ISSN 2616-7433 Vol. 8, Issue 2: 74-81, DOI: 10.25236/FSST.2026.080210

Psychological Game Mechanisms between Fraudsters and Adolescents in AI-Empowered Telecom Fraud—An Autoethnographic Study

Wenchu Gao

Wuhan ISA Wenhua High School, Wuhan, 430000, China
bill.gao28@isawuhan.com

Abstract: *Against the backdrop of the rapid development of artificial intelligence technology, such technologies are being embedded by criminals in the process of telecom fraud, continuously reshaping the modes and structures of fraud implementation. Due to their insufficient social experience and weak risk identification ability, adolescents have increasingly become key targets of AI-empowered telecom fraud. Adopting the method of autoethnography, this paper takes the researcher's personal experience of encountering telecom fraud as a detailed case, and analyzes the implementation process and internal psychological mechanism of AI-enabled telecom fraud under the theoretical framework of the Elaboration Likelihood Model (ELM). The study finds that under the condition that peripheral cues such as acquaintance identity simulation, time pressure creation and emotional appeal enhancement are significantly amplified by AI technology, adolescent targets are more likely to be continuously drawn into the peripheral processing route. Although central processing may be briefly activated at the moment of suspicion, it is often constantly suppressed by information overload, situational coercion and urgent rhetoric, eventually leading to "act first, judge later" decisions driven by high-arousal emotions. In this process, AI technology improves the verisimilitude and credibility of fraudulent information, weakens adolescents' ability to identify risks relying on traditional experience and routine verification methods, and thereby reshapes the psychological game structure in telecom fraud. Based on the above analysis, this paper further puts forward anti-fraud suggestions for adolescents from the perspectives of activating the central processing route, constructing technical countermeasures, and identifying and intervening in manipulated emotions.*

Keywords: *AI-empowered; telecom fraud; fraudsters and targets; Elaboration Likelihood Model (ELM); psychological game mechanism*

1. Introduction

In recent years, with the popularization of the Internet of Things and smart terminals, telecom fraud has become characterized by high frequency, high intelligence, and increasing concealment, posing a serious threat to citizens' property and personal security. Driven by the development and widespread application of artificial intelligence, technologies such as voice cloning, image synthesis, and conversational text generation can now be easily realized. This means that AI has lowered the threshold for committing fraud while making detection increasingly difficult. Traditional methods of identifying typical fraud, including video call verification, have become less effective. In this context, adolescents — who have limited social experience, lack practical and financial literacy, and have not yet fully developed self-protection awareness — have gradually become key targets and a high-risk group for telecom fraud by criminals. Against this background, this paper adopts the Elaboration Likelihood Model (ELM) as its theoretical foundation and focuses on typical fraud scenarios involving AI technology. Combining an autoethnographic account of the researcher's own experience of telecom fraud, it analyzes the critical stages, psychological nodes, and behavioral mechanisms in fraudulent interactions. The study pays particular attention to how fraudsters use technological simulation and scripted discourse to foster trust, build pressure, and manipulate cognition, and reveals how adolescent targets undergo the dynamic process of trust formation, emerging doubt, and decision-making under conditions of limited information. From an integrated perspective of cognition, emotion, and interactive strategies, this paper aims to deepen understanding of the psychological mechanisms underlying AI-empowered telecom fraud and provide theoretical references for anti-fraud education for adolescents, the development of intelligent early-warning tools, and the improvement of relevant governance policies.

ISSN 2616-7433 Vol. 8, Issue 2: 74-81, DOI: 10.25236/FSST.2026.080210

2. Literature review

In recent years, academic research on telecom fraud has gradually shifted from "victim characteristic identification" to process analysis of the "fraudster–target interaction mechanism". By constructing an index system of susceptibility to telecom fraud among college students, Chen Zhenxing et al. pointed out that experience, competence, psychological factors, and individual factors jointly affect fraud victimization risk, indicating that young targets are not passive victims, but enter a high-risk state due to the interplay of insufficient experience, lack of competence, and psychological vulnerability. [1] Abuelezz et al. found that appearance cues of fraudsters—such as age, gender, ethnicity, and attire—significantly influence targets' trust and risk-taking willingness, demonstrating that the psychological game occurs not only at the level of discourse content but also embedded in visual and identity representation. [2]

