

Research on the Dual-track Governance Path of Community Anti-fraud for the Elderly Against the Background of Digital Aging

Mingna Xia, Jia Yongfang*

School of Humanities, Inner Mongolia University of Technology, Hohhot, 010080, China

*Corresponding author: jiajf2020@imut.edu.cn

Abstract: With the accelerated advancement of digital aging, the elderly are facing increasingly concealed risks of marketing fraud in private-domain cyberspace. New-type scams such as private-domain live-streaming and community-group marketing target seniors' health anxieties and emotional voids, forming a complete chain of "offline lead-in — community-group relationship maintenance — private-domain exploitation". Traditional anti-fraud models can hardly cope with such threats. Based on the analytical framework of dual-track intelligent control featuring "AI monitoring plus social work intervention", this paper proposes a governance path that deeply integrates technical efficiency and humanistic care. The study finds that the effective operation of dual-track intelligent control relies on three key mechanisms: precise capture of semantic features of private-domain fraud by AI recognition models, graded intervention for high-risk groups through professional social work methods, and a complete service loop of "early warning — disposal — feedback — iteration". On this basis, this paper discusses optimization strategies for dual-track intelligent control from the dimensions of technical standard formulation, community-based workforce cultivation and multi-party collaborative governance. It provides theoretical references and practical approaches for community anti-fraud initiatives for the elderly under the background of digital aging.

Keywords: digital aging; anti-fraud for the elderly; dual-track intelligent control; social work intervention

1. Problem Formulation

1.1 Digital Inclusion and Risk Exposure of the Elderly

Data from the Seventh National Population Census shows that China's population aged 60 and above has reached 264 million, accounting for 18.7 % of the total population. Meanwhile, the scale of elderly netizens keeps expanding, and internet penetration among senior groups rises year by year. Digital technologies are supposed to empower and enrich later-life experiences, yet they also open windows for risk intrusion. Telecom and online fraud targeting the elderly remains prevalent. Fraud tactics have evolved from conventional telephone sales and false health-product promotion to sophisticated modus operandi including AI face-swapping, voice synthesis and precise algorithm-driven victimization.

"Digital aging" has risen onto the national policy agenda. The General Office of the State Council issued Implementation Plan for Effectively Solving the Difficulties Encountered by the Elderly in Using Intelligent Technologies, and local authorities have rolled out age-friendly transformations. Nevertheless, a notable gap exists between "being able to use digital tools" and "being capable of defending against risks". As Zhang Dongxiang, Party-branch secretary of Dongxiang Good-Mothers Workshop in Jiaozuo, commented: "Many seniors are eager yet afraid to embrace smartphones. They are curious about digital devices but fear operational mistakes and fraud, and consequently choose to stay away from them." Such "digital fear" mirrors the insufficient attention paid to safety dimensions in current digital-aging practices.

1.2 Concealed "Preying on the Elderly" in Private-domain Spaces

In recent years, a more insidious form of fraud has proliferated: private-domain marketing fraud. Research conducted by Professor Shen Qi's team at the Fudan University Institute of Aging Studies

reveals a full scam chain. Perpetrators attract seniors with free give-aways such as eggs, gain their trust through offline interactions, pull them into exclusive social-media groups for long-term emotional bonding, and finally defraud them of large sums of money via closed private-domain live-streaming sessions.

This operational logic precisely exploits core psychological vulnerabilities of older adults: health-related anxieties, emotional emptiness and lack of self-worth. The closure of private-domain environments enables fraudsters to evade censorship on mainstream platforms, while “warm companionship” within online groups builds strong emotional bonds between scammers and elderly victims. The experience of Cai Yaohui’s family is illustrative: even after being forced to quit health-related chat groups, the elderly family member secretly rejoined them without perceiving any wrongdoing. Such trust dislocation — seniors trusting scammers while doubting their own family members — constitutes a core barrier to anti-fraud intervention.

