From Reactive Response to Proactive Prevention: A Study on the Optimization Pathways for Anti-Fraud Governance Systems in Higher Education Institutions

Kaiyuan Liu, Jiali Zhu
Jiangxi Normal University, Nanchang, Jiangxi, China

Abstract: In recent years, college students are often targeted by fraud. Such cases occur frequently. They pose serious threats to financial security. They harm physical and mental well-being. Campus governance faces challenges. Social stability faces challenges. This paper examines current trends in digital society and intelligent crime, reviews past studies, and uses empirical research; it also looks at anti-fraud work in universities. Several deep-seated problems can be found: management mechanisms are outdated, information does not spread well, and technology is not applied enough. Based on these findings, this paper puts forward a complete anti-fraud governance system for universities, which has four parts (prevention, identification, intervention, and feedback), and it draws on ideas from modern governance and proactive control. The paper also discusses three ways to make improvements: data empowerment, cooperation between universities and police, and education that builds students' abilities. The main goal is to change university anti-fraud from reactive response to proactive prevention, and this change can offer both theoretical guidance and practical tools for making campus safety governance more effective.

Keywords: University Fraud; Anti-Fraud Governance; University-Police Collaboration; Pathway Optimization; Safety Education

1. Introduction

The survey was carried out by China Youth Daily and China Youth Campus Media, and they asked college students from 106 universities; the results gave a few figures. Among the students, 10.09% said they had been scammed before, 31.25% had encountered a scam but managed to avoid it, 50.98% knew someone around them who had been cheated, and only 25.97% had neither experienced any fraud nor heard of such cases among their friends [1]. These figures show that fraud is quite common on college campuses and affects a large number of students; Nowadays people live in a digital society, and in that society new technologies appear quickly, one after another, without much pause, and fraudsters make use of these technologies, so their tricks keep changing very fast. Criminals can leverage AIGC (Artificial Intelligence Generated Content) technology to automatically generate massive volumes of texts and images containing false information, as well as create criminal tools such as fraudulent websites and deceptive audio and video content. By exploiting these technologies, they execute scams and induce individuals to engage in online behaviors that expose them to the risk of victimization [2]. Currently, telecom and online fraud crimes are occurring at high frequencies. College students, characterized by relatively limited social experience and weak awareness of prevention, constitute a highly susceptible population to such victimization [3]. Making them high-risk targets that criminals specifically target.

In the face of these increasingly severe challenges, universities’ response mechanisms have shown significant lag. Many institutions have shortcomings in the development of anti-fraud and safety education systems, generally characterized by insufficient coordination among administrative units, overly formalistic educational content, and superficial application of technology. Prevention work and control measures are often only reaction-based, they act only after something happens, and they do not deal with the underlying causes of the risks; this situation creates immediate harm, for example students' money and property are not safe, and it also produces long-term problems, because campus order becomes unstable and stability is more difficult to preserve.

University education includes political and ideological training as well as safety governance, and both are being modernized; at the same time, these challenges affect students in several ways, they damage their mental health, physical health, and also their future development [4], so universities need to adjust their anti-fraud work, which is now reactive, they respond only after problems appear, but they should instead take preventive action and stop fraud before it occurs; they also need a regular system with clear rules, and this system should operate all the time; this adjustment is urgent and important, and it is a key part of the modernization process mentioned above.

2. Practical Challenges in Fraud Prevention at Universities

Now, fraud in colleges and universities is happening very often, the tricks are changing fast, and preventing and controlling it is becoming harder and harder; in the way management is set up, in how the society works together, and in dealing with technology, problems like "hard to collect evidence, hard to define, hard to get the stolen money back, and hard to fully stop it" are showing up, and this makes it clear that the old methods of prevention and control have limits and are failing when facing new kinds of crimes.

2.1 Management Dilemmas: The Tension between Open Environments and Specialized Prevention

Telecom network fraud is not like traditional cases; it breaks the limits of time and space, the people who are cheated and the ones who cheat are in different places, and the crime happens in a virtual digital space; many things make the investigation very hard, so the rate of solving these cases stays low [5]. Looking at the ways of crime, the cheating models have moved from old tricks like "fake customer service" and "winning fraud" to more technical, more precise and scene-based methods; criminals now use fake base stations, phishing links, and putting Trojans into QR codes, and they also bring in big data to build personal information profiles, pretending to be education or finance offices to do targeted cheating; the hiding and confusing parts of the cheating process have become much stronger.