Yan Tingting further focused on the university context and noted that fraudsters often use well-rehearsed scripts and emotional control strategies to gradually break down college students' psychological defenses, indicating that the fraud process is essentially a continuously unfolding process of psychological induction and trust manipulation. [3] Compared with traditional telecom fraud, the psychological game in AI-empowered scenarios relies more heavily on a media environment where truth and falsehood are increasingly indistinguishable. In a study centered on young people, Naffi et al. argued that the governance of malicious deepfakes and disinformation cannot rely solely on factual information; instead, it requires experiential and reflective learning to improve young people's ability to identify and counter manipulative media. This finding, conversely, suggests that young people are more susceptible to immersive persuasion in AI-synthesized contexts. [4] Lao et al. also found that young people often respond to deepfake content in everyday media use in an incidental, fragmented, and situational manner. This implies that they do not maintain constant high alertness but engage with AI-generated content at a low threshold during platform-based browsing, thereby increasing the likelihood of being manipulated. [5]

Furthermore, existing studies have begun to analyze fraudulent information as the core carrier of fraudsters' deceptive strategies. Wang Hongjing et al. found that fraudulent messages exert influence through four dimensions: information source, information form, information content, and information emotion, which respectively activate psychological responses such as trust, attraction, and anxiety in targets; among them, authority, relevance, and professionalism are more likely to induce trust; additional information, profitability, and operability tend to generate attraction; while severity and urgency enhance anxiety and compliance. This provides a relatively clear analytical framework for understanding how fraudsters dynamically allocate persuasive cues in interactions. [6] In terms of technology, Si Binzhou et al. proposed a risk analysis framework based on large language models and event fusion and identified high-risk links such as "information provision", which means that AI not only improves the ability to generate fraud scripts and construct situational contexts but also makes the fraud game more staged, adaptive, and iterative. [7] The study by Yasin et al. more directly reveals how fraudsters reconstruct trust relationships through AI media; they argue that the key to electronic fraud lies in the systematic exploitation of human trust, compliance, and judgment heuristics by AI, and that protection must therefore focus on people's cognitive vulnerabilities. [8]

In summary, existing studies have laid an important foundation by examining youth susceptibility, fraudulent message characteristics, persuasion in telecom fraud, and the media environment of deepfake technology, yet research that systematically analyzes AI-empowered telecom fraud as an ongoing psychological game between fraudsters and adolescent targets remains limited. Current contributions either focus on the static characteristics of victims or emphasize technical detection and educational interventions, and insufficient attention has been paid to how fraudsters construct trust, create urgency, and induce compliance through multiple rounds of interaction, as well as how adolescents experience shifts in judgment amid the interplay of emotion, cognition, and media cues. Accordingly, this paper introduces the ELM to analyze the psychological game mechanism between fraudsters and adolescent targets in AI-empowered telecom fraud from an interactive process perspective rather than from a single-actor viewpoint.

3. Theoretical model and research methods

The theoretical analytical model adopted in this study is the Elaboration Likelihood Model (ELM), which was proposed by psychologists Richard Petty and John Cacioppo in the 1980s. The ELM specifies that when individuals receive persuasive messages, they follow two distinct processing routes depending on their "level of elaboration," ultimately leading to different decisions. The first route is known as the

ISSN 2616-7433 Vol. 8, Issue 2: 74-81, DOI: 10.25236/FSST.2026.080210

central route, in which individuals engage in careful thinking and elaborate processing prior to decision-making with sufficient motivation and ability. The second route is the peripheral route, which occurs when individuals lack adequate motivation or processing capacity and rely primarily on superficial peripheral cues for judgment, such as the authority of the information source, the attractiveness of the speaker, the quantity and fluency of message presentation, and others' approval. Generally speaking, the central route leads to attitude change that is relatively strong, persistent, and resistant to counter-persuasion; by contrast, the peripheral route is characterized by superficiality and high susceptibility to environmental influences.[9]

