Elder Law
2025, VOL. 9, NO. 2, 42-47
DOI: 10.47297/wspelWSP2515-824409.20250902

# Research on the Optimization of Criminal Law Responses to Cyber Fraud Against the Elderly

Yuchan Luo

Xinjiang University of Finance & Economics, Urumqi, Xinjiang, 830000, China

**ABSTRACT**
With the accelerated aging of China's population and its deep integration with digital transformation, cyber fraud targeting the elderly is exhibiting increasingly technical, scenario-specific, and systematic criminal chains. This phenomenon severely infringes upon the property rights of older adults and undermines social stability. Although the existing criminal law system provides a foundational regulatory framework through charges such as fraud and the crime of infringing on citizens' personal information, supplemented by specific judicial interpretations, deficiencies remain. These shortcomings are evident in the appropriateness of charges, the precision of sentencing, procedural safeguards, and the effectiveness of asset recovery. Building upon existing research and judicial practice, this paper explores optimized pathways for the criminal law response to elder-oriented cyber fraud. The analysis proceeds from four dimensions: refining the system of criminal charges, optimizing sentencing mechanisms, strengthening procedural protections, and constructing a collaborative governance model between administrative and criminal law. The aim is to provide legal support for safeguarding the legitimate rights and interests of the elderly and advancing the national strategy for actively addressing population aging.

**KEYWORDS**
Elderly; Cyber fraud; Criminal law countermeasures; Sentencing optimization

## 1 Introduction

The dual context of population aging and digital transformation has positioned the elderly as primary targets of cyber fraud. Characteristics such as insufficient information discrimination ability due to the digital divide and strong needs for emotional companionship make older adults particularly vulnerable to exploitation by fraudsters. Criminal methods have evolved from traditional telecom fraud to upgraded models including AI face-swapping impersonation, private domain social marketing, and pension investment scams, forming a complete criminal chain covering information acquisition, precision targeting, and fund transfer. Such crimes not only cause property losses for the elderly but also trigger a series of social issues, including intensified family conflicts and mental anxiety among older adults, posing severe challenges to social governance.

As a crucial means of social governance, criminal justice plays a central role in combating cyber fraud against the elderly. In recent years, China has intensified its crackdown efforts through initiatives such as special campaigns targeting pension fraud and the issuance of relevant judicial interpretations. However, judicial practice still faces challenges including ambiguous application of charges, inconsistent sentencing standards, and insufficient procedural protections. Existing academic research has discussed various aspects of elder fraud, including the setup of criminal charges, sentencing circumstances, and procedural safeguards, forming diverse perspectives such as establishing independent offenses, refining sentencing standards, and strengthening source governance. Building on this foundation, this paper integrates existing research findings and judicial practical experience to systematically analyze the difficulties in the criminal law regulation of cyber fraud targeting the elderly. It proposes targeted optimization suggestions, aiming to improve the criminal law response system and achieve comprehensive protection of the rights and interests of the elderly.

## 2 Behavioral Characteristics and Current Status of Criminal Law Regulation Regarding Cyber Fraud Against the Elderly

### 2.1 Behavioral Characteristics of Cyber Fraud Against the Elderly

Cyber fraud targeting the elderly exhibits distinct contemporary characteristics, setting it significantly apart from traditional fraud.

At the technological application level, perpetrators widely employ digital technologies such as AI face-swapping and voice synthesis to impersonate the elderly's relatives, friends, or public officials. The deception is enhanced through the forgery of identity documents and transaction records, making it difficult for the elderly to identify the scams based on

* **Corresponding Author:** Yuchan Luo, 995022899@qq.com

traditional experience.

At the scenario design level, fraudulent activities are closely tailored around the core needs of the elderly. Characteristic scenarios have emerged, including "pension investments," "integrated medical and elderly care," and "health supplements or miracle drugs." These schemes exploit the elderly's urgent demands for health and old-age care, coupled with their general lack of financial knowledge, by luring them with false promises such as "high returns, low risk" and "cures for all diseases."

