The Risks, Challenges and Governance Logic of Female College Students' Telecom Fraud in the Digital Intelligence Era

Su Chen, Jingjing Xia*

Wuhan Textile University, Wuhan,430200,China

*Corresponding author's email: 13227351607@163.com

Abstract. Telecom fraud in the digital age is characterized by decentralization, anonymization and industrialization, and the risk exposure of female college students has significantly increased. Based on the theory of daily activities and pragmatic identity, it is found that negative externalities in the digital environment give rise to the dilemma of "digital transparency", and criminal gangs carry out precise fraud by relying on algorithmic profiling; Victim cognitive deficits and psychological silos further exacerbate victim vulnerability. In response to issues such as the decline in the effectiveness of traditional governance and the "decontextification" of anti-fraud education, a platform for building a closed-loop governance system of "learning, practicing, preventing, and protecting" based on the National Anti-Fraud Center APP is proposed. By reshaping the functional positioning of the platform and establishing a multi-agent agile response mechanism, it promotes the transformation of campus security governance to an active model of early warning in advance and precise policy implementation.

Keywords: Telecom fraud; Female college students; Risk evolution; Closed-loop governance; Agile Response

1 Introduction

While digital technology is fully embedded in the daily life scenarios of college students, it also increases the possibility[1] of data crawling and precise fraud attacks. According to statistics, women are at a significantly higher risk than men, and female college students have become a key target group of telecom fraud, with the essence of being deceived being the result[2] of the interaction between their own group traits and the digital risk environment. Questionnaire survey data indicated that female college students' fraud scenarios were concentrated in impersonating relatives/teachers (60%), online dating inducements (50%), winning prizes/free prizes (30%), etc. (Figure 1) The harm of fraud is not only reflected in direct property loss and academic interruption, but also may trigger the risk of "secondary chain fraud"; Psychologically, it can lead to intense self-blame and shame in victims, and socially, it can increase the financial burden on families and weaken the trust between parents and children. The effectiveness

T. Chamaratana et al. (eds.), *Proceedings of the 2026 12th International Conference on Digital Humanities and Frontiers in Social Sciences (DHFSS 2026)*, Advances in Social Science, Education and Humanities Research 1031,
https://doi.org/10.2991/978-2-38476-611-6_81

of the traditional localized and decentralized governance model continues to decline, and there is an urgent need to build an all-time defense system to promote the upgrading[3] of anti-fraud governance capabilities in schools.

Fig. 1. Proportion of reasons for female college students being deceived

2 Risk Causes and Vulnerability Assessment of Female College Students Being Deceived

2.1 Social Level: Risk Exposure and Data Distortion Empowered by Technology

(1) Algorithmic profiling of the "digital transparency" dilemma:

In the digital age, the logic of social governance shifts to behavioral prediction, and the all-scenario digital trajectories of female college students are continuously aggregated by algorithms and are in a state of "restricted transparency". Fraudsters can build precise user profiles through illegally obtained data, and women are significantly more[4] likely to be defrauded of large sums of money when they encounter "recruitment part-time" and "credit and wealth management" scams.

(2) "gender-sensitive" traps in identity construction:

The evolution of fraud scripts shows a distinct gender-differentiated design. Criminals often pose as "institutional identities" or "relational identities" and tailor their scripts based on the emotional needs and job-hunting anxiety of female college students, embedding fraud induction into life-like scenarios[5] such as emotional companionship and part-time job applications.

2.2 At the Individual Level: The Victimization Coupling of Cognitive Habits and Situational Psychology

(1)"Immune deficiency" in the cognitive closed loop:

There is a common problem of "knowledge-action break" in risk identification among female college students. The failure to cross-verify information when encountering fraud is the main cause[6] of being deceived, and the cognitive "immune gap"

leads to the complete failure of rational identification mechanisms at key stages of fraud.

(2)The symbiotic mechanism of psychological silencing and victims' stigma:

Fraudsters deliberately cut off the connection[7] between victims and their real-life support networks by creating a sense of urgency, inducing guilt, and forcing confidentiality. The "victim's guilt" at the social level further intensifies the victim's sense of stigma, making them reluctant to seek help and eventually forming a vulnerable loop.