From the perspective of this study, telecom fraud is essentially a persuasive act carefully designed by fraudsters to manipulate victims. Combining the characteristics of the central route and the peripheral route, the psychological game between fraudsters and targets can be understood as a process in which fraudsters continuously strive to confine adolescent targets to decision-making via the peripheral route while vigorously avoiding activating central route thinking. On the one hand, AI-empowered telecom fraud heavily accumulates peripheral cues by means of mimicking acquaintances' voices, forging authoritative identities, and creating time urgency and intense emotional pressure, making it difficult for adolescents to activate their central processing system to verify the authenticity of information under the dual pressure of emotion and time; on the other hand, adolescents' deficiencies in risk awareness, common sense, and understanding of finance and technology further restrict and weaken their motivation and ability to conduct central processing. Taking ELM as the theoretical framework, this study divides the fraudulent interaction into distinct stages to analyze specifically how fraudsters strengthen compliance through peripheral cues at each stage and how they attempt to block central processing when targets develop doubts. Meanwhile, through dynamic tracking of attitudes and decisions in the researcher's own case, this study reveals how the imbalance between central and peripheral processing routes reshapes the psychological game structure between the two parties following the intervention of AI technology, thereby providing theoretical support for explaining the susceptibility mechanism and designing targeted anti-fraud interventions.

In terms of research methodology, this paper adopts autoethnography as the core approach to uncover the psychological game mechanism in AI-empowered telecom fraud. Specifically, the researcher, as an "insider-observer", re-examines the entire experience of encountering telecom fraud from a rational perspective and within the ELM framework, and conducts a systematic retrospective analysis. The author reconstructs the whole process in chronological order, from initial exposure to the information, trust building, emotional manipulation, and critical decision-making to post-event reflection, while simultaneously documenting real-time cognitive judgments, emotional experiences, and physical sensations in the narrative. This autoethnographic account is treated as a core case for analyzing the psychological interaction between fraudsters and targets.

What follows is a personal experience of the author and is therefore presented in the first-person narrative form. At around 10 p.m. on August 15, 2025, a classmate named Zhou suddenly sent me a message on QQ asking if I was online. Zhou had been my schoolmate for many years in primary and junior high school, and we knew each other fairly well. I was about to go to bed when I saw the message and asked what was wrong. A moment later, he said his cousin had been hit by a bicycle and was waiting for surgery in the hospital, and asked me to help transfer money to his cousin's Alipay account. I found it somewhat odd and asked why he could not transfer the money himself. He explained that his Alipay account was restricted and unable to make transfers. After hearing his explanation, I agreed. He asked for my WeChat payment code, saying he would transfer the money to my WeChat account. A few minutes later, he sent a screenshot showing a successful transfer of 1,000 yuan, which looked identical to a real transfer screenshot and was virtually indistinguishable from the genuine one. As I did not receive the money immediately, I asked him why. He circled a note at the bottom of the original screenshot indicating a two-hour delayed payment and explained that he had previously set up this function and forgotten to turn it off. I checked online and confirmed that such a delayed payment function did exist, with funds arriving within 2 to 24 hours, so I did not think much of it, assuming the money would arrive in due course and that there would be no harm in first transferring the money to help with the emergency. Right after that, he added me to a group chat, in which a person claiming to be his cousin explained her accident and attached a graphic picture of a deep, bleeding wound on her lower leg. By this point, I had been drawn into the urgent emotional atmosphere created by the two of them. The cousin asked me to convert the 1,000 yuan Zhou claimed to have transferred to my WeChat account into Alipay through a platform called Vivibao. Once I completed the operation, she sent me the Alipay payment code of a person she claimed was a nurse collecting the medical fee on her behalf. I transferred the converted 1,000 yuan to the designated account. She then told me that additional money was needed for the operation and anesthesia. At that moment, Zhou sent me another three transfer records totaling more than 2,000 yuan,