At the criminal structure level, cyber fraud against the elderly has evolved into a specialized criminal chain. The upstream segment involves illegally collecting seniors' personal information—including names, addresses, and health status—through methods like "free health checks" or "gift giveaways." The midstream segment involves precisely delivering fraudulent information via methods such as phone bombardment and private community marketing. The downstream segment focuses on transferring illicit proceeds through "money-laundering platforms" and layered bank transfers, utilizing logistics and payment platforms to complete the criminal loop. Furthermore, these fraudulent activities demonstrate cross-regional and concealed characteristics. Criminal groups often employ fake identities for registration or operate from overseas to evade crackdowns, posing significant challenges for case investigation and evidence collection.

### 2.2 Current Criminal Law Regulation of Cyber Fraud Against the Elderly

China's current criminal law has established a fundamental regulatory framework for combating cyber fraud against the elderly by integrating its system of criminal offenses, judicial interpretations, and special campaigns.

Regarding the application of criminal charges, conviction and punishment are primarily based on offenses such as Fraud under Article 266 of the Criminal Law, Illegal Absorption of Public Deposits under Article 176, and Fund-raising Fraud under Article 192. To target the information acquisition phase of the fraud chain, the crime of Infringement of Citizens' Personal Information under Article 253-1 is applied. For the fund transfer and technical support phases, the crime of Aiding Information Network Criminal Activities under Article 287-2 is utilized, forming a comprehensive crackdown on the core crimes as well as upstream and downstream offenses.

At the level of judicial interpretation, the "Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Specific Application of Law in the Handling of Criminal Fraud Cases" explicitly lists "defrauding the elderly of their property" as a discretionary circumstance for imposing a heavier punishment, providing a basis for differentiated sentencing in judicial practice.

Regarding specialized governance, the nationwide campaign to combat and rectify pension fraud has intensified the crackdown on elder fraud through measures like "speedy arrest and prosecution" and the "Card Break Action," creating a high-pressure stance of criminal enforcement. Simultaneously, the enactment of laws such as the "Personal Information Protection Law" and the "Anti-Telecom and Online Fraud Law" interfaces with the Criminal Law, constructing a multi-dimensional legal regulatory system.

## 3 Practical Dilemmas in the Criminal Law Response to Cyber Fraud Against the Elderly

### 3.1 Ambiguity and Limitations in the Application of Charges

The existing system of criminal charges faces a dual dilemma of ambiguous characterization and inadequate regulation when addressing cyber fraud targeting the elderly. On the one hand, the legal characterization of certain new types of online fraudulent activities is contentious. For instance, in cases of "long-distance health product fraud" targeting the elderly, where perpetrators sell unapproved products through live streaming and false advertising, the conduct may constitute either the crime of fraud or the crime of producing and selling fake or substandard products. The significant differences in the applicable standards and sentencing ranges for these different charges lead to inconsistent adjudication standards in judicial practice.

On the other hand, existing charges struggle to comprehensively assess the social harm of some complex fraudulent schemes. For example, "pension investment" fraud often exhibits dual characteristics of both illegal absorption of public deposits and fraud. Conviction under a single charge may result in an imbalance between the crime and the punishment.

Furthermore, existing charges pay insufficient attention to the technical specificities of cyber fraud. The perpetration of elder cyber fraud heavily relies on technological support. Fraudsters use methods like setting up fake websites, developing fraudulent apps, and leveraging social media for traffic diversion to scale their operations. However, the regulatory provisions in the Criminal Law targeting technological means are relatively general, and the standards for establishing the liability of technology providers are unclear, making it difficult to effectively hold certain accomplices accountable.