2.3 Institutional: The Mismatch Between the Effectiveness of Governance Mechanisms and Practical needs

(1)The "de-contextualization" bottleneck of traditional anti-fraud education:

There is a paradox of "governance redundancy" and "insufficient effective supply" in current anti-fraud prevention in colleges and universities. Conventional educational content is difficult to resist the professional "brainwashing" rhetoric[7] of fraud gangs, and the flood education lacks practical scenario simulation, which is more likely to induce students' "defense fatigue".

(2)Fragmentation of the response chain and asynchronous governance dilemma:

The campus anti-fraud governance has not yet formed a complete work loop. The core reason for the failure of intelligence early warning is the cross-departmental information barrier[8]. The existing governance is mostly post-event remedial, lacking pre-warning intervention and regular data sharing mechanisms.

3 The Collaborative Governance Path Driven by the National Anti-Fraud Center APP

3.1 Platform Paradigm Shift: Evolution from Technology Terminal to Institutional Trigger

To enhance governance effectiveness, it is necessary to first reshape the functional positioning of this platform and incorporate it into the agile governance framework[9]. The platform integrates massive sample data of telecom fraud crimes with AI intelligent analysis capabilities to provide core technical support for campus fraud prevention. The core logic of its operation is to build a "learn, practice, prevent, protect" four-in-one mechanism, evolving from a single technical defense terminal to a "governance trigger node" that connects schools, police, families, and students, achieving millisecond-level scheduling and aggregation of defense resources, promoting the governance logic to shift from "layer-driven" to "data-driven", and the governance focus to shift from "post-case punishment" to "pre-case intervention".

3.2 Full life Cycle Design: "Learning - Practice - Prevention - Protection" Closed-loop Mechanism

(1)Front-end defense mechanism:

The platform can dynamically monitor high-frequency telecommunication signaling, risky web links and suspicious apps on campus, breaking the basis of precise profiling of fraudsters. When female college students enter high-risk fraud scenarios, the platform initiates stepwise intervention: sending targeted warning prompts in the low-risk stage, awakening their risk awareness through strong pop-ups in the medium-risk stage, and simultaneously sending early warning information to the school security department and family members and scheduling human intervention to dissuade them in the high-risk stage.

(2)Mid-range cognitive remodeling:

For typical gender-bound fraud scenarios, the platform pushes customized simulation confrontation training modules to help female college students form automated risk defense responses through "interactive desensitization" training, filling the cognitive "immune gap".

(3)Back-end closed-loop maintenance:

It builds a full-chain support mechanism after being deceived, focusing on eliminating the psychological isolation and social evaluation pressure of the victims. Integrate the functions of "one-click stop payment", automatic evidence solidification, and reporting process guidance to enhance the efficiency of recovering stolen assets; In collaboration with university psychological intervention centers and social assistance forces, an anonymous "composite assistance" channel was launched to provide an integrated supply of psychological counseling, legal consultation and economic assistance.

3.3 Co-Evolutionary Logic: Agile Responses of Multi-dimensional Agents

The effectiveness of collaborative governance depends on the degree of matching of the interaction logic among schools - police - society - students: police-school cooperation upgrades from "passive response after the incident" to "regular intelligence symbition", public security departments push local fraud situation analysis data to universities, universities send back early warning information on abnormal behaviors within the campus, achieving risk sharing and governance sharing; Society and schools work together to build a flexible outer defense line, and families can use the platform's "relatives and Friends Guard" function to establish a supervision and reminder mechanism for large consumption and abnormal transfers; The role of female college students has shifted from passive governance objects to governance participants. They can report fraud clues through the platform, modify the risk identification model, and drive the endogenous evolution[10] of the group defense mechanism.

4 Conclusions and suggestions

4.1 Research Conclusion: From System Vulnerability to Governance Resilience

Telecom fraud against female college students in the digital age is a result of the deep coupling of negative externalities in the digital environment and individual gullibility

traits. The process of fraud shows obvious individual differences, and its harm goes far beyond the scope of property loss. The "learn, practice, prevent, protect" full-cycle closed-loop system constructed in this study has transformed the governance logic from "post-case handling" to "source blocking", providing a practical path for solving the traditional campus anti-fraud governance predicament. The multi-party collaboration model centered on the platform and linked by intelligence sharing can effectively enhance governance agility and strengthen campus anti-fraud governance resilience at the system level.