ISSN 2616-7433 Vol. 8, Issue 2: 74-81, DOI: 10.25236/FSST.2026.080210

again set for delayed payment. I again converted the stated amount into Alipay and transferred it to two different accounts she designated. When all transfers were completed, the so-called cousin said she was going into surgery. Zhou told me he would stay up until all the money he had transferred arrived in my account. I then went to bed, still unaware of anything unusual, thinking the money he sent would probably arrive the next morning and that I had merely helped someone out as a favor. When I woke up the next morning, I found none of the funds had arrived. I saw messages in the group: at around two o'clock in the morning, Zhou had messaged the group saying that he had made too many consecutive transfers and the platform had not approved them, so the money would arrive later; at around seven o'clock the next morning, he messaged again saying he was going to a training class and would be online around five or six o'clock in the afternoon. He added that if I needed the money urgently, I could ask my family to transfer it to me first. By the afternoon, the money still had not arrived, and after calming down and reviewing the incident, I noticed many suspicious points. I then contacted my family and asked them to communicate with Zhou's family (Zhou's parents had been working away from home for a long time, and he was looked after by his grandmother). Meanwhile, I tried to contact Zhou and his cousin again. His cousin told me that Zhou would come online later and asked me to wait, saying the money would probably arrive that night. On my family's advice, I decided to call Zhou via voice chat to confirm his identity. Zhou agreed and spoke with me on a voice call at nine o'clock. The voice on the call was indeed Zhou's; he kept saying his grandmother was outside and that he would send me messages instead. By then, I already felt something was seriously wrong. Soon after, my mother called and told me she had contacted Zhou's grandmother: Zhou's QQ account had been stolen, and several other classmates had also been defrauded. It was later learned that Zhou had received a video call from someone claiming to be a friend who wanted to borrow his QQ account to log in to a game, and Zhou had handed over the account without second thought. In reality, the video call had been generated by AI, which ultimately led to the theft of Zhou's account.

4. Analysis of the psychological game mechanism between fraudsters and adolescent targets in AI-empowered telecom fraud

Overall, taking the deception of Classmate Zhou as the starting point, the entire case can be divided into five distinct stages along a chronological timeline. In each stage, fraudsters employ a variety of tactics, including AI-generated false evidence and emotional manipulation, to confine the victim's thinking route to the peripheral processing route; even if the victim's central processing route is activated, it is suppressed at an initial stage by such tactics. As a result, the victim maintains a high degree of trust in the information and demands provided by fraudsters and gradually falls into the trap, since the rational perspective and detailed analysis enabled by the central processing route remain absent throughout the process.

In the first stage, Zhou unquestioningly provided his QQ account to the fraudsters after receiving a video call manipulated by AI face-swapping. The nearly perfect match of biological and vocal characteristics between his actual friend and the figure in the AI-generated video minimized Zhou's motivation to activate the central processing route. In most daily situations, the identity of a friend generates additional trust. When a request to borrow an account is made on the basis of such trust, individuals usually do not harbor excessive doubt, because everyone has made countless peripheral-route decisions in the past based on trusting relationships with friends. In response to requests from acquaintances, any individual will automatically lower their defense mechanisms; maintaining constant vigilance toward all requests from acquaintances incurs extremely high time and energy costs and undermines the trust mechanism between acquaintances. From another perspective, Zhou's failure to activate the central route stemmed not only from a lack of motivation but also from insufficient ability to engage in central-route thinking in this scenario. Before falling victim to this AI video fraud, he was unaware of such criminal methods. This indicates that even if he had possessed a certain level of motivation, he would still have been unable to activate the central processing route. The fraudsters took advantage of Zhou's lack of relevant knowledge and ability, together with the low motivation induced by the seemingly friendly identity, to ensure that he had no possibility of activating the central route in this context. The fraudsters thus completed the most critical first step in their entire scheme: constructing a deceptive situation embedded with the characteristics of an acquaintance.

In the second stage, the fraudsters used Zhou's account to contact the author and requested help with transferring money to Zhou's injured cousin who was supposedly in the hospital. At this stage, the author's central processing route had already been activated, and doubts were raised to the fraudsters immediately, yet the author still chose to believe the explanation provided. Messages involving money transfers usually trigger high alertness in individuals, which rapidly activates the central route to

ISSN 2616-7433 Vol. 8, Issue 2: 74-81, DOI: 10.25236/FSST.2026.080210

scrutinize the fraudsters' request. Even so, the central route only remained at an initial stage. The acquaintance cue derived from Zhou's account automatically lowered the alertness caused by the transfer request. Meanwhile, the fraudsters were aware that students generally lack sufficient knowledge of payment and transfer mechanisms, so they easily dispelled the alertness and suspicion aroused by the request with seemingly reasonable explanations. Essentially, at this stage, the fraudsters conducted a highly advantageous "game" based on the acquaintance identity from the compromised account and the common lack of knowledge about payment platforms among students. The superficial activation of the central route was insufficient to resist the comprehensive interference from the fraudsters. In addition, the message that "Zhou's cousin had been hit" heightened the urgency and emotional appeal of the conversation. By describing an urgent, shocking, and oppressive incident, the fraudsters drastically compressed the "activation time" of the central route, triggered the author's emotional and intuitive thinking as constant interference, and minimized the possibility for the victim to detect abnormalities. This narrative was also framed around Zhou's family background—his parents working away from home provided room for the fraudsters to justify their story. Out of understanding and trust in their classmate, the author automatically filled in plausible details behind this emergency situation. In the second stage, the fraudsters rendered the activation of the central route ineffective through the superposition of multiple cues, broke through the author's psychological defenses, and paved the way for subsequent fraudulent acts.

