quickly overcome their emotional state and restore their normal lives.

7. The country should pay attention to legislation first, formulate specialized laws, regulations or policy documents to strengthen personal information protection, which is the condition and source of solving telecommunications fraud, increase punishment for illegal acts, and establish a sound telecommunications fraud crime prevention system.

8. The government should regulate and supervise the supervision and management of financial institutions such as telecommunications operators, networks, and banks, add additional responsibilities for telecommunications fraud cases, enhance their sense of social responsibility, encourage them to improve the management functions of key links in services, and maximize the occurrence of telecommunications fraud crimes and recover property losses caused by telecommunications fraud.

REFERENCES

- [1] The National People's Congress. (2022). Law of the People's Republic of China on Anti Telecommunications Network Fraud. The National People's Congress.44807https://baijiahao.baidu.com/s?id=1742933154387101137&wfr=spider&for=pc
- [2] Gao Shuang.(2021).The Harm and Countermeasures of Campus Loan: Based on the Consumption Perspective of College Students. Technology Economy Market.2021 (09)
- [3] Xi Dongsheng. (2022). Economic Thinking on telecommunications fraud Crime. Publication of Master's Electronic Journals at Guangxi University.2023 Issue 02 Online Publication Time: January 16, 2023- February 15, 2023. DOI: 10.27034/d.cnki.ggxix.2022.002356
- [4] Li Xinwei. (2022) .Research on the Prevention of Telecom Network Fraud Crimes: Based on the Characteristics of Victims in Gansu Province. Journal of Shanghai Public Security College.2022,

- [5] Sina Finance Headlines. (2023). Ministry of Public Security: 1207 suspect of telecom network fraud handed over to us. Sina Finance Headlines. <https://cj.sina.com.cn/articles/view/1831059072/6d23be80020016nph>
- [6] Lu Jing. (2021). Analysis of Several Difficulties and Issues in telecommunications fraud. *Legal System and Society*.2021.7 (bottom). DOI: 10.19387/j.cnki.1009-0592.2021.07.163
- [7] Cheng Xianyang & Feng Zitong. (2023). The Current Situation, Problems and Preventive Education Measures of Minors Suffering from Telecom Network Fraud. *Research on Preventing Juvenile Delinquency*.2023 (03)
- [8] Liu Bin & Fan Zijing. (2020). Process analysis of telecommunications network fraud from the perspective of victims [J]. *Journal of Zhejiang Police Academy*.2020 (2): 79-84
- [9] Sandra L Siedlecki.(2020).Understanding Descriptive Research Designs and Methods.Clinical nurse specialist *CNS* 34(1):8-12.January 2020. DOI:10.1097/NUR.0000000000000493
- [10] Jin Lei (2022). Research on the Problems and Optimization of Countermeasures in the Prevention and Control of Telecom Fraud in Hangzhou. *Master's Electronic Journal of Southwest University*. Issue 12, 2022. Online Publication Time: November 16, 2022- December 15, 2022 DOI: 10.27684/d.cnki.gxndx.2022.000406
- [11] Li Xinwei (2022). Research on the Prevention of Telecom Network Fraud Crimes - Based on the Characteristics of Victims in Gansu Province. *Journal of Shanghai Public Security College*. 2022,32 (01) DOI: 10.13643/j.cnki. issn2096-7039.2022.01.005
- [12] Liu Qiang (2021). Research on the Causes and Preventive Measures of Telecom Fraud among College Students in the Era of Big Data. *Legal Tracking*. 44256
- [13] Liu Xiaoqian (2021). Characteristics analysis and prevention strategies of telecommunications fraud victims. *Legal and Social*. 2021 (07) DOI: 10.19387/j.cnki.1009-0592.2021.03.065
- [14] Deng Yujie & Kang Mingxi (2020). The Application of Big Data in the Investigation of Telecom Fraud Cases. *Police Research*. April 2020, Issue 2
- [15] Zhuang Hua (2022), The Situation and Early Warning Measures of Online Swiping Fraud Crime, *Journal of Shanghai Police College*, Vol.32 No. 5, October.,2022. DOI: 10.13643/j.cnki.issn2096-7039.2022.05.003
- [16] He Jingqiu (2023), Governance Dilemmas and Optimization Approaches for the Prevention of Victims of Telecom Network Fraud Crimes, *Journal of People's Public Security University of China (Social Science Edition)*, Issue 4, 2023, No. 224 in total
- [17] Guo Hao (2022). The Process, Existing Sample Analysis, Grassroots Governance Paths, Network Security Technology and Applications of the Crime of Counterfeiting Public Prosecutors and Fraud 2022 (11)
- [18] Zhang Yingli (2018). Empirical Research on Telecom Fraud Crime from the Perspective of Victimology. *Journal of Zhejiang Police College*, Issue 1, 2018