Simultaneously, regarding the personal information leakage underlying "precise fraud," although the crime of infringing on citizens' personal information explicitly includes the personal information of the elderly within its protective

scope, the definition of "citizens' personal information" remains disputed in practice. The protection for sensitive information such as location tracks and health status is insufficient.

### 3.2 Difficulties in the Application of Sentencing Rules

The unreasonable application of sentencing rules is a prominent issue in the current criminal law response to elder cyber fraud. Firstly, the singular sentencing standard, primarily based on the amount involved, fails to reflect the particularities of defrauding the elderly. The elderly have a far lower capacity to withstand property losses compared to the general population. Fraud involving the same amount causes more severe life impacts and psychological harm to the elderly. Although judicial interpretations list "defrauding the elderly of their property" as a discretionary circumstance for heavier punishment, the application of this circumstance lacks clear operational standards. In practice, this leads to inconsistent application and insignificant increases in punishment, making it difficult to realize the principle of proportionality between crime and punishment.

Secondly, the consideration of sentencing circumstances is insufficiently comprehensive. The social harm of elder cyber fraud extends beyond property loss to include non-material damages such as harm to the physical and mental health of the elderly and the disruption of family relationships. However, current sentencing practices inadequately consider these factors, resulting in sentences that fail to fully reflect the overall social harm of the criminal conduct. Furthermore, there is a lack of specific provisions distinguishing principals and accessories within fraud rings, or recognizing circumstances like voluntary surrender and meritorious service, tailored to elder cyber fraud, which affects the fairness and reasonableness of sentencing.

Finally, the connection between restitution and sentencing is not tight enough. Recovery of illicit proceeds and restitution is the core demand of victims in elder cyber fraud cases. However, in practice, the connection between the actual restitution made and the sentence imposed is often weak. Some fraudsters, despite having the ability to make restitution, refuse to do so, yet courts do not sufficiently consider their attitude towards restitution during sentencing. Concurrently, the rapid transfer of funds in cyber fraud and the dispersal of involved accounts make recovering losses particularly challenging. Even if a court orders restitution, enforcement is often difficult, leaving the property losses of the elderly inadequately compensated.

### 3.3 Insufficient Tailoring of Procedural Safeguards

Criminal procedures exhibit numerous shortcomings in protecting the rights and interests of the elderly, failing to adapt to their special needs. During the evidence collection stage, due to memory decline and limited expressive ability, elderly individuals often struggle to clearly state the facts of the case. If investigators use traditional evidence collection methods, key evidence might be overlooked. Moreover, some elderly face mobility issues or live in remote areas, and remote evidence collection mechanisms are not yet widely implemented, leading to inefficient evidence collection and challenges in ensuring its validity.

During trial, elderly witnesses encounter many difficulties. Complex court procedures and specialized legal terminology may prevent them from fully expressing their views, impairing the exercise of their procedural rights.

Insufficient procedural safeguards are also evident in rights notification and relief. The elderly generally have relatively limited legal knowledge and understanding of their rights and obligations in criminal proceedings. Notifications of rights by judicial organs are often overly formalistic and fail to use easily understandable language, resulting in the elderly being unable to effectively exercise procedural rights such as the right to defend and the right to appeal.

Furthermore, judicial assistance mechanisms for elderly victims after being defrauded are imperfect. Some elderly, plunged into financial hardship due to their losses, struggle to obtain timely state judicial assistance or social support. Procedural justice fails to extend to the relief of their substantive rights.

### 3.4 Weakened Preventive Function of Criminal Law

The preventive function of criminal law has not been fully realized in combating elder cyber fraud, mainly evident in two aspects. On one hand, the effectiveness of special prevention is limited. Cyber fraud rings are often highly organized and possess strong anti-investigation capabilities. Some offenders, even after receiving criminal punishment, may exploit the anonymity of the internet to re-offend. Existing penal measures have a limited deterrent effect on their risk of recidivism.

