

A Study on Community Anti-Fraud Practice for the Elderly from the Perspective of Technology-Service Coupling-A Case Study of the “Private-Domain Eagle Eye” APP

Mingna Xia, Jia Yongfang*

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

*Corresponding author: jiajf2020@imut.edu.cn

Abstract: Against the backdrop of rapid development of the digital society, the number of elderly netizens keeps growing. Private-domain social scenarios such as WeChat groups and short-video private messages have gradually become high-risk spaces for fraud targeting the elderly. Fraud tactics including false marketing of health-care products, pension-related financial scams, and impersonation of relatives or community staff keep evolving. Embedded in acquaintance-based social relations, such frauds are highly concealed and difficult to identify and handle. Nevertheless, current anti-fraud governance for the elderly is confronted with the practical dilemma of separation between technical tools and humanistic services. Intelligent anti-fraud systems excel at identifying and warning of risk information yet lack follow-up intervention procedures implemented at the grassroots community level. Traditional community-based anti-fraud services rely on offline lectures and home visits. Restricted by manpower supply, they can hardly realize real-time capture and hierarchical disposal of risk clues. Technology-service coupling combines the risk-identification advantages of artificial intelligence technology with the human-intervention strengths of social work for the elderly, so as to build a collaborative governance model featured by technology empowerment and service guarantee. Taking the research-practice project “Private-Domain Eagle Eye” anti-fraud mini-program as the research carrier, this paper adopts field theory and conducts pilot practice in Community W of City H. Quantitative research methods are applied to analyze practical characteristics of fraud against the elderly in private-domain scenarios, interpret the operation logic of dual-track technology-service coupling, sort out practical dilemmas encountered in implementation, and explore feasible anti-fraud paths for the elderly suitable for urban communities in China. It provides practical references for the protection of the elderly’s property rights and interests under the background of smart-community construction.

Keywords: technology-service coupling; anti-fraud for the elderly; private-domain scenarios; community governance

Introduction

With mobile internet deeply integrated into daily life, more elderly people gain access to the digital world, and social software has become an important carrier for them to acquire information and engage in social interactions. According to Bourdieu’s field theory, a field refers to a network space composed of objective relations among different positions. Private-domain social interaction constitutes a special action field, where internal rules, capital and actors interact with one another and create breeding ground for pension-targeted fraud. Within private-domain fields, fraudsters build trust through emotional capital and conduct deceptive inducement by taking advantage of information asymmetry. Different from public online platforms, WeChat group chats and private messages are highly closed-off, which makes external supervision difficult and brings new challenges to grassroots anti-fraud governance.

At present, two major governance paths have taken shape for anti-fraud work among the elderly in China. The first is the technology-oriented governance path, which relies on artificial intelligence and big data to realize risk identification and call-warning services. The second is the grassroots-service-oriented path, where community grid workers and social workers deliver anti-fraud lectures and conduct home-based reminders. These two paths belong to different action fields. The

technical field pursues identification efficiency and focuses on algorithmic judgment, while the community-service field centers on human needs and attaches importance to case-based assistance and social-support-network construction. Lacking institutional connection channels, they have given rise to the governance contradiction of “unimplementable early-warnings and clue-deficient services”. Technology-service coupling promotes factor flow between the two fields, breaks barriers between technical systems and community services, and realizes process embedding of algorithm identification, risk warning, professional intervention and long-term education.

This paper takes the “Private-Domain Eagle Eye” anti-fraud mini-program as the practical carrier and carries out pilot research in Community W of City H. Boasting a high proportion of elderly residents, this community frequently encounters fraud-risk clues arising from private-domain marketing and serves as a typical field-research sample. Therefore, this investigation adopts questionnaire-based quantitative research, semi-structured interviews and action research. Based on field theory, it analyzes the occurrence logic of private-domain fraud, explores the operation mechanism of the technology-service coupling model, summarizes practical dilemmas and optimization strategies, and offers experience-based references for anti-fraud governance for the elderly in urban communities.

