



Digital Wellbeing in the Silver Economy: The Case for a Senior Mode on Chinese Short-Video Platforms

Sihan Zhang* and Juan José Lull Noguera

Department of Business Management, Universitat Politècnica de València, Spain

Abstract

China now has more than 300 million Internet users aged 50 and over, and older users' average daily online time has surpassed that of every other age cohort. Yet the “Elder Mode” currently offered by mainstream short-video platforms is confined to interface-level adjustments—font size, volume, navigation—and leaves the algorithmic back-end untouched. Adopting a critical qualitative research paradigm, this study constructs an empirical database of 21 cases (drawn from court judgments, prosecutorial announcements, and in-depth investigative reporting in mainstream media; covering 2020–2025) and identifies three patterns of exploitation: (a) e-commerce exploitation through a “digital lemon market” for overpriced inferior goods; (b) cognitive exploitation via pseudo-scientific content, mystical marketing, and predatory education; and (c) emotional exploitation through alienated parasocial interaction (PSI) and fictive kinship. The amount lost in a single case ranges from tens of thousands of yuan to RMB 3.5 million and, in commercial-fraud cases, over RMB 200 million—all of which exceed the interception perimeter of conventional bank risk control. Building on these findings, the paper proposes a three-layer “Deep Elder Mode” governance framework: algorithmic de-weighting and knowledge tracing at the content layer; cross-generational co-signing verification at the financial layer; and positive nudging combined with online-to-offline (O2O) coordination at the social layer. The paper repositions “Digital ESG” as the institutionalized expression of corporate social responsibility in the algorithmic era, breaking out of the zero-sum framing in which protecting vulnerable groups must come at the cost of business interests, and offering a culturally adaptable scheme for inclusive technology governance in aging societies.

Keywords: older adults, algorithmic exploitation, parasocial interaction, Deep Elder Mode, Digital ESG

1. Introduction

China now has more than 300 million Internet users aged 50 and over. The silver-haired population, once dismissed as “digital outsiders,” has rapidly become a core user base of platforms such as Douyin and Kuaishou—with average daily online time even exceeding that of younger cohorts. But the surge in participation conceals a set of structural tensions. The

business logic of short-video platforms is rooted in the attention economy, and algorithms are optimized around just two objectives: time-on-platform and engagement rate. When this capture system is aimed at older users, what it exploits is not only their limited digital literacy, but also something far harder to repair through technology alone: the “structural loneliness” produced by retirement, widowhood, and adult children living far away—an emotional void that offline social channels rarely fill.

Domestic platforms have not been entirely unresponsive. Successive iterations of the “Elder Mode” have introduced front-end changes such as larger fonts, louder volume, and simplified navigation, yet they have barely touched the back-end algorithmic mechanisms that drive exploitation. Through a systematic examination of 21 cases, this study identifies three exploitation pathways that already lie beyond the reach of conventional risk control. Single-case losses run from tens of thousands of yuan to over RMB 200 million, and the funds typically flow out as “voluntary loans” or “gifts to family,” leaving existing payment-side controls unable to intervene.

1.1 Theoretical Framework and Literature

1.1.1 The Digital Silver Divide and Vulnerability

Seifert et al. (2021) define the “digital silver divide” as the systematic inequality older adults face in accessing and effectively using digital tools. Cotten et al. (2013) found that more frequent Internet use was significantly associated with reduced loneliness among older adults, suggesting that digital connectivity can serve a social-compensation function. At the same time, older users’ vulnerability in information evaluation is pronounced: Shao et al. (2019) show that the interaction of cognitive aging, low digital literacy, and social isolation jointly raises the risk of online fraud.

1.1.2 The Attention Economy and Algorithmic Exploitation

Short-video platforms’ business logic rests on the attention economy. Pariser’s (2011) “filter bubble” theory describes how personalized recommendation algorithms enclose users within information environments highly homogeneous with their existing preferences. The effect is amplified for older users: once the algorithm detects a preference for emotional, health-related, or financial content, it continues to raise the recommendation weight for similar content, producing a positive-feedback loop. Empirical evidence from Xu et al. (2025) shows that intelligent recommendation, combined with flow experience, significantly intensifies platform dependence among middle-aged and older Chinese users.

1.1.3 Parasocial Interaction and its Algorithmic Alienation

Horton and Wohl (1956) defined the one-way emotional bond between audiences and media figures as parasocial interaction (PSI), a form of “intimacy at a distance.” The intervention of short-video algorithms has changed its character: PSI has been redesigned from a spontaneous psychological tendency into a capitalized tool. Streamers address older viewers as “Mother” or “Father,” stage family-ethics melodramas, and promise elder-care obligations—actively constructing fictive kinship and precisely activating older viewers’ longing for genuine family connection. McKenna and Bargh (2000) social-compensation hypothesis suggests that individuals disadvantaged in offline social life are more likely to seek emotional compensation through online media. Bao and Joo’s (2025) study of Douyin’s PK live-streaming demonstrates that the high-intensity design of interaction rituals significantly drives gift-giving by viewers.

1.1.4 Aging-Friendly Design and Gerontechnology

A substantial body of work in human-computer interaction (HCI) and gerontechnology has examined how to make digital systems usable and acceptable for older adults, documenting perceptual, motor, and cognitive barriers and the value of designing with rather than merely for older people (Czaja et al., 2006; Vines et al., 2015; Vaportzis et al., 2017). Knowles and Hanson (2018) further argue that older adults' non-use of technology often reflects reasoned distrust rather than incapacity. This tradition has concentrated primarily on interface accessibility and usability. The present study shifts attention from interface accessibility to algorithmic vulnerability: the harms documented here originate in the recommender back-end, which access-layer design leaves untouched.

The relevance of this literature to the present study lies less in its specific interface recommendations than in its normative orientation. HCI and gerontechnology research has long emphasized that older adults should not be treated as passive recipients of simplified technology, but as situated users whose choices reflect embodied ability, trust, social context, and life experience. This insight is central to Deep Elder Mode. The proposal advanced here does not seek to intensify paternalistic protection or to remove older users from digital participation. Rather, it extends the participatory and empowerment-oriented logic of aging-friendly design from the visible interface to the less visible algorithmic, payment, and platform-governance layers.

1.1.5 Regulatory Landscape

The framework below is situated within, rather than derived from, an emerging body of platform-accountability law. In China, the Personal Information Protection Law (PIPL; National People's Congress, 2021, art. 24) regulates automated decision-making, while the Anti-Telecom and Online Fraud Law (National People's Congress, 2022, art. 18) empowers payment institutions to delay suspicious settlements. In the European Union, the General Data Protection Regulation (GDPR; European Parliament and Council, 2016, art. 22) limits solely automated decisions, and the Digital Services Act (DSA; European Parliament and Council, 2022, arts. 27 and 38) requires recommender transparency and a non-profiling option.

These frameworks are cited only to define the compliance boundaries for Deep Elder Mode, not to duplicate the design discussion. The operational implications of transparency, consent, data minimization, contestability, trusted-contact models, and cross-jurisdictional implementation are therefore addressed in Section 4.1.2.

1.2 Research Gap and Contribution

Three gaps remain in the existing literature. The first is one of analytical level: research has stayed at the "access layer" and rarely engaged the "algorithmic layer." Studies of aging-friendly redesign have focused on UI optimization and offered little discussion of back-end algorithmic governance. The second concerns scope: PSI research has not yet fully entered the predatory alienation scenarios of short-video live streaming, which constitutes the theoretical focus of this paper. The third is the absence of a non-zero-sum perspective in governance frameworks: prevailing approaches reduce to single-channel technical interception or regulatory punishment. Taking PSI alienation and structural loneliness as its sociological backbone, this study reconstructs the mechanisms of exploitation at the algorithmic layer; with Digital ESG incentives at its core, it builds a non-zero-sum governance architecture that embeds business incentives within the protective framework. Figure 1 sets out the overall research roadmap.