On the other hand, the coverage of general prevention is insufficient. Although specialized crackdown campaigns have had some deterrent effect, legal education targeting the elderly lacks specificity and effectiveness. Traditional "street stall" explanations often fail to help the elderly truly understand the tactics of online fraud. Furthermore, criminal law publicity tends to emphasize the severity of punishment, failing to effectively guide the elderly in developing risk

prevention awareness.

Additionally, a coordinated prevention mechanism integrating criminal law with other legal branches has not been established. Effectively governing elder cyber fraud requires seamless coordination between criminal law, administrative law, and civil/commercial law. However, in practice, there is a tendency to "emphasize criminal crackdowns over administrative supervision." Administrative agencies' inadequate regulation of online platforms, the health product market, and financial services allows fraudulent activities to persist unchecked at the source. Simultaneously, the integration of criminal law with social governance measures is weak. The roles of communities, families, and social organizations in preventing elder cyber fraud are not fully utilized, resulting in a governance pattern where "the judiciary fights alone."

## 4 Optimization Pathways for Criminal Law Responses to Elderly-Oriented Cyber Fraud

### 4.1 Improving the System for Applying Criminal Charges and Clarifying Regulatory Boundaries

Aiming at the behavioral characteristics of elderly-oriented cyber fraud, it is necessary to further improve the system for applying criminal charges to achieve precise regulation. First, clear standards for characterizing new types of online fraudulent activities must be established. For typical fraud types such as "pension/healthcare scams" and "social security agency services scams," the distinctions between the crime of fraud and related offenses should be clarified through judicial interpretations or guiding cases to avoid characterization disputes in judicial practice. For example, for fraud conducted in the name of selling health products: if the primary purpose is illegal possession, involving fabricating product efficacy to cheat people out of property, it should be recognized as the crime of fraud; if the products have quality issues but still possess some use value, and the emphasis is on misleading consumption through false advertising, it may be characterized as the crime of producing or selling fake or substandard products or the crime of false advertising.

Second, the regulation of technological assistance behaviors in cyber fraud must be strengthened. Regarding the criminal liability of technology providers in cyber fraud, the application standards for the crime of aiding information network criminal activities should be clarified. Acts specifically dedicated to elderly cyber fraud, such as developing fraudulent software, setting up fake platforms, or providing precise information push services, should be brought within the scope of this crime. The criteria for determining "serious circumstances" should be defined to ensure effective accountability for technical assistance behaviors. Simultaneously, the judicial application of the crime of infringing on citizens' personal information should be improved. Information such as the health status, property information, and location tracks of the elderly should be classified as sensitive personal information, raising the protection level for such information and severely cracking down on the illegal acquisition and sale of elderly individuals' personal information.

Finally, rules for handling concurrence of offenses should be explored. For elderly cyber fraud behaviors that simultaneously constitute multiple crimes, the applicable situations for conviction and punishment based on the heavier offense or cumulative punishment for multiple offenses should be clarified, ensuring that the punishment corresponds to the social harm of the criminal act. For example, for "pension investment" fraud that involves both the act of illegally absorbing public deposits and the purpose of illegal possession, the crime of fund-raising fraud or cumulative punishment for multiple offenses should be chosen based on the specific circumstances to fully evaluate its dual infringement of financial order and citizens' property rights.

### 4.2 Optimizing Sentencing Rules to Achieve Proportionality between Crime and Punishment

Constructing a scientific and reasonable system of sentencing rules is key to achieving proportionality between crime and punishment for elderly cyber fraud. First, the application standards for discretionary circumstances warranting heavier punishment need refinement. Regarding the discretionary circumstance of "defrauding the elderly of their property," judicial interpretations should clarify its application conditions, incorporating factors such as the victim's age, health status, extent of property loss, and the egregiousness of the fraudulent methods. Specific ranges for increasing punishment should be formulated to ensure uniformity and fairness in sentencing. For example, for acts of defrauding special groups such as solitary elderly or seriously ill elderly, higher sentencing enhancement ranges could be stipulated; for fraud employing methods such as forging the identity of public officials or exploiting the trust of acquaintances, these should also be considered as factors for heavier punishment.