The open campus management model is used by many universities, and this model does help with academic exchange, but at the same time it also causes some problems, for example security boundaries become unclear and control points get scattered in many different places. Traditional security governance methods mostly depend on manual management and on running awareness campaigns, but these methods are not able to handle crimes that are enabled by technology, and these crimes cross different domains, they move around, and they are hidden, so they are hard to deal with. Because of this, there are some structural problems in the prevention and control system, and these problems include slow responses and not enough coverage, and student advisors also face practical difficulties in their daily management work, and these difficulties can be described as "hard to identify," "hard to intervene," and "hard to trace back to where things started."

2.2 Communication Challenges: Weakening of Authoritative Discourse and the Complexity of the Online Information Environment

In terms of information dissemination, although universities have established relatively well-developed campus network infrastructures, in actual communication contexts, official university media and faculty educational content face intense competition from the diverse information available on the internet. Students are in a stage where their values are still forming, and their ability to judge information is not yet strong, so they can be easily affected by online subcultures, wrong information, and extreme views, and these things make their thinking more confused and weaken their trust in others.

There is also a deeper problem: counselors, who represent traditional educational authority, find that their persuasive power and communication effectiveness are relatively weaker in the online environment; when compared with algorithmic recommendations, social media interactions, and popular online figures, the counselors' one-way and persuasive style of communication cannot easily reach the deeper levels of students' thinking, and this creates a communication problem where messages are sent out but not really taken in, and even if they are taken in, they are not really believed.

2.3 Implementation Challenges: The Disconnect Between Formal Education and Behavioral Change

When it comes to educational practice, colleges and universities now often use things like theme class meetings, talks, posters, sitcoms, social media posts, and police talks to do anti-fraud education; these ways have some coverage and a base in the system, but in the real carrying out, there is a clear habit of making it just a form; the education content is mostly given one-way, with not much interaction or chances for students to take part in real-like situations, and it is hard to make students actively build up understanding and feel emotionally connected.

A deeper problem is that the existing model does not truly move from "passing on knowledge" to "creating action"; even when students learn the knowledge in class, they still often have trouble recognizing fraud clearly, react slowly, or even do wrong things when facing intense and precise cheating situations; the education only stays on the surface of knowing, and there is a lack of ongoing training for behavior and a way to get feedback, so it is hard for the anti-fraud awareness to turn into steady mental strength and daily habits.

3. Analysis of the Causes Behind the Governance Dilemma in University Anti-Fraud Efforts

The anti-fraud work in universities has run into a trouble; it is dealt with again and again but the fraud still cannot be stopped; this trouble is rooted in failures of structure, thinking and strategy; and only by deeply analyzing what causes these failures, can a breakthrough in governance be found.

3.1 Structural Cognitive Imbalance: Discrepancy between Students' Risk Identification Abilities and the Evolution of Fraud Techniques

College students stay on campus for long periods, the campus environment is relatively closed, they do not have much real-world experience, and their understanding of risks is not very strong; studies show that after they enter college, they often use phones and computers to handle their studies, student activities, social connections, and entertainment, and this frequent use brings a high chance of personal information being leaked, which gives fraudsters a good opportunity to carry out their schemes [6]; fraudsters use data analysis and social engineering methods to design scam scripts that are highly targeted and fit specific situations, for example fake high-paying job offers or tuition refund scams, and students often lack the skills to recognize these tricks and also lack the ability to react in the right way when facing such carefully made scams.

Looking at how education is provided, anti-fraud courses have not been a priority in university teaching for a long time; the content has not been put into the regular curriculum, and there are no courses with credits for this topic, so students do not have strong reasons from the university to pay attention to it; even though there are national events like National Cybersecurity Awareness Week, universities have not set up regular ways to share knowledge and build skills on campus; as a result, what students know about fraud prevention is not complete and only stays at a surface level, and this makes it hard for them to deal with very clever fraud tricks.