1. Concept Definition and Analytical Framework

1.1 Core Concepts

1.1.1 Private-domain fraud against the elderly

The term “private-domain marketing” was mentioned in the 2026 315 Gala. It refers to deceptive behaviors including false marketing, investment-related fraud and identity-impersonation scams targeting the elderly in closed social fields such as WeChat private chats, group chats and short-video private messages. Fraudsters build emotional bonds through acquaintance-based social interactions. Information flows sluggishly within such fields, making it hard for external parties to detect risk clues in advance.

1.1.2 Technology-service coupling

Originating from system theory, the concept of coupling, when applied to governance scenarios, means that technical systems and community-service systems are no longer simply spliced together. Instead, they realize standard interoperability, process docking and two-way information feedback. In the anti-fraud field for the elderly, technical systems undertake private-domain information identification, risk grading and clue pushing; community-service systems receive early-warning clues and implement practical interventions. Case samples accumulated in service practice are fed back into technical systems to drive algorithm iteration, forming a bidirectionally-circulating organic system.

1.1.3 “Private-Domain Eagle Eye” APP

The “Private-Domain Eagle Eye” APP is a lightweight community-oriented anti-fraud tool developed for this project. It contains three terminals: an elderly-friendly user terminal, a social-worker operation terminal and a community-management terminal. Leveraging natural-language processing and speech-recognition technologies, it detects risks in private-domain texts, voice messages and short-video copywriting, outputs three-level risk results (high, medium and low), and binds hierarchical intervention procedures for social-work-based community-governance pilot applications.

1.2 Analytical Framework Based on Field Theory

From the perspective of field theory, private-domain social interaction forms a virtual independent action field. Fraudsters, elderly residents, community workers and technical tools are all actors within this field, who possess different forms of capital. Fraudsters own emotional-discourse capital; the elderly possess economic capital; community workers have service-related and institutional capital; and technical tools provide data-driven technological capital.

This study constructs a three-dimensional analytical framework. First, the private-domain-field dimension analyzes relational logic and practical characteristics of fraud occurrence. Second, the coupling-operation dimension explores how technical systems and community-service systems realize factor embedding within the field. Third, the constraint-condition dimension analyzes obstacles to the coupling-model operation from four perspectives: technical limitations, grassroots manpower, user

literacy and institutional compliance. On this basis, optimization paths for community anti-fraud work are proposed.

2. Practical Characteristics of Fraud against the Elderly and Governance Dilemmas in Private-Domain Fields

In Community W of City H, 100 questionnaires were distributed and 95 valid questionnaires were retrieved. Meanwhile, 20 semi-structured interviews were conducted with community grid workers, social workers and elderly residents. Questionnaire data show that 42 % of surveyed elderly respondents have encountered marketing information about health-care-product sales or pension-investment projects in WeChat groups or private messages, and 17 % have received messages sent by impostors claiming to be relatives or community staff. Fraud risks in private-domain fields have become a non-negligible practical problem for communities.

2.1 Main Characteristics of Fraud against the Elderly

First lies the field-operation logic of emotion priority. Instead of committing fraud directly in private-domain fields, fraudsters accumulate emotional capital via casual chatting, free-gift offers and health-science popularization. They gradually gain the elderly's trust before launching deceptive inducement. Deceptive behaviors are embedded in daily social interactions and thus become much harder to identify. Second, fraud types are concentrated. Three prevalent scam types are identified in survey samples: false marketing of health-care products that exaggerate product efficacy by exploiting the elderly's health-related anxiety; pension-investment scams that induce capital input with promises of high returns; and identity-impersonation fraud where perpetrators fabricate excuses to demand money by posing as relatives or public-service staff. Third, field closure leads to delayed clue discovery. Private-domain chat contents are only visible to internal participants, so external intervention can hardly be realized. More than 60 % of risk clues are discovered by family members or communities only when property losses are imminent, leaving obvious time lags for risk disposal. Fourth, discourses keep iterating. Fraudsters constantly evade obvious violation-related keywords and adapt to communication contexts within the field, which weakens the identification effect of traditional keyword-interception methods.

