

A Study on the Collaborative Governance of Electronic Payment Security for Older Adults

Heping Yang*

People's Public Security University of China, Beijing, China

**Author to whom correspondence should be addressed.*

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

Abstract: With the deepening of population aging and the rapid proliferation of electronic payment technologies, older adults have gradually become an important participant group in the digital payment system. While electronic payments have improved transaction efficiency and facilitated daily life, older adults face multiple security risks in the process of use due to their relatively limited digital capabilities, weak risk-identification abilities, complex platform operating rules, and unequal access to digital support from family members. These risks include fraud inducement, unintended charges caused by operational errors, personal information leakage, account theft, and even being coerced by criminals into becoming involved in illegal and criminal activities. Consequently, the security of electronic payments for older adults is no longer limited to technical risk prevention and control; rather, it has evolved into a comprehensive governance issue requiring the joint participation of multiple actors, including public security authorities, banks, payment platforms, families, communities, and society at large. To address these challenges, this study proposes that public security authorities should play a central coordinating and driving role in further promoting the development of cross-departmental data-sharing and coordinated response mechanisms. It is also necessary to improve the institutional design and age-friendly service standards for the security of electronic payments used by older adults, while strengthening the risk-identification, human-intervention, and emergency payment-suspension capabilities of banks and payment platforms. These measures can effectively enhance the systemic, coordinated, and practical effectiveness of electronic payment security governance for older adults, thereby better safeguarding their property security, information security, and legitimate rights and interests in the digital society.

Keywords: Elderly people; Electronic payment security; Collaborative governance

Online publication: August 14, 2026

1. Research background

With the deepening of population aging and the rapid proliferation of electronic payment technologies, older adults have gradually become an important participant group in the digital payment system. While electronic payments have improved transaction efficiency and facilitated daily life, older adults face multiple security

risks in the process of use due to their relatively limited digital capabilities, weak risk-identification abilities, complex platform operating rules, and unequal access to digital support from family members. These risks include fraud inducement, unintended charges caused by operational errors, personal information leakage, account theft, and even being coerced by criminals into becoming involved in illegal and criminal activities ^[1]. Consequently, the security of electronic payments for older adults is no longer limited to technical risk prevention and control; rather, it has evolved into a comprehensive governance issue requiring the joint participation of multiple actors, including public security authorities, banks, payment platforms, families, communities, and society at large.

To address these challenges, public security authorities should play a central coordinating and driving role in further promoting the development of cross-departmental data-sharing and coordinated response mechanisms, improving the institutional design and age-friendly service standards for electronic payment security among older adults, strengthening the risk-identification, human-intervention, and emergency payment-suspension capabilities of banks and payment platforms, and establishing a regular protection system involving families, communities, financial institutions, and digital platforms.

2. Current security risks in electronic payments used by older adults

2.1. Erroneous operations resulting in financial losses

With the development of technology, certain emerging products and services have made daily life more convenient while also generating negative effects for older adults as a special user group. Functions such as “buy now, pay later,” “continuous subscription,” and “password-free payment” have greatly facilitated and simplified the electronic payment process. However, their effects on older adults may differ significantly from those on younger users.

The personal characteristics of older adults may themselves affect the security of electronic payments. Take the “buy now, pay later” function as an example. Some older adults do not actively choose this option when purchasing goods. Instead, the function may be recommended by default on the payment page or activated inadvertently through an accidental click. Some platforms may even modify the default payment method or weaken or conceal the “add to cart” option on certain product pages. As a result, an item that a user originally intended merely to save or add to a shopping cart may instead be ordered directly.

2.2. Separation between users and devices damaging the payment security rights and interests of older adults

Another important factor affecting the payment security of older adults is the separation between users and their electronic devices. Older adults’ mobile phones are often used by their grandchildren for entertainment, while other family members may also operate their electronic devices. Consequently, cases in which the electronic payment security and rights of older adults are compromised are relatively common.

For example, an 11-year-old girl in Chashan Town, Dongguan, Guangdong Province, used her grandmother’s mobile phone to purchase a gaming account online and was defrauded of RMB 180,000. In addition to the risks arising when grandchildren use older adults’ mobile phones, adult children may also damage older adults’ electronic payment rights and interests through unauthorized use of their devices ^[2].

According to a typical case of cybercrime released by the Supreme People’s Court, Luo Luhua was the daughter-in-law of Ye Daijin and a person identified as Chi. Because she lacked money for online shopping

and was addicted to the game Honor of Kings, she privately linked a China Industrial and Commercial Bank bank card held in Chi's name to her own mobile phone number and activated online banking. She subsequently transferred money deposited by her parents-in-law from grain sales into her own private account. At the time the case was uncovered, a total of RMB 100,202.98 held in 12 bank cards belonging to Chi had been entirely spent by Luo Luhua, who was unable to repay the money.