- [19] Teng Baoyi (2023) Research on Social Network Intelligence Analysis of "Pig Slaying Plate" Network Fraud Crime. *Western Academic Journal*. 2023 (12) DOI: 10.16721/j.cnki.cn61-1487/c.2023.12.036
- [20] Yao Zhishuai (2020). Investigation and Research on Online Shopping Fraud Cases. *Master's Electronic Journal of People's Public Security University of China*. Issue 12, 2020. Online Publication Time: November 16, 2020- December 15, 2020 DOI: 10.27634/d.cnki.gzrgu.2020.000340
- [21-22] Liu Xinyue, Fan Chaoyun, Li Hui (2022). Characteristics and Preventive Measures of Victims of Telecom Network Fraud. *Journal of Yunnan Police Officer College*. 2022 (04)
- [23] Li Binbin (2010). I want to collect money twice for a promissory note. *People's Court Report*. 2010-06-02
- [24] Ge Lei (2012). Research on Legislative Issues of Telecom Fraud Crime. *Hebei Law*. 2012,30 (02) DOI: 10.16494/j.cnki.1002-3933.2012.02.019
- [25] Li Yongchao and Wang Li (2021). Determination of Subjective Knowledge and Serious Circumstances of the Crime of Assisting Information Network Criminal Activities. *People's Judiciary*. 2021 (35) DOI: 10.19684/j.cnki.1002-4603.2021.35.027
- [26] Miao Chen (2012). Research on the Governance of Telecom Fraud Crimes. *Master's Electronic Journal of Suzhou University*. Issue 03, 2012. Online Publication Time: February 16, 2012- March 15, 2012
- [27] Wei Shuyan & Zheng Meiling (2018). Research on the Co governance of Telecom Fraud in China from the Perspective of Collaborative Governance Theory. *Academic Exploration*. January 2018
- [28] Chen Shuting (2023). Research on the Difficulties and Countermeasures of Telecom Network Fraud Detection and Prevention from the Perspective of Victims' Psychological Characteristics. *Western Academic Journal*. Second Half of March 2023 (Total 183th Issue) DOI: 10.16721/j.cnki.cn61-1487/c.2023.06.017
- [29] Xiao Tongyu (2023). Investigation Difficulties and Countermeasures for Telecom Fraud Cases. *Network Security Technology and Applications*. Issue 1, 2023
- [30] Wei Shuyan & Zheng Meiling (2018). Research on the Joint Governance of Telecom Fraud in China from the Perspective of Collaborative Governance Theory. *Academic Exploration*. 2018 (01)
- [31] Wu Chaoping (2017). Governance of Telecom Fraud: Tackling the symptoms is more important than addressing the root cause. *Social Governance*. 2017 (01) DOI: 10.16775/j.cnki.10-1285/d.2017.01.011
- [32] Liu Yaohua & Shi Yue (2016). International legislative experience and inspiration for preventing communication information fraud. *Modern Telecommunications Technology*. 2016,46 (06)
- [33] Xu Xiaolu (2023). Research on the Prevention and Control of Telecom Fraud by the Public Security Organs in Quangang District, Quanzhou City. *Master's Electronic Journal of Huaqiao University*. Issue 04, 2023. Online Publication Time: March 16, 2023- April 15, 2023 DOI: 10.27155/d.cnki.ghqiu.2022.000380

- [34] Huang Yangbin (2021). Research on Collaborative Governance of Telecom Fraud - Taking the Airport District of Zhengzhou City as an Example. Master's Electronic Journal of Henan University of Finance and Law. 12th online publication time: 2022-11-12-2022-12-15 DOI: 10.27113/dc.cnki.ghncc.2021.000531
- [35] Zhu Chen (2020). Research on Strategies for Responding to Telecom Fraud. Economics and Law. Issue 24, 2019 (August)
- [36] Cai Zhiyan (2023). Research on Optimizing the Governance of Telecom Network Fraud - Taking Qingzhou City as an Example. Qingdao University Master's Electronic Journal. Issue 03, 2023. Online publication time: February 16, 2023
- [37] Li Peilin (2021). Difficulties in Identifying Telecom Fraud Crimes and Preventive Measures. Legal and Social Issues. February 2021 (Part 1)
- [38] Liu Zhichao (2023). Legal Application Issues on the Crime of Assisting in Information Network Criminal Activities and the Offences of Covering up or Concealing Crimes Volume 6, 2023, Shanghai Legal Research Collection. DOI: 10.26914/c.cnkihy.2023.016819
- [39] Han Zhaoyong & Han Long (2012). Reflections on Places for Interrogation of Duty Crimes. Legal and Social Issues. 2012 (35) DOI: 10.19387/j.cnki.1009-0592.2012.35.138
- [40] Yu Haisong (2021) The Pattern and Regulation of the Black and Grey Industrial Chain of Cybercrime ", published in the Journal of the National Institute of Prosecutors, 2021, Issue 1.
- [41] BIJWAARD D(2021). Survey on "scams and fraud experienced by consumers" -final report[J/OL].(2020-01-28)[2022-10-19].<http://policycommons.net/artifacts/2135251/survey-on-scams-and-fraud-experienced-by-consumers/2890549/>.