Statistics from the Yuyao Anti-fraud Center indicate that among online fraud cases involving seniors in 2025, impersonating customer service accounted for 48.65 %, fake online investment and wealth-management fraud 13.51 %, and shopping fraud 12.16 %. Although private-domain live-streaming “elder-targeted traps” have not generated massive reported cases, multiple regions have listed them as key priorities for prevention and rectification. Beneath the visible tip of the iceberg of private-domain fraud lies enormous governance demand.

1.3 Dual Dilemmas Facing Community-based Anti-fraud Work

Communities serve as both the first and last line of defense against fraud targeting the elderly. Still, community anti-fraud governance is plagued by two persistent dilemmas. The first concerns resource allocation: understaffed and overburdened community police officers and grid administrators serve thousands of households and cannot respond in real time to massive risk information. For instance, Qingshan Branch of Baotou Public Security Bureau published over 950 issues of its Daily Anti-fraud Bulletin reaching nearly 300 000 residents, yet tensions persisted between outreach coverage and targeting precision. The second dilemma relates to limited effectiveness of one-way education. Conventional practices including distributing leaflets, posting posters and reading manuscripts are poorly adapted to older adults’ cognitive habits. An anti-fraud lecture co-hosted by an H-city community and local police station achieved positive outcomes through real-case analysis and warning video screenings. Nevertheless, such face-to-face activities are constrained by manpower and cannot deliver regular, full-coverage risk monitoring.

2. Theoretical Logic of Dual-track Intelligent Control

2.1 AI Monitoring: From Random Search to Precise Profiling

In recent years, the application of artificial intelligence in anti-fraud work has shifted from crude screening to precise identification. Powered by natural-language processing and speech-recognition technologies, anti-fraud systems conduct semantic analysis on multi-modal content including texts, voices and short-video links to detect linguistic characteristics of fraud scripts. For example, W-city Branch of Industrial Bank constructed a data-driven intelligent elderly-protection anti-fraud system establishing comprehensive data-standardization systems covering terminology, models, interfaces and quality to deliver precise account-risk monitoring and protection for elderly clients. The core strengths of the technical track lie in efficiency and coverage. Unlike traditional anti-fraud outreach relying on home visits or group lectures, AI systems enable 7 × 24-hour real-time monitoring, rapidly screen risks from massive volumes of information and output risk levels together with supporting evidence. The Nanteng Community in Yuhang District deployed “social-work robots” connected to the Yuzhihuang big-data intelligent terminal. These robots answer policy inquiries and undertake repetitive work such as anti-fraud publicity and guided tours, freeing social workers from trivial tasks. This demonstrates that intelligent technologies can function as community-governance infrastructure to boost overall service efficiency.

Nevertheless, deep-rooted technical-adaptation challenges remain. General-purpose AI models struggle to fully grasp older adults’ unique linguistic habits, cognitive patterns and risk perceptions. Moreover, early-warning messages generated by online systems may be mistaken for scam calls and rejected without reliable delivery channels. Practices from Benxi Municipal Public Security Bureau show that AI voice-bot calls to seniors are frequently hung up as suspected fraud. Technology can

“detect risks”, yet it cannot guarantee that seniors “believe the risks”.

2.2 Humanistic Intervention: Professional Values of Work with the Elderly

Artificial intelligence addresses the problem of “identifying problems”, whereas human agents are required for “responding to problems”. Rooted in the core concept of “person-in-situation”, social work bears distinctive value in anti-fraud governance. Casework enables one-on-one intervention for seniors at high risk of victimization; group work facilitates peer-oriented anti-fraud education; community-work practices mobilize community resources to build mutual-support anti-fraud social networks.

Local humanistic anti-fraud practices have accumulated rich experience. The H-city Railway Transport Procuratorate and Industrial and Commercial Bank of China jointly launched procuratorial-bank anti-fraud campaigns. Tailored to older adults’ cognitive traits, they delivered precise publicity through case-based interpretation, on-site explanations and one-on-one consultations. Integrating anti-fraud education into digital-skill training for seniors, they held 403 training sessions attended by 6 918 participants, simultaneously advancing digital-skill improvement and risk-awareness cultivation. Therefore, the irreplaceable value of humanistic defense lies in its embodiment and trust-building. When community police officers sit beside seniors explaining fraud patterns in local dialects, or senior volunteers share anti-fraud experiences as peers, what is transmitted is not merely information but interpersonal relationships and trust. Even so, humanistic defense suffers from limited coverage, delayed responses and uneven professional competence.