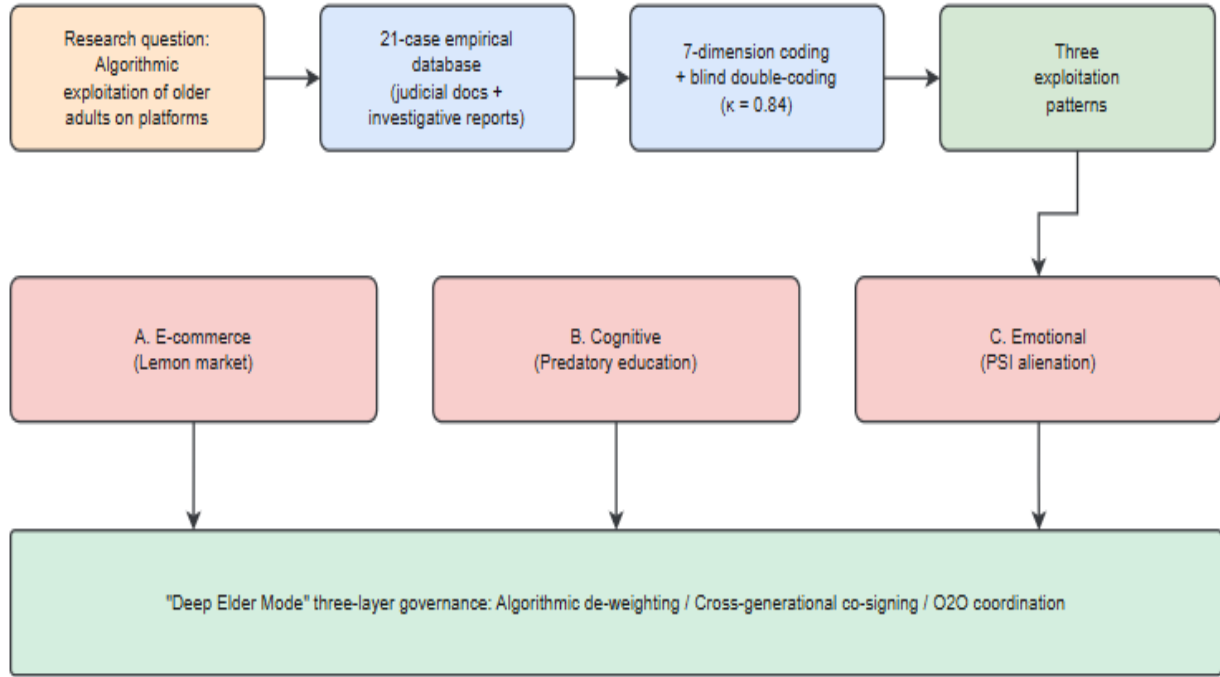


Figure 1. Research roadmap

2. Materials and Methods

2.1 Research Paradigm

This study adopts a critical qualitative research paradigm, with “conceptual framework development based on systematic case analysis” as its core methodological path. Two considerations motivated the choice of a qualitative approach. First, algorithm-driven emotional manipulation is an emerging phenomenon whose mechanisms have not yet reached scholarly consensus, so it lends itself to theory generation rather than hypothesis testing. Second, situational details such as deceptive scripts, money-transfer pathways, and points of risk-control failure are difficult to capture through standardized scales and require in-depth deconstruction of real cases. The work proceeded in two steps: case analysis was used first to build an empirical foundation and identify core exploitation patterns; these patterns then served as problem anchors from which the “Deep Elder Mode” was deduced through engagement with PSI theory and social-compensation theory.

2.2 Case Database Construction

To ensure systematic and replicable case selection, this study applied *ex ante* inclusion criteria rather than *ex post* screening: (i) the contact channel was a short-video platform or an instant-messaging tool to which it directed users; (ii) victims were aged 50 or over, or the case targeted cognitive vulnerabilities specific to older adults; (iii) sources were finalized court judgments, prosecutorial announcements, or in-depth investigative reports in mainstream media; (iv) incidents occurred between 2020 and 2025; and (v) the geographic scope was limited to mainland China. The resulting dataset draws on public judicial documents from courts and prosecutors’ offices in Zezhou, Songjiang, Danzhou, Yidu, Jiangyin, and other localities, alongside investigative reporting from outlets including CCTV, The Paper, and Caixin Media—constituting a triangulated corpus of “judicial documents plus investigative journalism.” Table 1 reports the dominant source-type distribution of the 21-case corpus.

Table 1. Source distribution of the 21-case corpus

Dominant public source type	Cases	Share of corpus	Traceability function
Finalized court judgments / civil decisions	4	19.0%	Provide legally established facts, victim profiles, and transaction details.
Prosecutorial announcements	2	9.5%	Provide official summaries of criminal patterns, case scale, and prosecution logic.
In-depth investigative reporting / media-documented public cases	15	71.5%	Capture emerging or underreported mechanisms and supply contextual detail beyond adjudicated records.
Total	21	100%	All cases were required to have public traceability and were triangulated where possible.

Note. Source type refers to the dominant public source used for traceability; several cases were triangulated across more than one source when available.

Sample size was judged against the standard of theoretical saturation (Glaser & Strauss, 1967): saturation is reached when new cases no longer yield new conceptual dimensions. During coding, the core dimensions of the three exploitation patterns (script strategy, risk-control evasion path, victim profile) ceased to generate new sub-categories from the 16th case onward, and Cases 17–21 served primarily a confirmatory function. Figure 2 summarizes the case-selection flow from the initial public-source universe to the final 21-case corpus.

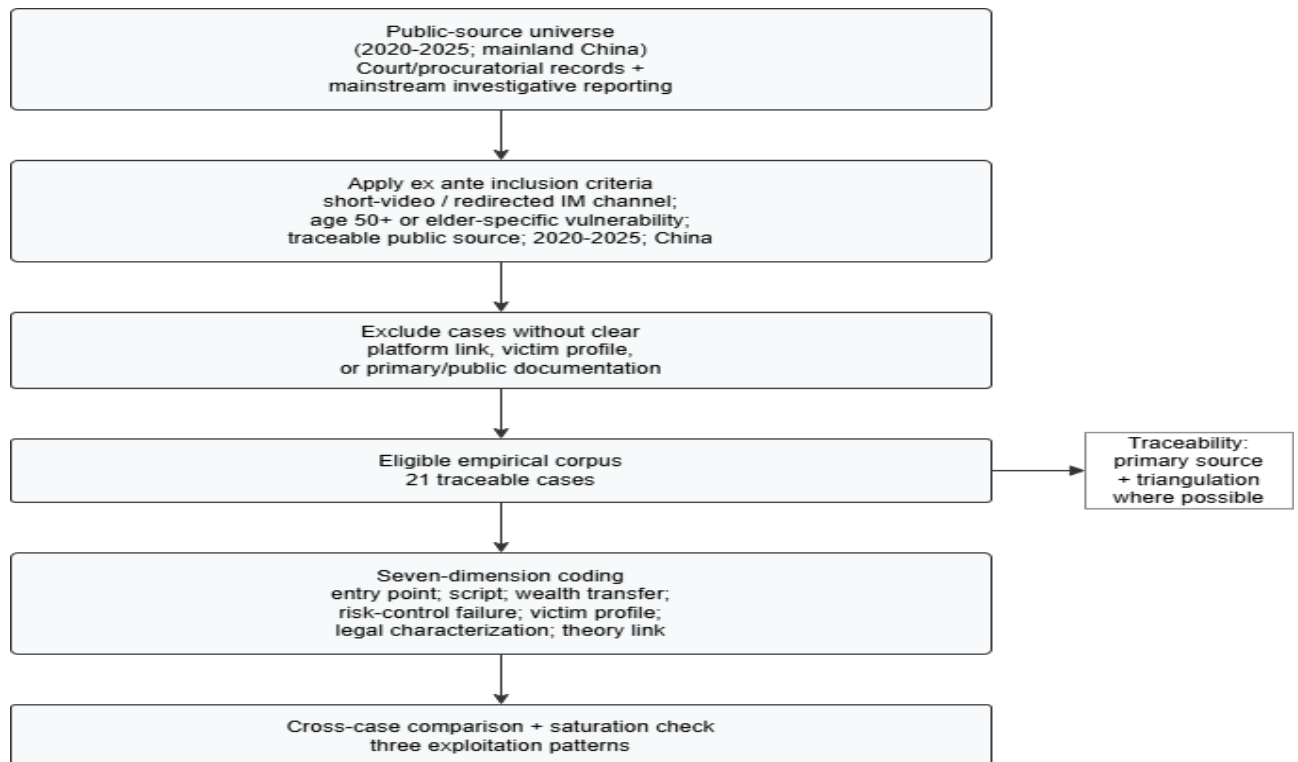


Figure 2. Case-selection flow for the 21-case corpus

2.3 Case Coding and Reliability

Following the qualitative data analysis framework of Miles et al. (2014), this study built a seven-dimension coding matrix: (i) entry point; (ii) manipulation script; (iii) wealth-transfer pathway; (iv) point of risk-control failure; (v) victim profile; (vi) legal characterization; and (vii) theoretical correspondence. After case-by-case coding, inductive thematic analysis was used for cross-case comparison, yielding the three exploitation patterns (Table 2; Figure 4). The patterns are not mutually exclusive—some cases display features of more than one—but are distinguished by the dominant manipulation mechanism.