Thus, the operation of older adults' electronic payment devices by relatives due to the separation between the device owner and the actual operator is also an important factor that seriously affects the security of electronic payments for older adults.

2.3. Older adults being induced to participate in money-laundering crimes

Money laundering is one of the primary areas affecting the security of electronic payments for older adults. Many risks involving older adults' electronic payment security are closely associated with money-laundering activities. As a special social group, older adults may be targeted by criminals because they are less likely to attract attention in everyday life and their financial transfers may receive less scrutiny^[3].

The use of older adults in money-laundering activities has gradually emerged as a growing trend. Criminal suspects take advantage of older adults' unfamiliarity with electronic technologies, limited understanding of mobile applications, and tendency to trust others, thereby inducing them to participate in illegal and criminal activities.

A short video released by the Beijing Daily-affiliated Beiqing Community Media in its Fangshan edition reported that Beijing police had arrested a man surnamed Liu. In a small 20-square-meter room in a residential community in Fangshan, dozens of older adults were crowded together and collectively operating mobile phones. These older adults had been deceived into helping process illegal funds through fictitious "transaction-flow" activities designed to launder money. The suspect claimed that participants could receive RMB 2.79 million in poverty-alleviation pensions free of charge, without paying any fees, and used the promise of free food and accommodation throughout the day as an inducement. He conducted illegal activities in the Changyang Central City residential community and deceived older adults into downloading an application called "Rural Revitalization." The bank cards of older adults were subsequently used to facilitate crimes involving assistance to cybercriminal activities.

2.4. Older adults becoming victims of telecommunications and online fraud

The term "pig-butcher scams targeting older adults" has become increasingly common in recent years. Telecommunications and online fraud is one of the major forms of illegal and criminal activity threatening the security of electronic payments for older adults.

Because fraudsters carefully design and package their schemes, telecommunications and online fraud targeting older adults is generally not significantly affected by the victims' educational backgrounds. Different groups of older adults may be targeted through different scripts, inducement techniques, and behavioral patterns characteristic of "pig-butcher" scams.

2.5. Electronic payment devices of older adults being used for illegal and criminal activities

Without their knowledge, older adults may have their electronic devices used by third parties to steal or transfer property through the repair, purchase, or sale of such devices^[4]. Older adults' lack of knowledge

and familiarity with electronic equipment may provide opportunities for criminals to exploit. For example, criminals may obtain control over an older adult's mobile phone under the pretext of repairing the device.

2.6. Older adults being victimized by online livestreaming fraud

With the widespread adoption of livestreaming technologies, combined with the relatively weak ability of some older adults to distinguish between genuine and fraudulent information, livestreaming fraud has become an emerging risk to their electronic payment security.

A case published by CNR News on January 5, 2025, reported that some livestreaming rooms sold large quantities of counterfeit antiques, jade, and other goods. By using attention-grabbing expressions such as “finding a bargain,” “investment appreciation,” and “high-price repurchase,” together with persuasive marketing scripts, these livestreaming rooms created an atmosphere suggesting that certain items were “rarely available” or “unique jade pieces” in order to attract older adults to make purchases. Some older adults even incurred substantial debt in order to purchase goods promoted in livestreaming rooms.

3. Analysis of the causes of electronic payment security risks among older adults

3.1. Insufficient leadership by public security authorities

The core responsibilities of public security authorities are to combat crime and maintain public safety. Faced with complex and extensive public security tasks, police resources have long been under considerable pressure. Relatively limited allocation of resources and police personnel to the security of electronic payments used by older adults has resulted in insufficient personnel for early warning, public education, and rapid response, thereby restricting the capacity for proactive prevention and control.

From the perspective of public security publicity methods, traditional approaches tend to rely more heavily on offline activities, while online education targeting older adults remains relatively limited ^[5]. As a result, public security authorities have not yet fully assumed a leading role in establishing and strengthening the first line of defense for the security of electronic payments used by older adults.

In addition, the “two teams and one office” structure of grassroots public security organs has not fully realized its potential. Community policing officers often attach insufficient importance to the electronic payment security of older adults, resulting in inadequate effectiveness of routine public education and prevention efforts.

3.2. Operational barriers faced by older adults

From the perspective of cognitive capacity, older adults generally experience physiological changes such as declining short-term memory and a reduced ability to process multiple tasks simultaneously. Consequently, when confronted with complex payment procedures, such as multiple authentication steps and dynamic password entry, they have significantly higher rates of operational errors than younger users. These deficiencies in understanding electronic payment procedures seriously affect their payment security.