2.2 Governance Dilemmas of Community Anti-Fraud Work

Clues are mostly discovered passively. Communities can hardly take the initiative to access residents' private-domain social scenarios. Most clues are obtained through police reports or feedback from family members, resulting in insufficient capacity for early risk warning. Disconnection between the technical field and the community-service-field means existing anti-fraud tools focus on individual-user warnings and lack functions for clue transfer and task assignment for communities. Even if algorithms identify risks, early-warning prompts cannot be transformed into practical risk resolution without support from community-service-field actors. The adaptive capacity of the elderly within the field varies: some elderly people suffer from insufficient digital literacy and weak ability to distinguish online social-interaction risks. Meanwhile, they are wary of new software, so subjective cognition restricts the implementation of technical tools. Cross-actor collaboration among public security bureaus, civil-affairs departments and communities is inadequate. Belonging to separate governance fields, they lack regular information-circulation mechanisms, leading to poor connection of cross-department disposal procedures after communities discover clues.

From the field-theory perspective, neither algorithm-based tools in the technical field nor public-oriented lectures in the community-service field can change the internal action logic of private-domain-fraud fields. Therefore, it is practically necessary to realize the coupling of technological capital and service-oriented capital.

3. Operation Measures of Technology-Service Coupling

The "Private-Domain Eagle Eye" APP promotes embedding of technical systems into community-services for the elderly. Technical systems output risk clues; social-work practitioners carry out hierarchical interventions. Case samples accumulated in service practice are fed back into technical modules to drive system optimization and update, thus realizing bidirectional coupling between the two

systems.

3.1 Age-Adaptive Technical Design

Developed through secondary development based on speech-recognition frameworks, this mini-program is positioned as a community-pilot tool rather than ground-level-algorithm-oriented research and development. The elderly-friendly terminal adopts large-font and high-contrast age-adaptive design. Users can submit texts, voice messages and screenshots for risk detection without registration. Risk levels and judgment grounds are output within 10 seconds. Results support voice broadcast, and an entrance for one-click consultation with community workers is embedded to fully accommodate elderly users' usage habits.

The social-worker operation terminal receives hierarchical early-warning tasks. High-risk alerts require telephone verification or home-visit investigation within 24 hours; medium-risk alerts push anti-fraud-reminder tasks; low-risk subjects are included in key-concern ledgers. After completing persuasion, psychological counseling and anti-fraud publicity, social workers input disposal records into the system to form complete service closed loops. The community-management terminal realizes visualized statistical charts of regional risk data and supports input of local fraud discourses for continuous iteration of identification models. For privacy-protection purposes, contents submitted by users are only used for real-time risk judgment and will not be stored for long unless necessary.

3.2 Intervention Procedures of Social Work

Based on different risk levels within the field, professional social-work methods are embedded into disposal chains. For high-risk scenarios, social workers conduct case work, visit households to expose scam logic, provide psychological comfort, coordinate with family members, and contact public-security departments when necessary to stop losses and implement persuasion. For medium-risk scenarios, grid workers and social workers deliver home-visit reminders and popularize easy-to-understand anti-fraud materials. Low-risk groups are included in regular-concern lists, and anti-fraud-themed group activities are organized to promote experience exchange among the elderly. Meanwhile, community-level anti-fraud publicity is carried out according to high-incidence-fraud types counted by the system. Low-aged healthy elderly residents are encouraged to form a "silver-age anti-fraud-propagandist" team to activate the elderly's own anti-fraud capital and reverse their passive-victim status in private-domain fields.

3.3 Pilot-Effect Optimization

After community-oriented operation training, community workers use this mini-program to judge risks of suspicious private-domain information collected within their jurisdiction. Questionnaire statistics show that the comprehensive satisfaction of community workers and elderly residents reaches 91 %. The mini-program can rapidly identify typical fraud discourses, and digital ledgers simplify community-work recording procedures. Some potential risks are intervened in at embryonic stages. Nevertheless, the pilot also reveals practical contradictions in the operation of the coupling model: limitations exist in dialect-speech recognition; newly-emerging fraud discourses may trigger identification omissions; some elderly people resist online tools; rising fraud-related clues will increase community manpower burdens. Multiple practical constraints still exist for factor coupling between the two fields.