Second, the scope of considerations for sentencing circumstances must be improved. During sentencing, attention should not only be paid to the amount involved but also full consideration should be given to non-material harms caused by the fraudulent act, such as damage to the physical and mental health of the elderly and the disruption of family relationships. The degree of the victim's psychological harm and whether they have been plunged into life difficulties due to the fraud should be important references in sentencing. Simultaneously, the connection between restitution and sentencing should be strengthened. Factors such as the amount of restitution, the timeliness of restitution, and the

degree of victim forgiveness should be incorporated as sentencing circumstances. Offenders who actively make restitution and obtain victim forgiveness may receive lighter punishment according to law, whereas those who do not should face heavier penalties according to law, thereby incentivizing offenders to proactively make restitution and safeguarding the property rights of the elderly.

Finally, a differentiated sentencing guidance mechanism should be established. Specialized sentencing guidelines should be formulated for different types of elderly cyber fraud. For example, for "emotional companionship" fraud, considering its more severe psychological harm to the elderly, a relatively heavier sentencing benchmark could be stipulated; for "pension investment" fraud, combined with its degree of disruption to financial order, factors such as the number of people involved and the scale of funds should be comprehensively considered to determine the sentencing range, ensuring precision in sentencing.

### 4.3 Strengthening Procedural Safeguards and Demonstrating Judicial Humanistic Care

In the trial, convenient measures for elderly witnesses to testify should be improved, allowing elderly individuals to testify via remote video. Court procedures should be simplified, avoiding unnecessary repeated questioning of elderly individuals; during the cross-examination process, judges should appropriately guide the parties to focus their debates on the core facts and afford full respect to the statements of the elderly. Simultaneously, the protection of the elderly's litigation rights must be strengthened. When judicial organs serve legal documents and inform about rights and obligations, they should use a combination of written and oral methods to ensure elderly individuals fully understand their litigation rights; for elderly individuals without appointed defenders, legal aid should be provided, assigning professional lawyers to defend them and guaranteeing the effective exercise of their right to defense.

At the level of rights relief, the linkage mechanism between judicial assistance and social assistance should be improved. For elderly individuals plunged into life difficulties due to fraud, judicial organs should proactively initiate state judicial assistance procedures and disburse assistance funds promptly; simultaneously, collaboration with departments such as civil affairs and communities should be strengthened to provide follow-up support for the elderly, including life assistance and psychological counseling, helping them return to normal life. A restitution enforcement tracking mechanism should be established, with dedicated personnel from the court's enforcement department responsible for enforcing restitution orders in elderly cyber fraud cases. Cooperation with banks and financial institutions should be strengthened to promptly freeze and transfer involved funds, ensuring the effective enforcement of restitution judgments.

### 4.4 Constructing a Multi-dimensional Collaborative Governance System to Leverage the Preventive Function of Criminal Law

The effective governance of elderly cyber fraud requires building a multi-dimensional collaborative governance system integrating "criminal enforcement, administrative supervision, and social prevention" to fully leverage the preventive function of criminal law. At the level of criminal policy, specialized enforcement campaigns should be regularized, maintaining a high-pressure stance against elderly cyber fraud. Simultaneously, the criminal policy of "tempering justice with mercy" should be upheld. Principal offenders and key members of fraud rings should be severely punished according to law, while first-time offenders, occasional offenders, and those who actively make restitution may receive lighter punishment according to law, achieving an organic unity between special prevention and general prevention.