At the level of human-computer interaction, the interface design of mainstream payment platforms has not fully considered the decline in visual, tactile, and other sensory functions commonly experienced by older users. Problems such as excessively small fonts, densely arranged functional buttons, and inconspicuous prompts may result in insufficient comprehension during the operation process.

It is worth noting that such operational barriers may produce a negative feedback loop. Initial

operational errors can trigger older adults' doubts and concerns about their own abilities, thereby reducing their willingness to use electronic payment methods and creating a vicious cycle of "unable to use—attempting to use—making operational errors—abandoning use."

3.3. Inadequate banking procedures for protecting the rights and interests of older adults

In the protection of electronic payment security for older adults, cumbersome banking remedies constitute a prominent practical problem. After experiencing abnormal deductions, fraudulent transfers, or unauthorized withdrawals from their accounts, older adults often need to repeatedly communicate with bank branches, customer service hotlines, mobile banking platforms, and public security authorities. The dispersion of complaint and remedy channels and the lack of clear procedural guidance can result in excessively high costs for protecting their rights and interests.

At the same time, banks often require various materials, including transaction records, chat histories, and police report receipts. However, older adults generally have limited capacity to preserve electronic evidence and may therefore be unable to provide complete documentation in a timely manner.

Insufficient human review and intervention also constitute an important manifestation of deficiencies in banking protection procedures^[6]. At present, banks rely heavily on system models and automated review mechanisms to identify electronic payment risks. Although such mechanisms improve processing efficiency, their ability to identify risks specifically associated with older adults remains limited.

3.4. Insufficient social support

Existing policies and regulations provide noticeably insufficient targeted protection for the digital payment security of older adults. Although the Law of the People's Republic of China on the Protection of the Rights and Interests of Older Persons emphasizes the right of older adults to participate in society, it lacks specialized legislative protection against specific risks in digital financial contexts, such as telecommunications fraud and unauthorized transactions.

Although financial regulatory authorities have issued documents such as the Security Management Specifications for Mobile Financial Client Application Software, these provisions are largely based on general security requirements and do not sufficiently take into account the cognitive characteristics and operational habits of older users. As a result, a certain degree of mismatch exists between existing policies and the actual needs of older adults.

At the social level, the insufficient use of technology-assisted services constitutes a key hidden risk affecting the security of electronic payments for older adults. Many technologies specifically designed to assist older users, such as intelligent voice announcements and real-time pop-up warnings for suspicious transactions, have not fully played their intended role in practice. Some older adults have not even actively enabled these functions.

Older adults generally lack adequate channels through which to learn about such technologies. Meanwhile, younger people in the community may also be unaware of the existence of age-friendly technological functions and therefore unable to provide effective guidance.

3.5. Insufficient family companionship and support

Digital intergenerational support refers to the training and assistance provided by younger generations to older adults in the use of digital technologies. Among Chinese adults aged 65 and above, very few can

receive systematic guidance on electronic payment from their children at least once a week ^[7]. As a result, channels for older adults to acquire payment security knowledge remain fragmented.

Most younger family members provide only basic operational guidance while neglecting the transmission of security knowledge. Consequently, older adults may acquire the ability to conduct payments but lack awareness of risk prevention.

Such fragmented support is insufficient to establish an effective security protection system. In essence, the absence of family support reflects a deviation in family members' understanding of their responsibilities. Many younger family members underestimate the particular importance of improving the digital security capabilities of older adults.

4. Analysis of collaborative governance strategies for the security of electronic payments used by older adults

4.1. Giving full play to the catalytic and leadership role of public security authorities

China's existing laws and policies have established the leading role of public security authorities in combating and governing telecommunications and online fraud and safeguarding the payment security of the public. Article 6 of the Anti-Telecommunications and Online Fraud Law of the People's Republic of China stipulates that the state shall establish an anti-fraud working mechanism, with public security authorities taking the lead in anti-fraud efforts, while financial, telecommunications, cyberspace administration, market regulation, and other departments shall perform their respective regulatory responsibilities.

This means that in the collaborative governance of electronic payment security for older adults, public security authorities should assume the organizational role of overall coordination, being responsible for the formulation of comprehensive plans and the implementation of tasks. Banks, payment institutions, communities, and other actors should undertake prevention and management responsibilities within their respective areas.

Public security authorities should strengthen cooperation with other government departments to ensure the effective implementation and enforcement of electronic payment security policies. In the governance of electronic payment security for older adults, public security authorities should not only act as law-enforcement bodies but also play an important role in policy guidance and social mobilization.

4.2. Improving the institutional design of electronic payment security for older adults

Under existing laws, consumer protection legislation requires business operators not to impose unfair or unreasonable transaction conditions, while the Civil Code emphasizes the duty to provide notice and explanations regarding standard terms. The Regulation on the Implementation of the Law of the People's Republic of China on the Protection of Consumer Rights and Interests further requires business operators to provide information in a plain and comprehensible manner and expressly prohibits the use of false or misleading publicity to induce older adults to purchase goods or services that clearly do not meet their actual needs.