4. Operation Dilemmas of the Technology-Service Coupling Model

4.1 Limitations of the Technical Field

Discourses in private-domain-fields keep updating, and fraudsters constantly adjust expressions to evade identification rules. Algorithm models require continuous supplementation of community-collected case samples. Short-term service pilots cannot support long-term iteration. In addition, recognition of colloquial and dialect-based chat contents still has deficiencies. Algorithms can only serve as primary-screening tools instead of achieving fully accurate judgment, so manual recheck procedures must be retained.

4.2 Manpower Shortages within the Field

Technical systems may output batches of early-warning information even on holidays, yet all offline disposal consumes community human capital. Community affairs are complicated during holidays and staff resources are limited. Massive surges of early-warning clues will easily lead to task overload. Manpower contradictions remain insignificant within small-scale pilot communities, but manpower shortages will become key factors restricting coupling-effect release once the model is promoted widely. Volunteers and silver-age anti-fraud propagandists can serve as supplementary forces, whereas their stability and professional competence cannot be guaranteed.

4.3 Subjective Practical Barriers among the Elderly

Some advanced-age elderly people lack the capacity to independently operate the APP. Others refuse to submit private-chat contents for detection out of privacy concerns. Technical tools can only cover groups proficient in smart-phone operation. For elderly residents with poor digital competence, the platform exerts limited effects, and traditional home-visit investigations and family-member supervision have to be adopted. Thus technical empowerment has objective boundaries.

4.4 Multi-party-collaboration and Data-privacy Constraints

This practice is merely a community pilot focusing on mechanism-level discussion. Interfaces with business systems of public-security and civil-affairs departments have not been realized, and cross-department clue transfer still relies on manual communication. Anti-fraud tools involve sensitive user information, while grassroots communities lack professional data-security operation-and-maintenance capabilities. For large-scale implementation, systems for data collection, storage, permission control and desensitization must be improved to prevent personal-information-leakage risks.

5. Optimization Paths for the Technology-Service Coupling Model from the Field-Theory Perspective

5.1 Strengthen Technical Adaptability

It should be clarified that online platforms are merely auxiliary governance tools, and anti-fraud governance cannot be fully entrusted to technologies. Adhere to lightweight development suitable for the elderly. Establish a two-way supply mechanism for anti-fraud cases from public-security authorities and local community-collected cases to continuously update identification-sample databases. Implement the mechanism of “AI primary screening plus manual recheck”. Algorithm outputs serve only as references, and final risk judgment shall be made by community workers in combination with local practical conditions. Meanwhile, abolish rigid requirements for independent operation by elderly users and support submission by social workers or family members to lower usage thresholds for the elderly.

5.2 Enrich Human Capital

In response to grassroots manpower shortages, build a multi-dimensional team consisting of “social workers + grid workers + silver-age anti-fraud propagandists + university-student interns”. Professional social workers are mainly responsible for high-risk case-oriented interventions; community grid workers undertake clue investigation and home-visit docking; low-aged elderly residents in communities are recruited as silver-age anti-fraud propagandists to give play to neighborhood-mutual-assistance advantages; university social-work-major interns share basic work such as ledger sorting and publicity-material production. Meanwhile, maintain hierarchical-disposal platforms and simplify data-processing work to reduce sorting burdens for grassroots communities.

5.3 Carry out Classified Anti-Fraud Services

It is particularly important to face up to differentiated digital-literacy levels among the elderly and reject one-size-fits-all promotion of technical tools. Provide accompanied practical-operation training for elderly residents capable of using mobile phones. Do not force senior citizens with advanced age

and low digital literacy to use software; instead, implement protection via family-member supervision and regular home-visit investigations. Questionnaire findings indicate that many elderly people fall victim to fraud due to lack of emotional-companionship from children in private-life fields. Anti-fraud work shall not only focus on property-right-protection but also take the elderly's emotional needs into account, so as to narrow the survival space for fraudsters who take advantage of emotional capital.