To strengthen the objectivity of coding, this study introduced double independent coding and inter-coder reliability testing. After the first author completed an initial coding pass, an independent researcher who had not participated in research design blind-coded all 21 cases against the same operational definitions. Cohen's kappa coefficients across the seven dimensions ranged from 0.78 to 0.91, with an overall mean of 0.84—meeting the threshold for “substantial agreement” as defined by Landis and Koch (1977).

2.4 Source Traceability and Sampling Bias

To ensure traceability, each case was anchored to at least one primary judicial or prosecutorial document and, where possible, triangulated against independent investigative reporting; cases failing this standard were excluded. A complete coding matrix is provided in Appendix A.

Reliance on adjudicated cases entails a known and directional bias. Judicial records over-represent incidents that were detected, reported, prosecuted, and convicted, while under-representing low-value, high-frequency exploitation and emotionally driven victimization. Accordingly, the purpose of this study is mechanism identification rather than prevalence estimation. The cases illustrate how exploitation operates, while theoretical saturation rather than case frequency underwrites the analytical claims.

Two additional steps were taken to prevent underreporting bias from distorting the analytical claims. First, the monetary amount involved in each case was treated as contextual information rather than as a proxy for empirical importance; small-value but high-frequency schemes were not considered less theoretically relevant than large-loss cases. Second, cases were compared by mechanism rather than by frequency. The study therefore does not infer that the three patterns are statistically representative of the broader population of older users. Instead, it uses legally and journalistically traceable cases to identify recurrent mechanisms of exploitation that can be examined further through surveys, platform behavioral data, or experimental audit designs. This caution is consistent with existing evidence that financial fraud against older adults is substantially underreported; therefore, publicly traceable legal and media cases should be read as a conservative source for mechanism identification rather than as a complete measure of victimization (Morgan & Tapp, 2024).

3. Results

Empirical evidence across the 21 cases shows that this deeper form of digital exploitation now lies wholly outside the interception perimeter of conventional payment-side risk control. Table 2 summarizes the distribution and scale of the three patterns; Figure 3 presents the distribution of case counts and financial amounts across the three patterns; Figure 4 maps their mechanism pathways. All three share a four-stage structure: entry point – manipulation core – wealth transfer – risk-control evasion.

Table 2. Distribution of the three exploitation patterns across 21 cases

Pattern	Cases	Core manipulation mechanism	Typical scale of loss
A. E-commerce	8	Health anxiety + information asymmetry + forged credentials	Several million to over RMB 200 million
B. Cognitive	9	Predatory education + authority persona + sunk-cost trap	Tens of thousands to over RMB 13 million
C. Emotional	4	PSI alienation + harvesting of loneliness + incremental psychological breach	Tens of thousands to RMB 3.5 million

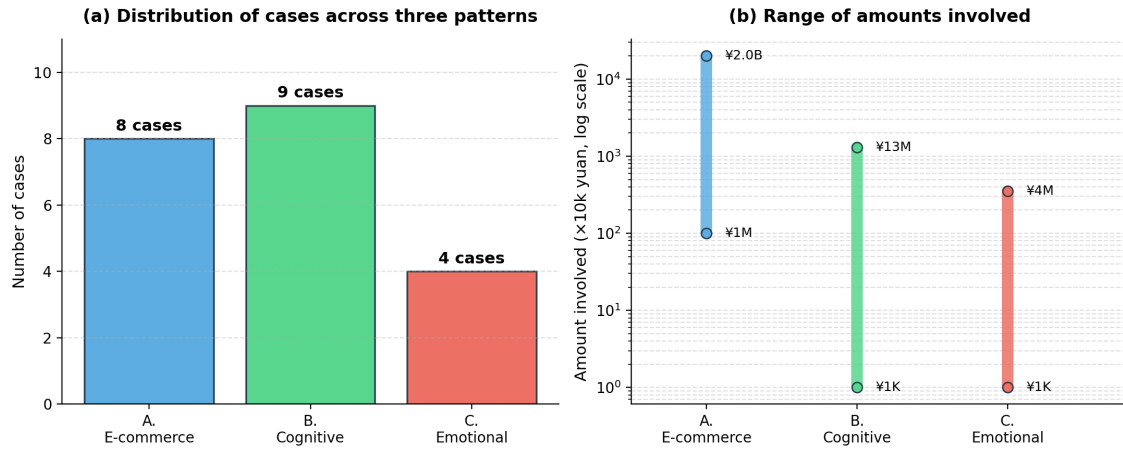


Figure 3. Distribution of case counts and amounts involved

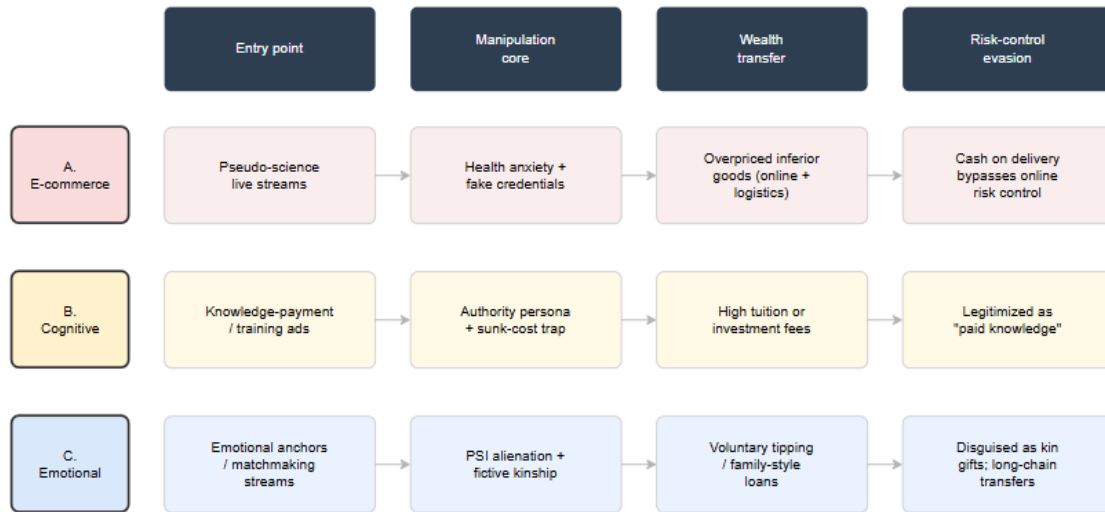


Figure 4. Mechanism-path comparison across the three exploitation patterns

3.1 E-commerce Exploitation

Live-streaming rooms selling antiques, jade, and health products are typical scenes for Pattern A, where steep professional information barriers create a “digital lemon market” (Akerlof, 1970). One common script involves emotional streamers who fabricate family-ethics conflicts to draw older audiences in, then use “fan-only deals” to sell low-grade plastic posing as jade. Other streamers first earn trust by mediating real or staged family disputes, then induce viewers to spend more than RMB 100,000 of their savings on defective jade. Health products are often sold through bait-and-switch schemes. In the “Sanhao Direct Supply” case, a criminal ring

repackaged propolis with an ex-factory price of RMB 5.8 as a “miracle drug,” involving more than RMB 92.64 million; in another case, a “miracle” blood-sugar drug accumulated over RMB 200 million in losses, with offenders bypassing every form of online risk control by relying on cash-on-delivery (COD) settlement. The shared feature of this pattern is that transactions are completed along a hybrid path stretching from online algorithmic recommendation to offline logistics-based settlement—a path that the risk-control systems of platforms and banks cannot penetrate.

3.2 Cognitive Exploitation

On the pseudo-science track, some MCN agencies repackaged unqualified personnel as “first-class health practitioners” and sold capsules costing RMB 18 at a retail price of RMB 499. On the mysticism track, accounts operating under banners such as “Chinese classical studies” or “I-Ching divination” used free face-reading to manufacture panic about an impending “disaster of blood,” then upsold a RMB 2,680 “master class” to lift the curse. Predatory financial education is the largest sub-category within Pattern B: in one short-video sales-training case, fabricated promises of platform traffic support extracted more than RMB 13.09 million from over 2,400 older students, and a scam dressed up as “AI-powered cross-border e-commerce monetization” induced victims to keep doubling down, with one individual losing RMB 160,000. Such exploitation cloaks itself in the legal language of “paid knowledge” or “entrepreneurial investment,” making it nearly impossible for platform or bank anti-fraud alerts to fire.