3.2 Educational Communication Failure: Mismatch between Content Supply and Reception Logic

Fraud prevention education at universities now has some systemic problems, and these problems are in the people who do the teaching, in the content that is taught, and in the methods that are used. When it comes to the people who do the work, universities depend too much on student advisors to carry out this specialized fraud prevention task, but these advisors usually do not get systematic training, and they also do not get enough professional support from the system. So, what the education does is mostly telling about cases and pushing policies; it doesn't go deep into how fraud tricks people's mind and how to stop it, and it's hard for students to get real understanding.

In terms of content and channels, anti-fraud propaganda still mainly uses traditional forms like banners, flyers and lectures; the content is very much the same and updates slowly, and it is seriously disconnected from the new media world that students use, such as short videos and interactive communities; some colleges and universities try to run new media platforms, but the content is mostly just reposted, without original explanations or new storytelling that fits their own university, so the communication effect keeps getting weaker; this one-way and lagging communication cannot build an emotional link or reach students' thinking, and it makes the useless cycle of education even worse.

3.3 Weak Prevention and Control Systems: Insufficient Technological Empowerment and Lack of Feedback Mechanisms

In using anti-fraud technology and building the ability to prevent and control in a systematic way, colleges and universities have clear weaknesses; on one hand, they have not fully used big data, artificial intelligence and other technologies to build a campus system for monitoring and early warning of risks, and they lack the ability to notice changes quickly and step in smartly for key risk points like students' unusual spending and social activities; the prevention and control methods still stay at the stage of reacting after things happen.

On the other hand, the education process is seriously short of changing behavior and getting feedback; most of the education now is aimed at passing on knowledge, and there are no practical training parts like fake fraud situations and stress tests, so students cannot train their ability to recognize and respond in a safe environment. Also, a good way to evaluate and track the education effect has not been built by colleges and universities; it is hard to find out students' reactions and weak points in real life, so there is no data to help change the education methods, and the trouble of "preaching again and again but being cheated again and again" appears.

4. Pathway Development: Systematic Strategies for Transitioning from Passive Response to Proactive Prevention

A safe campus environment is the foundation for university development; management should be strengthened and a safe environment should be created, so that students can study with peace of mind and not be disturbed by fraud and other things [7]. Because the anti-fraud work in universities has problems like poor management coordination, failed education communication and weak technical prevention, it is necessary to change the way of handling things from only reacting after something happens to actively preventing and controlling, including early warning, intervening during the process and repairing after the event. A systematic path is proposed here, with the core of "rebuilding education supply, using technology together, and closing the loop of system guarantee", aiming to build an all-round, smart and sustainable anti-fraud management system in universities.

4.1 Restructuring the Educational Supply System: From Fragmented Communication to Targeted Cognitive Enlightenment

We need to rebuild the anti-fraud education system from three parts: content, channels, and ability; this is to solve problems like "unbalanced understanding" and "education communication failure".

1. Content Reconstruction and Curriculum Integration. To stop telecom fraud, we need to do some things; first, young victims often have common weaknesses in thinking and personality, so we should design some courses that train their thinking and develop their personality in specific ways [8]; and we also need to make anti-fraud knowledge more systematic, develop courses that include modules like fraud psychology, financial security and data privacy, and put these courses into general education or required ideological and political courses, using credits to make sure students learn well; the content should follow the changes of technology, pay attention to new fraud tricks such as "AI face change" and "precise targeting", and be deeply connected with students' common activities like job hunting, social networking and shopping; besides, with real cases, we can carry out teaching of principle analysis and scene application, helping students build a complete framework for understanding risks.

2. Channel Integration and Targeted Outreach. We can build a media system around platforms like Weibo, Wechat and Douyin where students gather, then online and offline resources can be put together so that anti-fraud information is able to reach every corner; by using big data, student profiles can be made and content that fits their own needs can be sent to them; it is also good to get teachers and students to make things together, like short films against fraud and scripts for interaction, and to tell stories with feelings to make the messages more attractive; through live Q&A, online contests and other activities, interaction can be increased and the communication gap can be broken.

3. Capability Building and Practical Application. College students are active in cyberspace. They lack discernment ability. They are vulnerable to online rumors. This harms cybersecurity. This harms ideological security [9]. Universitiess can organize simulation exercises. Exercises are highly realistic. Students can hone identification skills. Students can hone response skills. Scenarios include impostor counselors. Scenarios include high-paying part-time jobs. Police officers and anti-fraud experts can be invited. They provide on-site guidance. Guidance enhances learning. Universitiess can

establish student volunteer teams. Teams conduct peer education. Students move from knowing to putting knowledge into practice.