4.2 Policy Recommendations: Building a New Paradigm for Digital and Intelligent Campus Governance

Digital intelligent technologies are reshaping the paradigm of telecom network fraud, necessitating a breakthrough beyond the limitations of ad hoc and temporary control measures in campus anti-fraud governance.A systematic,(omnichannel) digital-intelligent collaborative defense system must be established to build a sustainable, dynamic, and routine risk prevention framework. As the primary front for combating fraud among youth, universities should collaborate with public security agencies, telecommunications operators, financial institutions, and other stakeholders to form a coordinated governance community. They should jointly develop tiered and detailed anti-fraud implementation guidelines, clarify cross-departmental responsibilities and data-sharing boundaries for fraud intelligence, and establish standardized mechanisms for verifying and dynamically correcting discrepancies in risk data exchange. Based on the victimization patterns and scam scenarios specific to female college students, a gender-sensitive risk identification and assessment system should be developed, incorporating dedicated early-warning and intervention indicators for high-incidence fraud types such as online dating, fake online part-time jobs, and fraudulent refund schemes, enabling precise and targeted risk response. Local governments should increase policy support and financial allocation, promoting deep collaboration among university psychological counseling centers, legal aid organizations, and specialized anti-fraud units from public security departments to create an integrated, multifunctional victim assistance platform that ensures information anonymity and privacy protection. Leveraging massive risk data and advanced analytical capabilities from digital platforms such as the National Anti-Fraud Center app, fraud risks can be intercepted proactively and traced back to their sources, effectively cutting off the transmission chain at its origin. This provides dual institutional and technological support for building long-term, dynamic, and secure campuses.

References

1. Deng W, Liang G, Yu C, et al. An Early Warning Model of Telecommunication Network Fraud Based on User Portrait[J]. Computers, Materials & Continua, 2023, 75 (1) : 1561-1576. https://doi.org/10.32604/cmc.2023.035016

2. Zhao G, Mu P. The relationship between materialism and susceptibility to online fraud among Chinese college students: A moderated mediation model from trait and state perspectives[J]. Asian Journal of Social Psychology, 2025, 28(3): e70040.. https://doi.org/10.1111/ajsp.70040
3. Becker R A, Volinsky C, Wilks A R. Fraud Detection in Telecommunications: The History and Lessons Learned [J]. Technometrics, 2010, 52 (1) : 20-33. https://doi.org/10.1198/TECH.2009.08136
4. Zhao Q, Chen K, Li T, et al. Detecting telecommunication fraud by understanding the contents of a call[J]. Cybersecurity, 2018, 1(1): 8. https://doi.org/10.1186/s42400-018-0008-5
5. Tong A, Chen B, Wang Z, et al. GDFGAT: Graph attention network based on feature difference weight assignment for telecom fraud detection[J]. PLOS One, 2025, (5) : 20 e0322004. https://doi.org/10.1371/journal.pone.0322004
6. Li R, Chen H, Liu S, et al. TFD-IIS-CRMCB: Telecom Fraud Detection for Incomplete Information Systems Based on Correlated Relation and Maximal Consistent Block[J]. Entropy, 2023, 25 (1) : 112. https://doi.org/10.3390/e25010112
7. Yang J, Li S, Huang Z, et al. An improve fraud detection framework via dynamic representations and adaptive frequency response filter[J]. Scientific Reports, 2025, 15 (1) : 19051. https://doi.org/10.1038/s41598-025-02032-9
8. Xu F, Liu A, Li X. Victimization mechanisms and countermeasures in telecom network fraud: A dual-system theoretical perspective[J]. Frontiers in Psychology, 2025, 16: 1637935. https://doi.org/10.3389/fpsyg.2025.1637935
9. Luna A J H de O, Marinho M L M, de Moura H P. Agile governance theory: Operationalization[J]. Innovations in Systems and Software Engineering, 2020, 16(1): 3-44. https://doi.org/10.1007/s11334-019-00345-3
10. Wang T, Yang B. Countermeasure of telecom network fraud investigation based on big data[J]. Scientific Programming, 2022, 2022 (1) : 7219080. https://doi.org/10.1155/2022/7219080