2.3 Dual-track Intelligent Control: Mutual Construction Rather Than Simple Superposition

The core merit of dual-track intelligent control resides not in simple addition of technology and humanistic services, but in their mutual construction. On the one hand, artificial intelligence renders social-work interventions more forward-looking and targeted. Instead of reacting passively to reported incidents, social workers deliver proactive services guided by real-time early warnings. On the other hand, feedback from social-work interventions supplies real-world scenario data and effectiveness validation for AI-model iteration, driving technological evolution from “accurate identification” toward “effective intervention”. Such mutual-construction relationships are practiced through a closed-loop workflow: “identification — early warning — intervention — follow-up — capacity-building”. Drawing on pilot design in Community W of City H, the online platform monitors private-domain content and outputs risk levels. High-risk alerts trigger home visits by social workers within 24 hours. Service data recorded during interventions flows back to the system to optimize recognition models and update local-scenario feature libraries. Long-term follow-up builds seniors’ self-defense capabilities, shifting from passive protection to active risk prevention.

Preliminary prototypes of dual-track coordination can be observed in field research on Qingshan Public-Security Sub-bureau in Baotou. Its Daily Anti-fraud Bulletin is distributed daily across 73 communities and 1 056 community service groups. Police officers combine bulletin content with on-site anti-fraud explanations during household visits. This model of “online targeted push plus offline in-person explanation” exemplifies coordination between technically-produced content and human-relationship networks.

3. Key Mechanisms of Dual-track Intelligent Control

3.1 Precise Modelling for Fraud Identification

The starting point of dual-track intelligent control lies in accurate identification of private-domain fraud. A dedicated feature library of fraud scripts targeting seniors should be constructed, covering high-frequency fraud types including false health-product promotion, elderly-care wealth-management scams and impersonation of relatives or community staff. The typical operational chain of private-domain fraud has become clear: offline lead-in via free benefits → emotional bonding within online groups → financial exploitation via private-domain live-streaming. Recognition models should capture not only keywords and rhetorical patterns but also behavioral characteristics such as “group-nurturing cycles”, coupon-redemption thresholds and fabrication of public-welfare personas. Light-weight deployment is critical technically. The system shall support one-click detection of diverse private-domain materials including WeChat chat records, group messages, short-video private messages

and voice messages, outputting risk grades and supporting grounds within a short time frame. Dynamic updating of local-case libraries accelerates responses to emerging fraud tactics. When new fraud variants are discovered in communities, feature extraction, model training and version updates can be completed within a short cycle, shortening the time lag between fraud emergence and technical detectability.

3.2 Converting Information Output into Action Instructions

Governance value of AI-monitored risk grades cannot be realized if outputs remain purely informational. The core of graded early-warning mechanisms is translating technical judgments into actionable operational directives. Specifically, high-risk scenarios (e.g., large-sum transfers, impersonation of judicial authorities) trigger emergency responses: real-time pop-up alerts are sent simultaneously to community social workers and elderly users' family members, requiring prompt home or telephone verification. Medium-risk scenarios (e.g., health-product sales, wealth-management pitches) trigger anti-fraud reminders and flag individuals for priority attention. Low-risk scenarios automatically push customized anti-fraud knowledge for regular education. A technical challenge concerns scientifically-calibrated early-warning thresholds. Over-high thresholds produce missed risks; over-low thresholds generate excessive false alarms leading to "alert fatigue" among social-work practitioners. A viable solution accumulates real-world early-warning and disposal datasets in community pilot operations, dynamically optimizing grading criteria through machine learning to continuously improve warning accuracy throughout operation cycles.