At the level of administrative supervision, the connection between criminal law and administrative law should be strengthened. Market regulatory, financial regulatory, and cyberspace administration departments should be urged to fulfill their supervisory duties, strengthening daily oversight of online platforms, the health product market, and financial institutions. Illegal activities such as false advertising and illegal collection of personal information should be promptly investigated and dealt with to curb fraudulent activities at the source. For clues discovered during administrative supervision that are suspected of constituting criminal offenses, a rapid transfer mechanism should be established to ensure a seamless connection between administrative violations and criminal crimes.

At the level of social prevention, the targeting of criminal law publicity and legal education should be strengthened. Judicial organs should collaborate with communities, universities for the elderly, and other institutions, using methods easily accepted by the elderly such as case exhibitions, scenario simulations, and explanations in dialect to expose common tactics of cyber fraud and prevention techniques; using online platforms to release anti-fraud short videos, public service announcements, and other content to improve the risk prevention awareness of the elderly. Simultaneously, the preventive role of families and communities should be leveraged. Children should be encouraged to strengthen communication with elderly family members, helping the elderly improve their digital literacy; community

grid workers and police officers should regularly visit elderly households to promptly identify and prevent fraudulent activities.

## 5 Conclusion

The criminal law response to cyber fraud targeting the elderly constitutes a crucial component of the national strategy for actively addressing population aging and is an essential requirement for criminal justice to achieve substantive justice. Currently, China's criminal law system has established a fundamental regulatory framework for combating such fraud; however, deficiencies persist in areas such as the appropriateness of charges, the precision of sentencing, and procedural safeguards, making it difficult to fully meet the governance demands posed by emerging fraudulent schemes.

Enhancing the targeting and effectiveness of the criminal law response can be achieved by refining the system of criminal charges to enable accurate characterization, optimizing sentencing mechanisms to reflect substantive justice, strengthening procedural safeguards to improve relief pathways, and establishing coordinated administrative-criminal governance to reinforce source prevention and control.

Addressing cyber fraud against the elderly through criminal law requires not only leveraging its punitive function but also emphasizing the realization of its protective and preventive roles. While combating crime, full consideration must be given to the unique physiological and psychological characteristics of the elderly. Through differentiated legal regulation and humanistic, the unity of legal and social effects can be achieved. Moving forward, continuous attention must be paid to new trends and features of elderly-oriented cyber fraud. In conjunction with developments in digital technology and the demands of social governance, the criminal law response system should be continually refined to provide a solid legal safeguard for the elderly's peaceful enjoyment of their later years.

## About the Author

Yuchan Luo, currently pursuing a postgraduate degree, Research Focus: Criminal Law.

## References

[1] Xu F ,Liu A ,Li X . Victimization mechanisms and countermeasures in telecom network fraud: a dual-system theoretical perspective[J].Frontiers in Psychology,2025,161637935-1637935.

[2] Suzuki A , Shikata K , Shimada T. Patterns and predictors of cyber fraud victimization: Testing routine activity theory and general theory of crime in Japan[J].Journal of Economic Criminology,2025,9100186-100186.

[3] Lazarus S , Tickner P , McGuire R M. Cybercrime against senior citizens: exploring ageism, ideal victimhood, and the pivotal role of socioeconomics[J].Security Journal,2025,38(1):42-42.

[4] Lyu C, Gao S , Zhang Q. The impact of time pressure and type of fraud on susceptibility to online fraud[J]. Frontiers in Psychology, 2025, 161508363-1508363.

[5] Wang D, Duan Y ,Jin Y. Navigating online perils: Socioeconomic status, online activity lifestyles, and online fraud targeting and victimization of old adults in China[J]. Computers in Human Behavior,2025,162108458-108458.

[6] Jia J. The Empirical Research on the Identification of Telecommunication Network Fraud Crime[J].International Journal of Social Science and Education Research,2024,7(10):205-213.

[7] Ma X. Research on the Problem of Network Fraud Crime in the Era of Big Data—Taking "Killing Pig Plate" Type Network Dating Software as an Example[J].Journal of Humanities, Arts and Social Science,2024,8(3):55-58.