In the third stage, the fraudsters sent the author a screenshot indicating a successful transfer, and the so-called "cousin" joined in defrauding the author. It was at this stage that the author suffered actual financial loss. The 1,000-yuan successful transfer screenshot sent by the fraudsters was AI-generated. The powerful image simulation and template-learning capabilities of AI enabled the screenshot to be almost identical to a real transfer screenshot in appearance and even pixel details. The emergence of the transfer screenshot represented another breakthrough in the author's psychological defenses. With the central processing route shut down and relying solely on the peripheral route for judgment, the author viewed the screenshot as proof that the other party had completed the transfer, so the act of helping with the transfer was based on the mistaken belief that the payment had already been made. The high fidelity of AI-generated images led the victim to regard the successful transfer screenshot as direct evidence of the funds being deposited into the author's account. When the author noticed that the money did not arrive immediately and questioned the fraudsters, the central route was activated once again, as a huge inconsistency existed between the authoritative proof represented by the screenshot and the absence of real-time funds, giving the author sufficient motivation to doubt the authenticity of the transfer. However, the fraudsters' explanation about delayed payment resolved this apparent contradiction, and they again used the screenshot, circling the label indicating delayed transfer to restore the link between the screenshot and the alleged transfer. After hearing this explanation, the author checked online and confirmed that such a function did exist, with funds possibly arriving within 2 to 24 hours. This consistency restored the authority of the transfer screenshot and neutralized the activation of the central route. According to the ELM, both motivation and ability are indispensable for the central processing route to function effectively, yet the fraudsters exploited the victim's lack of ability, preventing the rational and in-depth thinking and verification represented by the central route from serving as an effective barrier. When the operation of the central route was impeded by limited ability, the victim's thinking pattern naturally reverted to the peripheral route to relieve anxiety caused by "cognitive incapacity" [10]. Subsequently, the involvement of the "cousin" completely broke down the victim's psychological defenses. The "cousin" reinforced the earlier claim of a traffic accident with a graphic AI-generated image of a bleeding wound. By this point, the author's central processing route had been completely deactivated, and the peripheral route was defenseless against such visually striking images. The photo evoked the author's empathy, and rational thinking was entirely replaced by emotional compassion and eagerness to help. At this stage, although the author had not yet made the final transfer, vigilance and critical thinking had been completely lost, making financial loss virtually inevitable. This explains why, when the "cousin" asked the author to transfer the funds to Alipay via the "Vivibao" platform, the author raised no further questions, such as doubting the legitimacy of the Vivibao platform or why the hospital only accepted Alipay payments. In hindsight, the fraudsters revealed numerous unavoidable flaws during this stage, yet due to the preceding setup and emotional manipulation, the author completely lost the ability to detect these inconsistencies, because the peripheral route processes information in a subconscious and habitual manner.

In the fourth stage, the fraudsters demanded the victim to transfer money to multiple accounts and provided a series of explanations. When the fraudsters asked the author to transfer funds to several personal accounts, the author noticed something unusual due to previous anti-fraud education, despite the many seemingly reasonable explanations offered by the fraudsters. Such cognition was formed via

ISSN 2616-7433 Vol. 8, Issue 2: 74-81, DOI: 10.25236/FSST.2026.080210

the peripheral route, relying on simple judgments based on past experience and knowledge. However, since the author had already completed the first transfer of 1,000 yuan, the victim had fallen into the trap set by the fraudsters based on the sunk cost fallacy[11]. Confirming the abnormality of subsequent transfers would require acknowledging that the earlier transfer had been defrauded; unwilling to let the sunk costs go to waste, the victim continued to follow the transfer demands of the fraudsters, and as long as seemingly reasonable explanations were provided, the victim could not stop. From a rational perspective, recognizing such anomalies and realizing that the previous transfer losses constituted sunk costs would minimize further losses. Yet the problem was that, unwilling to abandon the sunk costs, the victim preferred to interpret the irregularities in the fraudsters' transfer demands independently rather than re-examine the information from a rational viewpoint. The sunk cost fallacy stems from inherent human weaknesses and is highly common in fraud scenarios.