3.3 Emotional Exploitation

Emotional exploitation typically involves deep psychological manipulation that targets structural loneliness with precision. The manipulation pathway falls into two sub-types. The first is celebrity-identity impersonation combined with stepped small-amount probing: in multiple fake-celebrity fraud cases, perpetrators first lowered psychological defenses with small gifts, then set escalating membership thresholds of RMB 299, RMB 399, up to RMB 22,888—a salami-slicing tactic that kept early transfers below any risk-control threshold. The second sub-type is long-cycle emotional investment combined with fictive kinship. In a case heard by the Songjiang District Court, a male streamer addressed a 70-year-old woman living alone as his “godmother,” promised to provide elder-care, and then “borrowed” more than RMB 550,000 via WeChat under invented pretexts of cancer treatment and being “hunted by criminals.” In one online dating group, an older user wired RMB 3.5 million in retirement investments to an online “partner” she had never met. Perpetrators deliberately repackage wealth extraction as “gifts to family” or “voluntary tipping,” and conventional risk-control logic is wholly ineffective against these voluntary, long-chain transfers.

4. Discussion

4.1 The “Deep Elder Mode” Governance Framework

In response to the three exploitation patterns, this study proposes a three-layer governance framework spanning content, financial, and social layers (Figure 5). The guiding principles are active opt-in, data minimization, and digital empowerment—the goal is to disrupt predatory structures, not to constrict older users’ digital autonomy in the name of protection.

Before laying out the layers, one logical question must be addressed. Section 3 attributes exploitation to platforms’ algorithmic recommendation, yet several of this section’s key levers

sit on the financial-payment side. The answer lies in an internal tension within the platform itself. Short-video platforms' business model depends heavily on the attention economy; large-scale algorithmic de-weighting amounts to a restructuring of their core revenue base and, absent mandatory regulation, exposes them to severe commercial backlash. The framework therefore adopts a dual-layer fallback strategy: content-layer de-weighting (4.1.1) functions as the front line of defense, while acknowledging that its enforcement firmness is limited; financial-layer co-signing (4.1.2) acts as a structural “chokepoint” at the wealth-transfer stage, independent of any individual platform’s willingness to police content; and social-layer O2O coordination (4.1.3) addresses structural loneliness at its root.

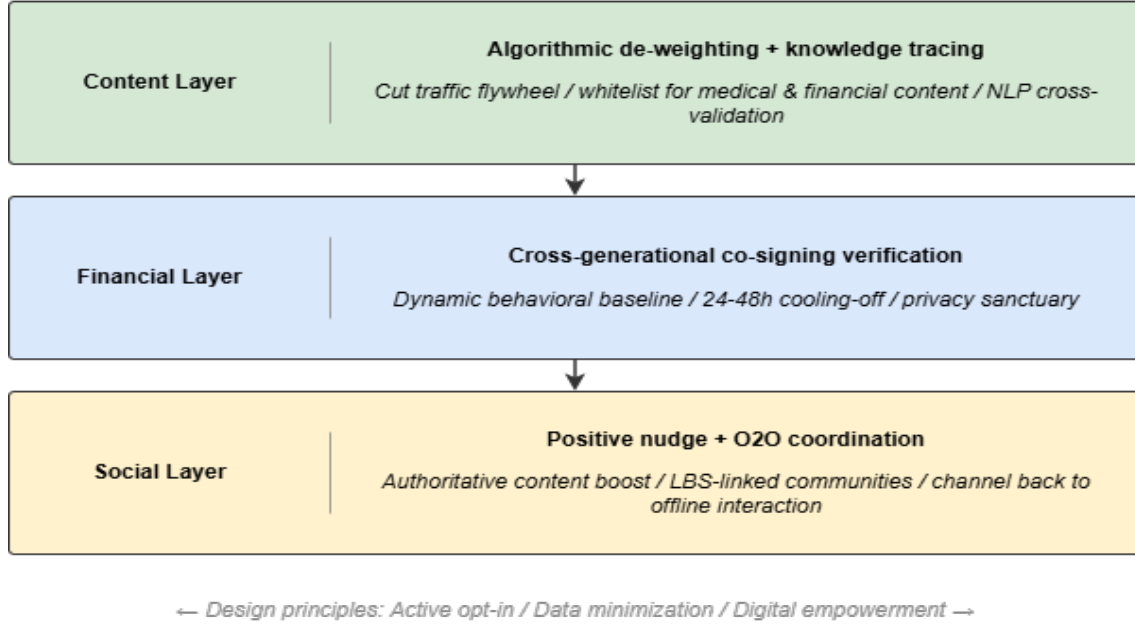


Figure 5. Three-layer governance architecture of the “Deep Elder Mode”

4.1.1 Algorithmic de-Weighting and Knowledge Tracing

To break the vicious cycle in which more extreme content travels more easily, platforms need to revise the objective function of their recommendation algorithms. Two approaches are feasible. The first is to introduce “algorithmic friction” that interrupts the traffic flywheel: content judged to carry high emotional incitement, induced scripts (e.g., “cure-all” claims), or frequent association with low-quality goods has its exposure weight actively reduced within older users’ recommendation pools. The second is to build whitelisting and cross-validation systems for medical and financial content: only accounts holding official credentials may push health guidance to older users, and video text is cross-validated in real time against authoritative knowledge graphs using NLP techniques. When sensational claims that contradict scientific consensus are detected, the content is blocked immediately and an authoritative correction is appended.

4.1.2 Cross-Generational Co-Signing Verification

Conventional single-point payment limits can no longer reconcile consumer autonomy with precise risk control under the dual risks of incremental psychological breach and voluntary exploitation. Drawing on the multi-tier authorization mechanisms used in commercial-bank corporate banking, this study proposes a “cross-generational co-signing verification” model, with the overall flow shown in Figure 6.

Co-signing verification is not a simple transplant of banking practice; it is a sociotechnical design for intergenerational power-sharing and transfer. It converts part of an individual's financial autonomy into the collective decision-making of a family-level “digital community,” and this conversion rests on bidirectional informed consent rather than the unilateral idea that elders “cede authority to children.” Beyond enterprise risk-control logic, cross-generational co-signing thus carries a deeper sociological meaning as “family-scale digital network governance.”