4.2 Strengthening the Technological Collaborative Defense Line: From Isolated Early Warning to Intelligent Proactive Intervention

Technological support is insufficient. Coordination is lacking. A data-driven approach must be adopted. It should be the core. A proactive intervention system must be established. The system combines on-campus intelligent prevention and control. It also combines coordination and collaboration between the university and local authorities.

1. A platform that does intelligent joint prevention and control should be set up, and this platform should connect universitiess with law enforcement groups. There should be work together with public security departments, cyber security and information offices, financial institutions, and also other related groups, so that they can together build an anti-fraud command platform that brings everything together, and through this platform, important information can be shared in real time and can be exchanged in both directions, for example databases that have high-risk phone numbers and websites that are related to fraud. Blockchain technology that is used by a group of organizations can be used to make sure that data is safe and can be trusted, and also a system for having regular joint meetings and a system for looking at cases should be put in place, so that universitiess and law enforcement can work together in a collaborative way, and this collaborative effort can be pushed forward through joint prevention and control measures.
2. A campus-wide intelligent early-warning system should be deployed. To build an early warning system for fraud risks, we can bring in big data and AI analysis methods, and put together data from campus network, consumption and social interactions. It monitors abnormal money transfers. It monitors online behavior. It monitors social media activity. It identifies students at risk of becoming victims. It triggers a tiered intervention mechanism. Precise risk management is enabled. Management ranges from system pop-ups to manual intervention.
3. Implement routine environmental governance. Collaborate with cyber security authorities and telecom operators to regularly monitor and remove fake base stations, malicious Wi-Fi networks, and phishing websites around campus, thereby blocking channels for the dissemination of fraudulent information. Strengthen campus network security, upgrade security equipment, and identify and remove non-compliant advertisements related to fraud to create a safe and secure campus network and physical environment.

4.3 Improving Institutional Safeguards to Close the Loop: From Ambiguous Roles to Long-Term Collaborative Governance

Current research on safety education in higher education institutions is largely conducted within the framework of “formal institutional systems.” That is, universities impose top-down requirements and constraints on student behavior and ideology through methods such as issuing regulations and conducting various forms of classroom education. To ensure the sustained effectiveness of anti-fraud efforts, it is essential to establish an institutional safeguard system with clear roles and responsibilities, effective incentives, and full-process coverage.

1. Clarify primary responsibilities and evaluation mechanisms. Establish a university-level special task force for anti-fraud efforts, formulate implementation plans, and clearly define the division of responsibilities among departments such as Student Affairs, Campus Security, and Academic Affairs. Incorporate core indicators—such as incident rates within universities and colleges and early warning response rates—into performance evaluations. Hold units and individuals accountable for inadequate performance, thereby transforming anti-fraud work from a “soft task” into a “hard constraint.”
2. Establish an incentive ecosystem that involves everyone. Count student participation in anti-fraud initiatives toward extracurricular credits and link it to awards and honors; create honors such as the “Fraud-Free College” and “Anti-Fraud Pioneer” to foster a campus-wide anti-fraud culture. Incorporate anti-fraud training into the regular professional development of faculty and staff, encouraging them to participate in oversight and outreach efforts, thereby creating a collaborative anti-fraud ecosystem involving both faculty and students.
3. Establishing a Feedback Loop for Support and Assessment. Extensive research indicates that gaining a deep understanding of the

psychological and behavioral characteristics of susceptible populations is instrumental in conducting more targeted educational campaigns and early warning interventions [10]. Higher education institutions should establish an individualized support mechanism ("one student, one file") for victimized students, providing legal and psychological assistance to mitigate secondary harm. Universities can check how well their work is doing through surveys, interviews, and looking at case data, they can find problems from this information, then they can change their strategies and methods, and they can also set up a process that keeps improving over time, this process follows a cycle of checking, then giving feedback, then making adjustments, and this helps the whole governance system keep evolving and stay up to date.