The Personal Information Protection Law recognizes individuals' rights to know, access, copy, correct, and delete their personal information and requires data processors to establish convenient mechanisms for exercising such rights ^[8].

The next step in legislation should not merely remain at the level of general principles. Instead, these

general rules should be transformed into specific statutory obligations applicable to electronic payment scenarios involving older adults. For example, the duties to provide important notices and adequate explanations, restrictions on standard terms, default security settings, and the principle of minimum necessary processing of personal information should be formulated more explicitly. This would provide older adults with stronger legal grounds on which to assert and protect their rights.

4.3. Strengthening the government's capacity for multi-party coordination and overall planning

To achieve genuine effectiveness in protecting the electronic payment security of older adults, governance cannot rely solely on concentrated campaigns and temporary publicity. First and foremost, the government must establish corresponding institutional safeguards and clarify responsibilities in order to promote the formation of a stable and sustainable long-term mechanism.

In other words, the government must not only “build the platform,” but also “establish the rules” and, more importantly, “ensure implementation.”

On the one hand, it is necessary to accelerate the improvement of the policy system for protecting the electronic payment security of older adults. The government may further refine age-friendly payment service standards, risk-warning specifications, complaint-handling procedures, and accountability rules based on the specific scenarios of electronic payment use by older adults, thereby promoting the establishment of a more operational institutional framework.

On the other hand, the targeted delivery of early-warning information should be improved. Previous publicity efforts have often focused on general reminders, resulting in broad coverage but insufficient targeting. Since older adults have distinctive risk-identification capabilities, usage habits, and life circumstances, the government should promote differentiated and classified warning mechanisms when coordinating early-warning efforts.

5. Research summary

This study focuses on the security of electronic payments for older adults as an important social issue in the digital era. It not only reveals the multiple risks and challenges faced by older adults in the process of using electronic payments but also proposes a collaborative governance approach centered on public security authorities, coordinated with other judicial authorities, and jointly involving banks, platforms, and families.

Traditional studies often regard older adults primarily as “victims.” Under the framework of collaborative governance, however, this study argues that older adults may not only be the objects of rights violations but may also, without awareness, become participants in criminal chains.

In existing research, older adults are often placed in a passive position requiring protection, with discussions focusing primarily on their victimization through fraud, misleading consumption, and information infringement. This study further argues, from the perspective of collaborative governance, that although older adults are generally a vulnerable group in electronic payment activities, under certain circumstances they may also become unintentionally involved in illegal and criminal chains due to cognitive limitations, information asymmetry, or manipulation by others, and may even become part of a criminal operation.

Disclosure statement

The author declares no conflict of interest.

References

- [1] Sahi AM, Khalid H, Abbas AF, et al., 2022, The Research Trend of Security and Privacy in Digital Payment. *Informatics*, 9(2): 32.
- [2] Almaiah MA, Al-Rahmi A, Alturise F, et al., 2022, Investigating the Effect of Perceived Security, Perceived Trust, and Information Quality on Mobile Payment Usage through Near-Field Communication (NFC) in Saudi Arabia. *Electronics*, 11(23): 3926.
- [3] Patra GK, Rajaram SK, Boddapati VN, et al., 2022, Advancing Digital Payment Systems: Combining AI, Big Data, and Biometric Authentication for Enhanced Security. *International Journal of Engineering and Computer Science*, 11(8): 10.18535.
- [4] Chand K, Tiwari R, Gupta A, et al., 2025, How Does Perceived Security Influence Mobile Wallet Users' Behavior? A SEM Investigation. *Managerial Finance*, 51(1): 146–165.
- [5] Luo RH, Wang N, Zhu X, 2025, Fraud Detection and Risk Assessment of Online Payment Transactions on E-Commerce Platforms Based on LLM and GCN Frameworks. *arXiv preprint*, arXiv: 2509.09928.
- [6] Dhar BK, Omar MA, Yusuf AH, et al., 2026, Ethical Imperatives in Digital Finance: Advancing E-Payment Inclusion in a Fragile Economy. *Business and Society Review*, 131(1): e70031.
- [7] Nurlaila F, Kusmiati E, Shiddieq DF, 2026, Consumer Preferences in Choosing Payment Methods on the TikTok Shop and Shopee Platforms. *Golden Ratio of Mapping Idea and Literature Format*, 6(1): 886–897.
- [8] Galilea M, Farazi S, Mare DS, 2026, Firm Credit Constraints and Electronic Payments: A Global Analysis. *SSRN*: 6065193.

Publisher's note

Bio-Byword Scientific Publishing remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.