3.3 Unifying Standardization and Flexibility

Post-warning interventions need to balance standardized workflows and flexible service delivery. On the one hand, standard operating procedures must be guaranteed to secure response timeliness and service quality, including 24-hour home-visit protocols for high-risk alerts, interview templates for on-site verification, operational guidelines for loss mitigation, and formatting specifications for service documentation. On the other hand, given individual disparities and situational complexities among older adults, social workers must flexibly adjust communication approaches and service strategies based on professional judgment, avoiding rigid execution that damages trust-building.

Unification of standardization and flexibility relies on digital service ledgers. Ledger systems document every early-warning event, intervention approaches and assistance outcomes, supplying evidence for standardized assessment as well as materials for professional reflection among gerontological social workers. More importantly, ledger-recorded data feeds back into the anti-fraud application-system model, closing the loop of "monitoring-intervention-feedback-optimization" and enabling continuous system evolution during operation.

4. Optimization Pathways for Dual-track Intelligent Control

4.1 Establishing Technical Standards for "Senior-oriented Protection"

Current anti-fraud products for seniors suffer from "products without standards". Existing age-friendly transformations mostly focus on interface adjustments such as enlarged fonts and simplified icons, while security protection is seldom treated as a core objective. Enterprises are therefore encouraged to formulate technical standards for a "senior-protection mode", specifying functional norms for intelligent information filtering, abnormal-behavior monitoring and family-linked early warnings. Province S has carried out age-friendly digital-technology transformations by launching "Elder Mode" and "Care Mode" for mobile applications, yet standardization of security-protection functions remains insufficient. Policy incentives granted by governments to certified mobile phones and applications can accelerate popularization.

4.2 Cultivating Community-based Anti-fraud Service Capacity

Humanistic-service delivery under dual-track intelligent control requires locally-rooted professional community teams. Community grid administrators and gerontological social workers currently exhibit uneven anti-fraud competence, calling for systematic training systems. Practices in City H offer references: over 30 key instructors received training to build a digital-help-the-elderly lecturer cohort delivering courses on smartphone operation and anti-fraud knowledge. Training curricula should cover

fraud-pattern recognition, on-site-interview communication skills, psychological-counseling techniques and crisis-disposal workflows. Meanwhile, development of “senior anti-fraud propagandist” teams can be explored, mobilizing physically-fit community young-old residents for anti-fraud outreach and neighborhood mutual supervision. Peer-education approaches enhance acceptance among elderly residents.

4.3 Promoting Multi-party Collaborative Governance

Private-domain-fraud governance involves overlapping responsibilities across public-security, market-regulation, cyberspace-administration and other departments. Joint-rectification mechanisms established by market-regulation, health-authority, comprehensive-law-enforcement and public-security departments in Yuyao City provide references. Market-regulation authorities conduct source investigation and law enforcement; health-authorities carry out senior-targeted publicity; public-security bureaus build a three-dimensional prevention-and-control system combining early-warning interception, full-chain crackdown and targeted publicity. Effective dual-track intelligent control necessitates breaking inter-departmental data barriers. Under premises of personal-information protection, information-flow loops for “monitoring-early-warning-disposal-law-enforcement” should be promoted. The AI cloud-broadcasting system jointly built by Babu District of Hezhou City and China Telecom establishes a three-level broadcast-control network covering district-level general platforms, township sub-platforms and village-community terminals for regular anti-fraud outreach. Such “technology-plus-organization” collaborative models merit replication.

4.4 Embedding Initiatives Within Digital-aging Policy Frameworks

Elderly anti-fraud work should not progress in isolation but be embedded within overall digital-aging policy frameworks. Ideas from Shandong civil-affairs authorities on constructing a four-level home-community elderly-care service network deserve attention. Leveraging day-care centers, rural happiness homes and senior-dining facilities, information-based tools extend professional elderly-care services to seniors’ bedsides, homes and neighborhoods. Anti-fraud functions shall coordinate with popularization of smart devices for seniors, age-friendly application renovation and digital-literacy promotion for older adults. When anti-fraud becomes a standard component rather than an add-on of digital-aging initiatives, dual-track intelligent control gains sustainable institutional foundations.