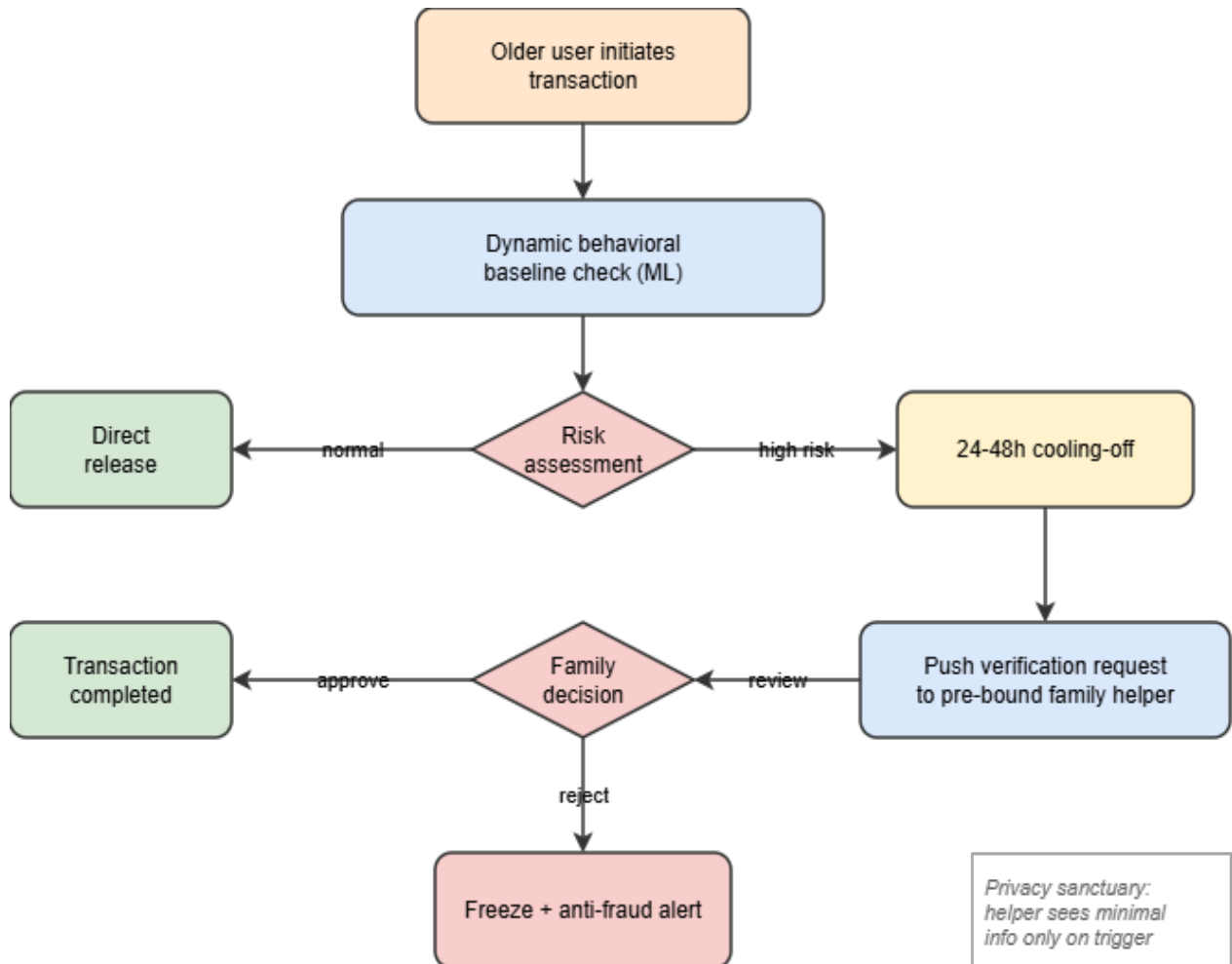


Figure 6. Cross-generational co-signing verification flow

The mechanism has three core components. The first is a dynamic behavioral baseline. Machine learning is used to construct a digital behavior baseline for each older user, capturing routine small-amount spending, frequently used social accounts, and typical geographic patterns; once a fund flow deviates from this baseline—for example, a large gift to an emotional streamer with no prior interaction—penetrative identification is triggered. The second is trigger-based co-signing with a cooling-off period. High-risk transactions trigger a 24–48 hour cooling-off period that disrupts the in-the-moment decision pressure of live streams. During the cooling-off period the system pushes a verification request to a pre-bound family helper: the older user is the “initiator” and the family member the “reviewer.” The third is a privacy sanctuary. Family helpers have no access to routine transactional records and are shown only the minimum necessary information when an exception is triggered; while the older user retains civil capacity, they themselves can set and revise the relevant thresholds.

When family-based digital co-governance relies on cultural norms of filial piety alone without institutional limits, however, this form of care can readily slide into “digital proxy

guardianship,” eroding the dignity of older persons as independent civil subjects. The framework proposed here transforms existing “filial care” into “empowerment-based co-governance”: care exists in an institutionalized, trigger-based, and switchable form, rather than expanding without limit through emotional appeals or moral obligation.

One issue must be confronted directly: bringing enterprise-level risk-control logic down to the household scene inevitably produces secondary emotional friction. As reviewers, family members may, through subjective bias, over-block routine social spending—for example, imposing paternalistic scrutiny on “atypical” outlays such as donations to temples or financial support to distant relatives—while older users, repeatedly denied legitimate spending, may experience intense family conflict that turns intergenerational co-governance into a new form of patriarchal or filial coercion. To preempt this risk, the framework specifies three accompanying constraints. (i) Transparency of review power: every interception record is fully visible to the older user, who may apply for one-click release of any specific threshold. (ii) Third-party arbitration: where the older user and the family helper disagree, a local anti-fraud center or community mediator may step in. (iii) Minimal helper privileges: helpers can only choose to release or reject a transaction; they cannot view the broader transaction context or unilaterally initiate a freeze.

Regarding legal feasibility and cross-jurisdictional risks, the legal feasibility of cross-generational co-signing is jurisdiction-contingent. In the Chinese context, the mechanism can be aligned with anti-fraud risk control and family-based risk sharing, provided that the older user remains the initiator of authorization and retains the ability to revise or withdraw thresholds. In EU-style data-protection regimes, however, the same mechanism would have to be reframed more narrowly as a user-authorized trusted-contact or support-person model. A comparable logic already exists in U.S. financial regulation, where FINRA rules require firms to make reasonable efforts to obtain trusted-contact information and permit temporary holds on disbursements when financial exploitation of specified adults is reasonably suspected (Financial Industry Regulatory Authority [FINRA], 2022a, 2022b). It could not operate as default family access to financial data, because informational self-determination, data minimization, and the right to withdraw consent would be central compliance requirements.

The most serious unintended consequences are not technical but relational. Co-signing could intensify family conflict, enable financial surveillance by adult children, disadvantage older users without close kin, or produce excessive false positives that block legitimate consumption. These risks can be reduced only if the mechanism is optional, revocable, trigger-based, and plural in its choice of reviewer. Older users should be able to appoint a family member, community worker, bank anti-fraud officer, or other trusted person; platforms and payment providers should also maintain human appeal channels and periodic audits of false-positive rates. Thus, co-signing should be understood as a bounded autonomy-support tool, not as digital guardianship.

Table 3. Comparison of the Chinese familism path and the Western digital-individualism path

Governance dimension	Chinese familism path	Western digital individualism path (e.g., GDPR)
Ethical foundation	Family as a risk-sharing unit; “filial piety” includes care responsibilities	Individual as an independent civil subject; informational self-determination
Authorization logic	Cross-generational co-signing: older user as initiator, family member as reviewer	Single-subject authorization: the individual is the sole legal authorizer

Governance dimension	Chinese familism path	Western digital individualism path (e.g., GDPR)
Data access	Contextual disclosure: only the necessary information is disclosed in exception scenarios	Strict minimization: no third-party access without explicit consent
Exit mechanism	Dynamic thresholds set and switched off by the user	Right to withdraw and right to erasure as fundamental rights
Integration path	Preserve family risk-sharing while institutionalizing filial piety as trigger-based and switchable	Introduce three guardrails: necessity-based minimization, explicit consent, and easy exit

4.1.3 Positive Nudging and O2O Coordination

Truly aging-friendly governance must also reduce the cognitive vulnerability that arises from structural loneliness. Once the traffic flywheel for fraud-related and low-quality content has been cut, the algorithmic system should actively deliver “information feedback”: it should establish direct data connections with the National Health Commission, the National Anti-Fraud Center, and mainstream media, and assign the highest distribution weight to officially certified health-literacy content, anti-fraud guidance, and high-quality cultural content (such as opera and documentary). “Value orientation” should replace time-on-platform as the central optimization signal.

A parallel pathway is to use digital technology to guide older users back into real-world social interaction. Platforms should open APIs to local communities, universities for older adults, and elder-care institutions, and use location-based services (LBS) to push offline cultural and recreational events, free clinics, and senior-university enrollment information; one-click registration or navigation should be embedded directly into the content stream. Table 4 summarizes how the three governance layers map onto the three exploitation patterns.

Table 4. Mapping of the three governance layers to the three exploitation patterns

Exploitation stage	Governance mechanism	Intervention effect
Content reach: high-risk video exposure	Algorithmic de-weighting and knowledge tracing	Cuts the traffic flywheel; whitelisting and cross-validation for medical and financial content
Wealth transfer: voluntary transfers and stepped tipping	Cross-generational co-signing verification	Cooling-off and family authorization on anomalous transactions disrupt in-the-moment decision pressure
Psychological substrate: structural loneliness	Positive nudging and O2O coordination	Prioritizes authoritative and cultural content; uses LBS to channel virtual companionship into offline community life

4.1.4 From Framework to Deployment

The proposed framework is intended as a staged governance model rather than a single intervention. Initial deployment may focus on content-layer de-weighting and social-layer coordination, while financial-layer co-signing remains optional and user-controlled. Effectiveness should be assessed through both protective and autonomy-related indicators,

ensuring that reductions in exploitation are not achieved at the expense of older users' rights and independence.

These layers can be evaluated through a staggered pilot comparing the Deep Elder Mode with the existing Elder Mode, using high-risk-content exposure, fraud losses, and wellbeing (e.g., UCLA-3 loneliness) as outcomes. For ethical reasons, the control condition should remain the existing Elder Mode rather than an unprotected feed, and participation should be opt-in and revocable.

More specifically, deployment should proceed from low-intrusion to high-intrusion measures. At the content layer, the first pilot can target de-weighting for high-risk health, financial, and emotional-manipulation content among older users who have voluntarily enabled Elder Mode. At the financial layer, platforms and payment institutions can then introduce optional transaction friction, including warning prompts, cooling-off periods, and user-defined co-signing thresholds. At the social layer, verified health information, anti-fraud education, local community activities, and senior-university resources can be integrated into recommendation flows.

Operational evaluation should combine protective and autonomy-related KPIs. Protective indicators may include exposure to high-risk content, click-through rates for corrected information, high-risk transaction completion rates, confirmed fraud losses, and repeat contact with flagged accounts. Autonomy-related indicators should include false-positive rates, user override rates, appeal success rates, withdrawal rates from Deep Elder Mode, and self-reported trust in the system. Wellbeing outcomes may be measured through short loneliness scales such as UCLA-3 and through participation in offline community activities.