In the fifth stage, the fraudsters covered up and managed their fraudulent acts. The fraudsters followed up on the arrival of the transfers intermittently throughout the night, offering explanations such as transfer limits and contacting customer service. As the victim, the author normally assumed that fraudsters would block the victim once the scam was completed; such continuous follow-up created a sense of responsibility that deviated from common fraud scenarios, delaying the moment when the victim realized the deception. Furthermore, victims are usually reluctant to admit that they have been defrauded, so the rhetoric used by the fraudsters after the scam ensured that the victim remained in a state of self-deception driven by the sunk cost fallacy for a certain period, thereby buying more time for the fraudsters to process and transfer the illicit funds. In the end, prompted by family members, the author finally emerged from self-deception and requested a voice call for verification, but the fraudsters once again obstructed the victim's thinking pathway through the high fidelity of AI-generated voice. For the victim, the consistency of the voice signaled the credibility of the other party. By the time the author discovered that Zhou's QQ account had been stolen, the fraudsters had already maximally delayed the victim's recognition of the scam, completed the follow-up disposal of the funds—thereby rendering recovery far more difficult—and bought additional time to potentially target other relatives and friends close to Zhou for further fraud.

The above five stages present in detail the process of the psychological game between fraudsters and victims as analyzed under the ELM. It is evident that AI elements played a crucial role, repeatedly bypassing the victims' activated central processing route and vigilance, repeatedly convincing the victims of the authenticity of the fraudsters' identity and requests, and ultimately resulting in the victim being defrauded and realizing the fact of the scam only after a considerable delay.

5. Prevention pathways for adolescents against AI-driven telecom fraud

As can be seen from the empirical analysis, the tactics used by fraudsters to hinder the activation of the central route or render it ineffective fall into two categories: first, exploiting the high fidelity of AI technologies, acquaintance-based cues, emotional manipulation and other means to suppress the motivation to activate the central route; second, taking advantage of the lack of knowledge among students and adolescents regarding AI-enabled crimes, transfer procedures and payment platforms, so that the central route lacks critical identification ability and thus becomes dysfunctional. In response to these two types of tactics, the author proposes two corresponding prevention pathways.

To address the insufficient motivation for activating the central route, the essential solution lies in artificially creating "friction" to forcibly pull victims back from the peripheral route, where they have been trapped by fraudsters' interference, to the central route of rational thinking. From this perspective, social platforms including WeChat and QQ need to introduce AI synthesis detection functions for voice messages and text conversations. When images, voice recordings, or video calls sent by users exhibit high AI-generated characteristics, a prominent on-screen prompt indicating "suspected AI-generated content" should be displayed immediately. Such visual interference will largely prevent victims from falling into the trap of false explanations constructed by fraudsters using AI-generated materials. In addition, for sudden large-value transfers involving student groups and high-risk accounts, payment platforms should adopt delayed settlement procedures. The extra thinking time helps victims break away from the peripheral route that leads to blind trust in fraudsters within a short period, and enables them to activate the central route to respond upon detecting abnormal information provided by fraudsters. An additional interval of 15 to 30 minutes is crucial for this cognitive process. Once victims detect anomalies and contact the platform, they will have a much higher chance of recovering the defrauded funds. Apart from measures that can be implemented by relevant platforms, victims' own awareness of vigilance must also be enhanced. Anti-fraud lectures should be offered in primary and secondary schools to inform adolescents of the typical features of fraud, cultivate their sensitivity to transfer requests, and encourage

ISSN 2616-7433 Vol. 8, Issue 2: 74-81, DOI: 10.25236/FSST.2026.080210

them to communicate and consult with parents promptly when facing similar demands.