5. Conclusion

Digital aging is not one-sided technological embedding into elderly life, but value transformation through technologies adapting to senior needs. In anti-fraud work for older adults, deep integration of AI monitoring and social-work interventions responds to a core governance proposition: technological tools need calibration by humanistic values, while humanistic services require empowerment via technical instruments. Neither can stand alone; they mutually construct and reinforce each other. Intelligent technologies resolve efficiency challenges of risk detection; social-work practice addresses human-oriented risk-response challenges. They empower one another.

The recurring prevalence of private-domain marketing fraud originates from its precise exploitation of gaps between seniors’ emotional needs and digital capabilities. Solutions depend not merely on “smarter algorithms”, but also “more compassionate services”. Intelligent platforms act as “far-reaching eyes” for social workers, while social workers serve as “trust-building bridges” for intelligence. The essence of the “dual-track” approach lies in enabling technologies to understand seniors’ expressions and risk perceptions, and equipping humanistic services with technical early-warning capabilities. Dynamic closed-loop operations drive the transition from passive interception to active risk prevention. This constitutes the innermost proposition of digital aging: the humanity of technology lies in how it serves human dignity. Safeguarding elderly property security represents a vital task for digital-society construction and grassroots-community governance. The dual-track governance path integrating artificial intelligence and humanistic care supplies practical inspiration for community anti-fraud work targeting seniors. It strives to endow technologies with human warmth and furnish human services with technical support, enabling older adults to participate safely in digital life and consolidating protective safeguards for their property interests.

Funding information

Supported by the Basic Scientific Research Operating Funds Project for Directly-Affiliated Universities of Inner Mongolia Autonomous Region (Grant No. ZYT2026031).

References

- [1] Wu H X. Guarding the Elderly's Money-bags through Anti-fraud Actions. *Yixing Daily*, 2024-10-25(003).
- [2] Huang W. Research on Prevention Paths of Elder-targeted Telecom-network Fraud //Proceedings of the 2025 Academic Symposium on Social-structural Change and Governance Innovation in the Digital Era (Volume II). Chinese Society of Wisdom Engineering Research, 2025:285-287.
- [3] Yu X L. Upholding Rule-of-law Governance to Protect Seniors from Fraud. *Masses*, 2023(8):41-42.
- [4] News Feature: Assisting the Elderly and Preventing Fraud to Safeguard the "Red Sunset". *China Telecommunications Trade*, 2022(10):8.
- [5] Chen Y N. Research and Practice on Design of Popular-science Picture Books for Seniors' Digital-life Education. Sichuan Normal University, 2026.
- [6] Zhang Q M. Research on Elderly-care Fraud from Dual Perspectives of Digital Divide and Intelligent Anti-fraud. *China Anti-counterfeiting Report*, 2026(7):72-77.
- [7] Wang Y. Research on Government-responsibility Optimization During Urban-elderly Digital-inclusion in Smart Communities — A Case Study of Community C in City R. *Qufu Normal University*, 2026.
- [8] Zhao Y H. Group-work Intervention for Improving Anti-fraud Competence of Urban Solitary Seniors. Beijing University of Civil Engineering and Architecture, 2025.
- [9] Wang Y. Research on Group-work-based Improvement of Seniors' Financial Literacy: A Case Study of Community X in Wuhai City. Ningxia University, 2025.
- [10] Bian Y. Research on Group Intervention for Seniors' Financial Literacy Under the EPS Model. *Social Welfare*, 2025(10):23-35.
- [11] Yu X, Liu S. Effects of Primary-group Support on Seniors' Vulnerability to Fraud Victimization //Proceedings of the 2023 Annual Academic Conference of the Chinese Gerontological Society and Geriatrics Society. Chinese Gerontological Society and Geriatrics Society, 2023:420-428.