A/B testing is appropriate for low-risk content-ranking interventions, but higher-intrusion financial features should use opt-in pilots with explicit consent and human review. This staged evaluation design ensures that the reduction of exploitation is assessed together with the preservation of autonomy, privacy, and dignity.

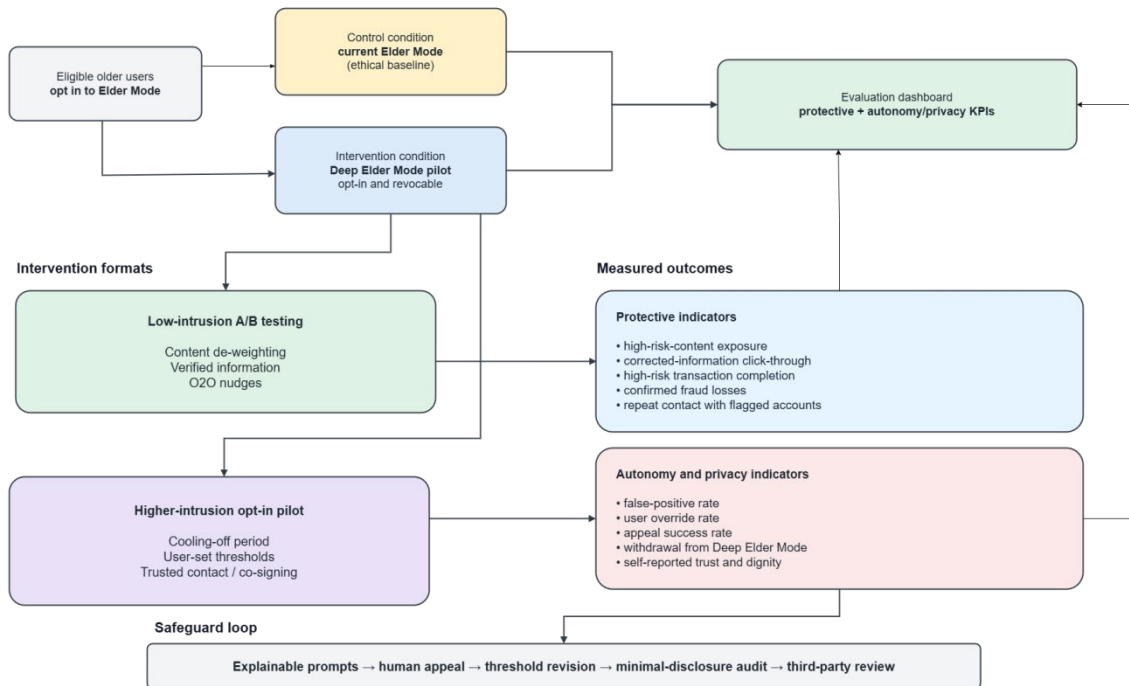


Figure 7. Staged evaluation design and autonomy safeguards for Deep Elder Mode deployment

Table 5. Implementation roadmap, measurable KPIs, and safeguards for Deep Elder Mode deployment

Stage / layer	Core action	Evaluation KPIs	Autonomy/privacy safeguards	Pilot and A/B design
Stage 1: Content layer	De-weight high-risk health, financial, and emotional-manipulation content; increase verified health and anti-fraud information.	Exposure rate to high-risk content; correction-click rate; repeat exposure to flagged accounts; engagement with verified content.	Explainable warning prompts; user appeal channel; no forced activation; false-positive review.	Existing Elder Mode vs. Deep Elder Mode content feed; low-intrusion A/B testing.
Stage 2: Financial layer	Introduce trigger-based cooling-off, warning prompts, user-defined thresholds, and optional trusted-contact or co-signing review.	Confirmed fraud-loss reduction; high-risk transaction completion rate; override rate; appeal success rate; withdrawal rate.	Active opt-in; revocable thresholds; minimal disclosure to trusted contacts; no access to routine transaction history; human review.	Opt-in pilot for anomalous transactions; no compulsory co-signing.
Stage 3: Social layer	Redirect users to verified well-being content, anti-fraud education, offline community activities, free clinics, and senior-university resources.	Offline activity sign-ups; click-through rate for community resources; UCLA-3 loneliness score; engagement with public-interest content.	LBS opt-in; no continuous location tracking; user-controlled recommendation preferences; voluntary participation.	Staggered community rollout across selected localities or user groups.
Stage 4: Accountability layer	Publish Digital Wellbeing Reports and conduct third-party audits of Elder Mode interventions and complaint handling.	Audit completion rate; complaint resolution time; transparency-report completeness; disclosure of protection-related indicators.	Public reporting; independent review; contestability of automated interventions; separation from commercial engagement metrics.	Before-after platform-level comparison and periodic external audit.

4.2 Integrating the Design Principles

The Chinese familism path and the Western digital-individualism path are not opposed but emphasize, respectively, family-level risk-sharing and respect for individual boundaries. This study argues for a shift in governance logic from paternalistic protection to autonomy-based empowerment, organized around three principles: active opt-in (Elder Mode must not be forcibly enabled), graduated dynamic thresholds (users themselves set the amounts and behavioral preferences that trigger family verification), and a technical-level privacy sanctuary (data minimization and on-device processing). In a Chinese context, these principles serve to put boundaries around familism; in an EU context, they introduce the possibility of family-level co-bearing into digital individualism.

4.3 Limitations and Cross-Cultural Comparisons

This study is subject to a cultural limitation, as the sample draws exclusively from Chinese judicial and media cases.

Herrera and Hastings (2024) examined romance scam trends in the United States across the period 2004–2023, drawing on multiple public data sources including web searches and news reports. Their findings indicate that, despite a decline in official reports, scam activity continued to rise—a pattern attributed largely to chronically low victim reporting rates, with the U.S. Federal Trade Commission (FTC) estimating that only 2% to 6.7% of elderly fraud cases are formally reported. This cross-cultural regularity lends support to the present study’s reliance on judicial cases, while simultaneously confirming that such sources inevitably underrepresent the true scale of victimization.

Soares and Lazarus (2024), employing a documentary analysis of fifty convicted romance fraud offenders in Nigeria—a methodology comparable to that of the present study—found that exploitation in Western contexts operates predominantly through direct interpersonal manipulation, with 56% of victims originating from the United States. By contrast, the present study reveals that elderly Chinese users are primarily targeted through algorithm-driven emotional and consumption inducement on short-video platforms. This distinction highlights a fundamental difference in fraud mechanisms across cultural contexts, and underscores the theoretical relevance of the familism-versus-individualism framework proposed in this study. Future research should extend this inquiry to short-video platform users across diverse cultural settings, in order to assess the cross-cultural applicability of the proposed three-layer Deep Elder Mode governance framework.

4.4 Digital ESG as a Tech-Ethics Framework

In the short term, the Deep Elder Mode may reduce the profits platforms extract from low-quality consumption. This study offers a non-zero-sum proposition for digital governance in aging societies: build an ethics-based governance framework grounded in Digital ESG.

Digital ESG, as used here, is not a purely financial-incentive instrument but the institutionalized expression of corporate social responsibility in the algorithmic era. Its core is to translate the abstract slogan of “tech for good” into observable algorithmic-behavior indicators. A platform’s investment in protecting older users—algorithmic de-weighting, subsidies for high-quality content, R&D on co-signing mechanisms—should be made visible, verifiable, and accountable through ESG ratings, third-party ethical audits, and a public Digital Well-Being Report. When the degree of protection a platform extends to cognitively vulnerable users becomes an indicator in its overall evaluation, algorithmic design shifts from a single business-maximization logic to a multi-objective optimization that also weighs user well-being. Linkages with green-credit interest rates, credit lines, and other financial-market mechanisms are treated here as auxiliary pathways for embedding ethical consensus, not as the primary driver: the legitimacy of Digital ESG as a tech-ethics framework stands on its own, even without such financial incentives.

5. Conclusion

This study analyzes the deeper digital risks that older users face on short-video platforms in the context of China’s silver economy. The Deep Elder Mode proposed here—integrating algorithmic de-weighting, cross-generational co-signing, and O2O coordination—marks a shift in aging-friendly redesign from mere usability improvements to safety and well-being protections at the underlying logic of the system.

Theoretically, the paper repositions Digital ESG as the institutionalized expression of corporate social responsibility in the algorithmic era and offers a non-zero-sum perspective on platform governance; it also lifts cross-generational co-signing from a financial operation to a

sociological concept of family-scale digital network governance, engaging the tension between Chinese family ethics and digital individualism. Practically, the paper offers a transferable governance blueprint for inclusive technology design in aging societies, and the dual-layer fallback logic suggests an interdisciplinary route for cross-border digital fraud protection.