5.4 Open up Collaborative-Governance Chains

Implement laws related to personal-information protection in society, adhere to the principle of minimum-necessary data collection, complete data desensitization and permission control, establish safety-protection plans for vulnerable groups, and stick to information-security bottom lines. Promote the establishment of regular clue-transfer mechanisms among communities, public-security bureaus and civil-affairs departments. Major community-discovered risk clues shall be rapidly transferred to public-security authorities, and typical cases released by public-security departments shall be fed back to communities for science-popularization purposes. Social workers actively explore government-purchased-service modes to introduce social-organizations into anti-fraud services and guarantee sustainable operation of anti-fraud models.

5.5 Realize Community-Oriented Services in Light of Local Conditions

Field-resource conditions vary among different communities, so identical implementation schemes cannot be copied mechanically. Large-scale urban communities can fully activate complete functions including data visualization and task assignment. By contrast, micro-communities shall simplify data-statistics workload and focus on risk detection and simple ledgers. In township communities where digital competence is relatively poor, dependence on online tools shall be weakened, and priority shall be given to offline-volunteer-assistance modes, so that models can match local field-condition characteristics.

6. Conclusion

Private-domain social interactions constitute a unique action field. Fraudsters take advantage of field closure and emotional-interaction logics to commit fraud against the elderly. Neither pure technical governance nor pure offline services can resolve current anti-fraud dilemmas. The technology-service coupling model promotes two-way flow of technological capital and community-service capital, and forms a complete governance closed loop of “identification – early-warning – intervention – long-term cultivation”, which provides new practical paths for community-based anti-fraud work for the elderly.

Analysis of the “Private-Domain Eagle Eye” APP pilot based on field theory shows that the coupling model possesses governance value, yet it is constrained by multiple factors including data-sample-iteration pressure, grassroots-manpower supply, digital literacy of the elderly and data compliance. Technologies themselves cannot replace community-social-work services; the two form a complementary and symbiotic relationship. Technologies focus on solving the problem of “early detection” of risk clues, while social-work practitioners complete on-site interventions based on human-centered demands within the field. Looking ahead, community anti-fraud work for the elderly shall adhere to the people-oriented principle, be rooted in practical community-field conditions, enrich grassroots-service resources while optimizing technical tools, improve cross-department-collaboration mechanisms, and build a comprehensive protection network jointly driven by technologies, services and institutions. Limited to a single urban community, this study has a small sample scope. Its conclusions need further verification through more community-based practices. Future research can expand investigations into township-level communities and continuously improve implementation paths for technology-service coupling.

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] Li Q X. *Research on Paths of Improving the Elderly's Digital Literacy to Cope with Telecom-Fraud from the Perspective of Social Work*. University of Chinese Academy of Social Sciences, 2025.
- [2] Wu Y P. *Research on Group-Work Intervention for Raising Anti-Fraud Awareness among Urban Elderly Residents — A Case Study of Community W in City S*. Shenyang University of Chemical Technology, 2024.
- [3] Lin Y. *Research on Innovation of Social-Work-Service Modes for Smart-Community-Based Elderly Care under the Background of Digital Empowerment*. *Society and Public Welfare*, 2026(13): 51-53.
- [4] Xie J. *Research on the Application of Digital-Intelligent Technologies in Social Work for the Elderly*. Guangdong University of Technology, 2024.
- [5] Li C H. *Research on Age-Adaptation of Community-Services in the Context of Smart-Community Construction: A Case Study of City S*. Shenyang Normal University, 2023.
- [6] Wang Y F. *Research on Pension-Fraud Prevention and Control from the Perspective of Community Governance*. People's Public Security University of China, 2024.
- [7] Zhang Y X. *Research on the Elderly's Fraud-Exposure Risks and Rights-and-Interests-Protection Strategies*. Sichuan Academy of Social Sciences, 2025.
- [8] Bai H. *Research on Group-Work Intervention for Improving the Elderly's Ability to Guard against Financial Fraud — A Case Study of Elderly Residents in Community C of Chengdu*. Southwestern University of Finance and Economics, 2025.