5. Conclusion

The anti-fraud work in universities has become a big problem now, because digital technology is developing quickly and fraud methods keep changing all the time; this problem is about student safety, campus stability, and the modernization of education management. This paper does a systematic analysis of the practical challenges that universities are now facing, and these challenges are in three areas, which are management coordination, educational outreach, and putting things into practice in real situations. The paper also finds out the reasons that are underneath these problems, and these reasons are things like cognitive imbalances that exist in the structure, failures that happen in educational outreach, and weak points that are in the prevention and control systems. Then the paper puts forward a systematic approach that has three parts, and these three parts are called "restructuring of educational provision," "technology-enabled collaboration," and "institutional safeguards," and the purpose of this approach is to push for a fundamental change in anti-fraud work, so that it moves from just responding after things happen to doing prevention and control before things happen. Anti-fraud efforts in higher education institutions are something that needs work from the whole system, and this means that barriers between different departments have to be broken down, and different groups both on campus and off campus need to be brought together to work in a collaborative way. Reforming the method of delivering education comes first, it builds students' awareness of risks and sharpens their ability to respond. Then there's technology: using it to strengthen skills lets us target interventions more accurately through things like smart early warnings and data sharing. Institutional safeguards lock in support and keep things running smoothly over time. Put all three together, and you get a strong, intelligent anti-fraud system—nothing less will do.

Acknowledgments

This work was supported by the 2025 Ministry of Education Special Task Project on Humanities and Social Sciences Research (University Counselor Research) "Exploration of the Construction and Practical Pathways of University-Family-Community Collaborative Education Consortia under the Theory of Overlapping Influence Domains" (No.: 25JDSZ3091); the 2024 Research Project of the National Training and Research Center for University Ideological and Political Work Teams (Jiangxi Normal University) "Research on the Construction of a University Student Safety Education System from the Perspective of the Comprehensive National Security Outlook"; and the Jiangxi Provincial Association for Ideological and Political Education in Higher Education 2024 Project: "A Study on Behavioral Characteristics of University Student Victims in Fraud Cases and Intervention Strategies" (No.: XSGZ24202).

References

[1] Bi, R.X.; Luo, X.; Cheng, S. Over 90% of Surveyed College Students Hope for Anti-Fraud Education on Campus. China Youth Daily, 25 October 2021.
[2] Zhou, S.L.; Xu, R.; Chen, T.G.; et al. A Study on the Identification of Vulnerability to AI Face-Swapping Fraud. Data Anal. Knowl. Discov. 2025, 1–14.
[3] Sun, C.B.; Zhao, X.L.; Zhao, G.F.; et al. Development of a Questionnaire on College Students' Vulnerability to Telecommunications and Internet Fraud. Chin. J. Ment. Health 2024, 38(10), 894–900.
[4] Meng, Q. T. Review and Prevention of Minors' Participation in Telecom and Cyber Fraud Crimes. J. Journal of Jiangsu College of Engineering and Technology, 2026, 26(1): 106-112.

[5] Yin, M. Empirical Study of Victims of Telecommunications Fraud Cases: A Quantitative Statistical Analysis Based on Victim Statements. J. China Crim. Police Coll. 2017, 3, 57–62.

[6] Xu, Q. Strong Education and Weak Perception: The Impact of Formal and Informal Systems in University Safety Education on College Students' Risk Perception—A Multi-Case Study Based on Telecommunications Fraud. J. Guangzhou Univ. (Soc. Sci. Ed.) 2022, 21(2), 32–43.

[7] Wang, H.Y.; Han, X.M. Delivering the "First Lesson" in Anti-Fraud Safety Education. Chin. High. Educ. 2016, 18, 57–58.

[8] Zhao, L.; Huang, X.M.; Chen, H.M. Trust Formation and Psychology of Young Victims of Telecom Fraud: A Qualitative Analysis of 9 Post-90s Victims. China Youth Stud. 2020, 3, 49–54.

[9] Luo, Y.T.; Luo, H. On Enhancing College Students' Ability to Identify Online Rumors. Ideol. Theor. Educ. 2020, 3, 73–79.

[10] Wang, H.Y.; Wang, D.; Yang, C. Development and Evaluation of the Reliability and Validity of the Vulnerability Scale for Telecommunications and Internet Fraud. Chin. J. Ment. Health 2025, 11, 981–987.