More broadly, the contribution of Deep Elder Mode is not a claim that one institutional design can be directly transplanted across jurisdictions. Rather, it offers a jurisdiction-sensitive governance template: in China, it can build on family-based risk sharing and anti-fraud infrastructure; in EU-style regimes, it must be redesigned around explicit consent, trusted contacts, minimal disclosure, and contestability. The transferable element is therefore not co-signing as such, but the broader principle of moving aging-friendly design from interface accessibility to algorithmic, financial, and social safeguards.

A further limitation of this study concerns its reliance on judicially verified cases. Given the well-documented low reporting rates associated with online fraud—particularly among elderly victims—the cases that reach the judicial system represent only a fraction of actual victimization. Consequently, the three exploitation models identified in this study may underestimate the true breadth and diversity of algorithm-driven fraud targeting older users. This limitation points to the need for future research to complement case-based analysis with user surveys and platform behavioral data, so as to more comprehensively assess the digital risk exposure of elderly users on short-video platforms.

As an exploratory conceptual-framework study, this work has two additional limitations. First, it lacks large-scale empirical data with which to quantitatively evaluate the interception success rate of algorithmic de-weighting in real-world environments. Second, the compliance boundaries of cross-generational co-signing under different legal regimes such as the GDPR require deeper legal analysis. In addition, owing to the ethical limits of data collection and platforms' terms of service, this study could not directly capture the original interaction corpus inside live-streaming rooms, and the secondary judicial documents on which it relies may carry structural discourse bias. Future research should advance along three lines: testing the suppressive effect of de-weighting algorithms on "infodemic" transmission through simulated environments or randomized controlled experiments; using computational social-science tools on first-party live-streaming corpora—where lawful access can be obtained—to subject the manipulation scripts identified here to a larger-scale robustness test; and examining the feasibility boundaries of cross-generational co-signing and Digital ESG mechanisms across the regulatory regimes of the European Union, East Asia, and North America.

References

- Akerlof, G. A. (1970). The market for "lemons": Quality uncertainty and the market mechanism. *Quarterly Journal of Economics*, 84(3), 488–500. <https://doi.org/10.2307/1879431>
- Bao, H., & Joo, H. (2025). "I should pay": Interaction ritual presentation in PK live streaming. *Symbolic Interaction*, 48(1), 69–90. <https://doi.org/10.1002/symb.1217>
- Cotten, S. R., Anderson, W. A., & McCullough, B. M. (2013). Impact of Internet use on loneliness and contact with others among older adults: Cross-sectional analysis. *Journal of Medical Internet Research*, 15(2), e39. <https://doi.org/10.2196/jmir.2306>
- Czaja, S. J., Charness, N., Fisk, A. D., Hertzog, C., Nair, S. N., Rogers, W. A., & Sharit, J. (2006). Factors predicting the use of technology: Findings from the Center for Research and Education on Aging and Technology Enhancement. *Psychology and Aging*, 21(2), 333–352. <https://doi.org/10.1037/0882-7974.21.2.333>

- European Parliament and Council. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council: General Data Protection Regulation. *Official Journal of the European Union*. <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
- European Parliament and Council. (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services: Digital Services Act. *Official Journal of the European Union*. <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng>
- Financial Industry Regulatory Authority. (2022a). FINRA Rule 4512: Customer account information. *FINRA Manual*. <https://www.finra.org/rules-guidance/rulebooks/finra-rules/4512>
- Financial Industry Regulatory Authority. (2022b). FINRA Rule 2165: Financial exploitation of specified adults. *FINRA Manual*. <https://www.finra.org/rules-guidance/rulebooks/finra-rules/2165>
- Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research*. Aldine.
- Herrera, L. D., & Hastings, J. (2024). The trajectory of romance scams in the U.S. In *2024 12th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1–6). IEEE. <https://doi.org/10.1109/ISDFS60797.2024.10527224>
- Horton, D., & Wohl, R. R. (1956). Mass communication and para-social interaction: Observations on intimacy at a distance. *Psychiatry*, 19(3), 215–229. <https://doi.org/10.1080/00332747.1956.11023049>
- Knowles, B., & Hanson, V. L. (2018). The wisdom of older technology (non-)users. *Communications of the ACM*, 61(3), 72–77. <https://doi.org/10.1145/3179995>
- Landis, J. R., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics*, 33(1), 159–174. <https://doi.org/10.2307/2529310>
- McKenna, K. Y. A., & Bargh, J. A. (2000). Plan 9 from cyberspace: The implications of the Internet for personality and social psychology. *Personality and Social Psychology Review*, 4(1), 57–75. https://doi.org/10.1207/S15327957PSPR0401_6
- Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3rd ed.). SAGE.
- Morgan, R. E., & Tapp, S. N. (2024). *Examining financial fraud against older adults*. National Institute of Justice. <https://nij.ojp.gov/topics/articles/examining-financial-fraud-against-older-adults>
- National People’s Congress. (2021). 中华人民共和国个人信息保护法 [Personal Information Protection Law of the People’s Republic of China]. https://en.spp.gov.cn/2021-12/29/c_948419.htm
- National People’s Congress. (2022). 中华人民共和国反电信网络诈骗法 [Anti-Telecom and Online Fraud Law of the People’s Republic of China]. https://en.moj.gov.cn/2023-12/15/c_948363.htm
- Pariser, E. (2011). *The filter bubble: What the Internet is hiding from you*. Penguin Press.
- Seifert, A., Cotten, S. R., & Xie, B. (2021). A double burden of exclusion? Digital and social exclusion of older adults in times of COVID-19. *The Journals of Gerontology: Series B*, 76(3), e99–e103. <https://doi.org/10.1093/geronb/gbaa098>

- Shao, J., Zhang, Q., Ren, Y., Li, X., & Lin, T. (2019). Why are older adults victims of fraud? Current knowledge and prospects regarding older adults' vulnerability to fraud. *Journal of Elder Abuse & Neglect*, 31(3), 225–243. <https://doi.org/10.1080/08946566.2019.1625842>
- Soares, A. B., & Lazarus, S. (2024). Examining fifty cases of convicted online romance fraud offenders. *Criminal Justice Studies*, 37(4), 328–351. <https://doi.org/10.1080/1478601X.2024.2429088>
- Vaportzis, E., Giatsi Clausen, M., & Gow, A. J. (2017). Older adults' perceptions of technology and barriers to interacting with tablet computers: A focus group study. *Frontiers in Psychology*, 8, Article 1687. <https://doi.org/10.3389/fpsyg.2017.01687>
- Vines, J., Pritchard, G., Wright, P., Olivier, P., & Brittain, K. (2015). An age-old problem: Examining the discourses of ageing in HCI and strategies for future research. *ACM Transactions on Computer-Human Interaction*, 22(1), Article 2. <https://doi.org/10.1145/2696867>
- Xu, J., Ramayah, T., Arshad, M. Z., Ismail, A., & Jamal, J. (2025). Decoding digital dependency: Flow experience and social belonging in short video addiction among middle-aged and elderly Chinese users. *Telematics and Informatics*, 96, Article 102222. <https://doi.org/10.1016/j.tele.2024.102222>

Appendix A. Empirical Case Database (21 Cases)

This appendix provides the complete coding for all 21 cases analyzed in this study. All cases are drawn from publicly available sources (final court judgments at various levels, prosecutorial announcements, and in-depth investigative reports in mainstream media) covering 2020–2025.