To address the "dysfunction" of the central route caused by a lack of critical identification ability and insufficient understanding of transaction platforms after activation, the core of governance lies in eliminating information asymmetry and equipping students with basic judgment and scrutiny capabilities when facing complicated transfer procedures. From this perspective, anti-fraud education for adolescents should not remain at the level of empty slogans, but be refined to deconstruct the nature of transfer operations; for instance, teaching students about platform functions that are often misused in fraudulent practices. Only when students understand the main functions of payment platforms and their corresponding risks can they effectively break through the information cocoon constructed by fraudsters based on students' ignorance in relevant fields. In addition, payment platforms should issue timely risk prompts during key steps such as code scanning and verification code input, with warnings similar to: "Your funds will be transferred to a private account in another province with a low credibility rating, indicating a high risk of fraud." Such immediate reminders compensate for users' insufficient knowledge of financial operations through the intuitiveness of visual text. Finally, the state needs to introduce relevant regulations to promote the use of digital watermarks for AI-generated images and audio, which allow quick identification of the account that generated the content. This critical post-incident remedy enables rapid technical tracking of fraudsters' information. It not only facilitates timely tracing and punishment of fraudsters after the event, but also provides psychological confidence and support for potential victims to compensate for their deficiencies in identification capacity.

6. Conclusion

Against the backdrop of AI-empowered telecom fraud, this paper examines the psychological game between fraudsters and adolescent targets using the autoethnographic method and the ELM as the analytical framework. The study finds that AI technology has not altered the basic logic of telecom fraud, which centers on persuasion, induction, and manipulation, but has significantly strengthened the capacity for identity disguise, scenario construction, and emotional pressure. It renders peripheral cues such as acquaintance trust, urgent atmosphere, and forged evidence more realistic and penetrating, while continuously reducing the room for targets to activate central processing. For adolescents with insufficient social experience and risk identification ability, such technology-enhanced persuasion is more likely to induce unbalanced judgment and compliant decision-making. It is thus clear that the prevention and control of AI-driven telecom fraud is not merely a matter of technical governance, but also involves cognitive intervention, media literacy improvement, and the construction of a collaborative protection system. It should be noted that this paper is mainly based on a single case analysis, and the scope of empirical materials remains limited. Future research may adopt interviews, questionnaires, scenario experiments, and other methods to further explore the differentiated victimization mechanisms of various adolescent groups in AI-related fraud.

References

[1] Chen Z X, Dong H W, Hao Q, et al. Construction and analysis of index system for influencing factors of susceptibility to telecom fraud [J]. Journal of Xi'an University of Science and Technology, 2022, 42(2): 389-396.

[2] Abuelezz I, Barhamgi M, Nhlabatsi A, et al. How demographic and appearance cues of a potential social engineer influence trust perception and risk-taking among targets?[J]. Information and Computer Security, 2024, 33(3): 320-343.

[3] Yan T T. Psychological analysis of college students suffering from telecom fraud[J]. Advances in Psychology, 2023, 13(7): 2904-2910.

[4] Naffi N, Charest M, Danis S, et al. Empowering youth to combat malicious deepfakes and disinformation: an experiential and reflective learning experience informed by personal construct theory[J]. Journal of Constructivist Psychology, 2025, 38(1): 119-140.

[5] Lao Y, Hirvonen N, Larsson S. Everyday encounters with deepfakes: young people's media and information literacy practices with AI-generated media[J]. Journal of Documentation, 2025, 81(7): 216-235.

[6] Wang H J, Liu W J, Liu T C. Identification of characteristics and deception mechanism of vulnerable groups adopting fraudulent information in telecom fraud scenarios[J]. Information Science, 2024, 42(4): 184-191.

[7] Si B Z, Sun H C, Wu Y. Risk analysis of telecom fraud events based on large language models and

ISSN 2616-7433 Vol. 8, Issue 2: 74-81, DOI: 10.25236/FSST.2026.080210

event fusion[J]. Data Analysis and Knowledge Discovery, 2025, 9(7): 38-51.
[8] Yasin A, Fatima R, Liu L, et al. Counteracting social engineering attacks[J]. Computer Fraud & Security, 2021(10): 15-19.
[9] Petty R E, Cacioppo J T. The elaboration likelihood model of persuasion[A]//Berkowitz L, ed. Advances in Experimental Social Psychology[C]. New York: Academic Press, 1986, 19: 123-128.
[10] Petersen R C, Smith G E, Waring S C, et al. Mild cognitive impairment: clinical characterization and outcome[J]. Archives of Neurology, 1999, 56(3): 303-308.
[11] Arkes H R, Blumer C. The psychology of sunk cost[J]. Organizational Behavior and Human Decision Processes, 1985, 35(1): 124-140.