Appendix Table A1. Case identification and theoretical coding

	Case ID / source	Legal characterization	Victim profile	Contact medium	Theoretical alignment
1	2025 Zezhou County Court	Fraud	368 middle-aged and older adults	Short-video stream redirected to WeChat	PSI alienation / celebrity impersonation
2	2023 Short-video sales-training case	Fraud	2,495 victims	Short-video keyword targeting	Predatory education trap
3	2022 Yidu Procuratorate	Fraud	Group aged 50+	Live classes and group chats	Health anxiety as commodity
4	2024 Songjiang District Court	Fraud	70-year-old woman living alone	Live-stream interaction redirected to WeChat	PSI alienation / fictive kinship
5	2025 Danzhou Procuratorate	Fraud / credit-card fraud	Adults aged 60+	Kuaishou financial live-streams	Predatory financial education
6	Kangshibang false-advertising case	Fraud	Group aged 50+	Brick-and-mortar pull groups / live-stream links	Health anxiety as commodity
7	Personal-information infringement case	Infringement of citizens' personal information	Older adults at street markets	Offline outreach stalls	Information gap and cognitive exploitation
8	Consumer-contract dispute case	Civil breach of contract	69-year-old consumer	Online education contract	Predatory education trap

	Case ID / source	Legal characterization	Victim profile	Contact medium	Theoretical alignment
9	False-matchmaking fraud case	Fraud	Single older men	Short-video matchmaking ads	Digital romance scam
10	Jiangyin City Court judgment	Fraud	Older adults with diabetes	TV ads / live streams	Health anxiety as commodity
11	Cross-border e-commerce training case	Fraud	Older adults eager to invest	“Gold-coin withdrawal” ads	Predatory financial education
12	Paid-likes scam	Fraud	Older adults seeking part-time work	Short-video / QQ-group funneling	Cognitive exploitation
13	Mini-drama / clipping scams	Civil / fraud	Adults nearing 70	Free-course funnels	Predatory education / cognitive exploitation
14	Pseudo-science account fake-product case	Fraud	Older adults with health concerns	Short-video pseudo-science accounts	Health anxiety as commodity
15	Classical-studies / fortune-telling live-stream scam	Fraud / consumer fraud	Superstition-prone older adults	Mini-program live-streams	Information gap and mystical marketing
16	“RMB 1 flash sale” funnel case	Consumer fraud	Short-video users	Short-video bait ads	Cognitive exploitation
17	Emotional streamer “ErChen” case	Fraud / false advertising	Emotionally lonely older adults	Emotional-mediation live-streams	PSI alienation
18	Emotional-streamer staged sales	Consumer fraud	Middle-aged and older audiences	Live rooms / short videos	Emotional monetization / lemon market
19	Streamer-jade emotional manipulation case	Consumer dispute / fraud	Retired older adults	Emotional-confession live rooms	PSI alienation
20	Older-adult dating-group scam	Fraud	Divorced or widowed older adults	Social-platform dating groups	Digital romance scam / investment fraud
21	Online wellness / Bigu retreat case	False advertising / unauthorized medical practice	Older adults with chronic illnesses or interest in wellness	Public accounts / wellness groups	Health anxiety as commodity

Appendix Table A2. Manipulation pathways and intervention points

	Manipulation script	Wealth-transfer path	Risk-control failure point	Co-signing intervention point
1	Impersonated a celebrity; used ginseng gifts to build trust; promised earnings via fake “celebrity team” membership	Stepped transfers (RMB 299 to RMB 22,888)	Cross-platform jumps evade single-platform monitoring; small early transfers stay below alert thresholds	Monitor large transfers to new contacts that deviate from the baseline
2	Built an “authoritative mentor” persona; falsely promised	Paid high tuition fees (RMB 13.09 million in total)	Wears the legal cloak of paid knowledge, blurring normal	Whitelist online-training credentials; large transfers to

	Manipulation script	Wealth-transfer path	Risk-control failure point	Co-signing intervention point
	platform traffic support; appealed to learning and earning motives		consumption from fraud	non-credentialed accounts require review
3	Fake medical-research-institute titles; daily “red-envelope” greetings; fabricated curative claims for supplements	Private-message orders to group leaders; receipts via WeChat or corporate accounts (RMB 92.64 million)	Legitimate-looking trading companies route corporate transfers, bypassing personal AML monitoring	Whitelist medical content with NLP cross-validation; trigger alerts on large purchases
4	Male streamer addressed her as “Mother,” positioned himself as her “son” promising elder-care; faked cancer to borrow money	Multiple WeChat transfers under “borrowing” pretexts (over RMB 550,000 total)	Disguise as kin gifts makes long-cycle voluntary transfers hard to flag	Trigger cross-generational verification for high-frequency private transfers to non-whitelist accounts
5	Posed as streamer assistants; built trust via “earn coins by completing tasks” scheme	Induced group red-envelopes; or stole verification codes via screen-sharing	Screen-sharing exploits bypass payment passwords	Forcibly block financial-app calls when high-risk system permissions are invoked
6	Distributed red envelopes in live rooms to evade keyword filters; insinuated curative properties of red yeast capsules	High-priced purchases of ordinary food via agency stores or live rooms (millions of yuan in sales)	Online indoctrination plus offline / agency-store payment; capital flows are dispersed	O2O community coordinated governance; flag high-risk merchants offline
7	Posed as JD.com staff; offered free gifts as bait	No direct fund transfer, but stole phone numbers and verification codes for the black market	Lack of identity verification in the physical setting; limited privacy awareness among older users	Issue a black-market warning when a device receives high-frequency registration verification codes
8	Promised high view counts and “official traffic support”	Pre-paid service fee of RMB 29,800; provider then refused to perform	Typical contract fraud; high cost for older users to seek redress	Set a longer cooling-off period for high-value “account management” contracts with uncertified MCNs
9	Fabricated romantic relationships and demanded money for “wedding supplies”	Multiple demands totaling over RMB 120,000, then blocked the victim	“Romance / marriage” spending is hard to intervene in; social logic camouflages the exploitation	Require co-signing for large transfers to recently added strangers under “marriage / bride-price” pretexts
10	Posed as rehabilitation experts; pitched cheap supplements as miracle drugs for diabetes	Cash-on-delivery via courier (over RMB 200 million)	COD physical settlement bypasses online risk control	Bind logistics data to Elder Mode; alert family members on high-frequency, high-value COD orders
11	Fabricated an “AI cross-border e-commerce store” promising risk-free returns	Cumulative RMB 160,000 transferred to a fake store-services platform	Counterfeit e-commerce interface led victims to believe they were “investing in stock”	Block transfers to corporate accounts of unqualified, fake platforms

	Manipulation script	Wealth-transfer path	Risk-control failure point	Co-signing intervention point
12	Promised commission for likes; required upfront membership fees	Paid ~RMB 100 via QR codes or red envelopes, then blocked	Amount too small (under RMB 200) to trigger AML blocks	Group-chat risk scoring; intercept transactions in groups with high-frequency “cash-back” phrases
13	Promised “barrier-free earnings” from posting videos; lurid mini-dramas to attract clicks	Paid RMB 2,997 in tuition; or induced to enable password-free auto-deduction	Algorithm targets older users; password-free auto-deduction exploits digital blind spots	Disable default password-free payments on older accounts; require separate authorization for recurring subscriptions
14	MCN hired social-media accounts and fabricated “first-class health practitioners” promoting cholesterol-reducing capsules	Inferior capsules costing RMB 18 sold at RMB 499	Operates as gray-zone live-commerce; unit prices fall within normal e-commerce ranges	Knowledge-graph tracing; on detecting non-whitelist “doctors” recommending supplements, surface a refutation
15	Manufactured panic about a “disaster of blood” via free face-reading; promoted “master classes” to lift the curse	Course fees from several thousand to RMB 20,000+	Religious mysticism repackaged as “cultural training,” evading financial regulation	Stepped review of large “paid-knowledge” orders from informal training providers
16	Advertised “RMB 1 flash sale” for branded phones, or low-priced trial finance courses	Induced membership purchases of tens of yuan or follow-on courses of thousands	Sunk-cost trap; the first transaction amount is very small	De-weight ads containing “flash-sale” phrasing in older users’ feeds
17	Hired actors to perform family-ethics dramas (abandoning wives and children) and built a “righteous person” persona	Induced purchases of inferior jade or plastic necklaces from a few thousand to RMB 20,000	In-stream impulse buys; no standard pricing for low-quality crafts	Daily spending caps for high-risk goods (jade / jewelry); cooling-off period on overlimit purchases
18	Scripted family-conflict dramas to extract tips; staged “price-cut” performances	Tips in Douyin coins plus sales of “three-no” cosmetics or e-books	Tips and sales sit within compliance frameworks; “family” rhetoric covers the sale of fakes	Anchor-anomaly complaint risk model; restrict distribution of low-quality goods to Elder-Mode users
19	Used the desire to confide to build trust; induced “repayment of kindness”	Spent over RMB 100,000 of savings on defective jade; or tipped RMB 500,000 of retirement funds	Exploited limited tech literacy; emptied savings after gaining trust	“Anti-addiction caps on large tipping” combined with account-balance fuses for irrational tips
20	Online “partners” never met in person; combined matchmaking with investment indoctrination	Victim covertly transferred RMB 3.5 million	Family awareness lagged; banks often release large interbank transfers from high-net-worth older clients	Apply “dynamic behavior penetration recognition” to large remittances; cross-confirm anomalous accounts

	Manipulation script	Wealth-transfer path	Risk-control failure point	Co-signing intervention point
21	Habit-formation via cash-back check-ins; psychological control via “cure-all” personas claiming lineage	Three-no devices, RMB 13,000 offline fasting, RMB 199,000 advanced courses	Progressive psychological capture from free, to RMB 1, to thousands, to tens of thousands	Trigger anti-fraud alerts when over RMB 100,000 is moved out under “wellness” pretexts