# Financial Network Fraud and Legal Regulation

Yurong Zhao
*Continuing Education College, Nanjing University of Science and Technology, Nanjing, China*

Keywords: Financial Network Transactions, Financial Network Fraud, Social Security.

Abstract: With the development of the Internet, financial network transactions have provided convenience for daily life, but they have also given rise to the problem of financial network fraud. Fraudsters harm consumers' interests through false information fraud, leading to financial losses and psychological burdens, and increasing the public's concern about financial security. This study focuses on the types of financial network fraud, the implementation process and its impact on victims, and analyzes its impact on market stability and public trust. Through case analysis, normative analysis and literature research, it explores online loan and investment and financial management frauds, revealing the fraudulent techniques and victimization process to provide an effective basis for prevention. At the same time, it analyzes the deficiencies of existing financial laws and regulations and puts forward suggestions for improvement, aiming to improve the regulations, strengthen supervision, and enhance the public's financial knowledge, to curb financial network fraud and enhance the public's trust in the financial market.

## 1 INTRODUCTION

The development of Internet technology makes financial network transactions convenient but also brings serious financial network fraud. This kind of fraud is covert and efficient, the fraudster with the complex network environment to hide their identity, the lack of consumer safety awareness, coupled with defective laws and regulations and supervision, it difficult to resist the new fraudulent means, a serious threat to social security, improve laws and regulations, and strengthen the supervision can not be delayed.

Financial network fraud endangers personal and family property safety, disrupts the financial order, and affects economic stability, if not controlled, it will reduce public trust in the financial system and hinder market development.

This paper focuses on financial network fraud prevention countermeasures, focuses on the application of financial technology in anti-fraud, and aims to enhance anti-fraud capabilities. Enhancing public awareness of financial security, improving the financial regulatory system, and promoting financial technology innovation can help build a safe and transparent financial environment, enhance public trust, and promote healthy economic development, while publicity, education, and training are important ways to reach this goal.

## 2 OVERVIEW OF RELEVANT THEORIES

### 2.1 Explanations of Financial Network Fraud

Financial network fraud is diverse, sophisticated and harmful. Using false investments, impersonation of bank personnel and false loans, fraudsters take advantage of online anonymity and information asymmetry to lure victims into transferring money and undermine trust in the financial market. Victims not only suffer financial losses but also face the risk of personal information leakage and identity theft.

To this end, effective measures need to be taken by multiple parties. The government should strengthen the construction of laws and regulations, and increase the strength of the fight; financial institutions should improve security technology, strict identity verification, protection of customer information, and enhance the user's awareness of protection; the public should improve financial literacy, learn to identify fraudulent practices, and increase vigilance.

Combating financial network fraud requires the combined efforts of the government, financial institutions and the public to build a safe and healthy network financial environment, maintain social



Zhao, Y.
Financial Network Fraud and Legal Regulation.
DOI: 10.5220/0014293500004859

In *Proceedings of the 1st International Conference on Politics, Law, and Social Science (ICPLSS 2025)*, pages 39-43
ISBN: 978-989-758-785-6

harmony and stability, and protect people's wealth.

## 2.2 Types of Financial Network Fraud

With the rapid development of the digital financial ecosystem, fraudsters build a complex full-chain fraud system, bringing significant risks to the public. Investment frauds such as "Qianbao.com","OneCoin" and other counterfeit foreign exchange platforms occur frequently; credit fraud, unsecured loans charging high fees, and campus loans lead to a student debt crisis; payment fraud through phishing sites to steal information, the daily average intercept The average daily number of suspicious visits was 12,000 times. Identity impersonation and false service fraud are common, and cross-border financial fraud borrows from underground money banks and offshore platforms, making it difficult to combat. Fraud presents the characteristics of technology integration, life scenarios and organizational grouping, and it is expected that the proportion of technology-based fraud will reach 68% in 2024.

To this end, it is necessary to establish a "technical interception + manual intervention + public education" line of defense. Financial institutions to strengthen intelligent risk control, the public to enhance risk identification capabilities, the government to improve cross-border judicial cooperation mechanisms, and joint prevention of fraud, to protect public property security.

## 2.3 Means And Typical Cases of Financial Network Fraud

With the rapid development of the digital economy, financial network fraud is rampant, and diverse forms of harm. False information fraud is frequent, forged financial website or APP theft account to more than 50-million-yuan loss, P2P platform fraud amount rose 42% year-on-year, "Jin Sheng wealth" involved in the case of 2 billion. Technical attack fraud is serious, phishing to make financial staff lose 12 million yuan, malware leakage of 150,000 bank card data, and hacking virtual currency platform loss of 320 million U.S. dollars.

Impersonation of identity fraud is common, disguised as a financial institution requesting a verification code for more than 200 million yuan in losses, posing as a public prosecutor and social software theft fraud of 470 million yuan. Induce the operation of class fraud hidden, live platform false "stock god", brush single rebate caused 280 million, more than 500 million yuan loss. Cross-border composite fraud borrowing virtual currency and offshore server money laundering, the amount of money involved is expected to increase by 67% year-on-year.

The government, financial institutions and society need to cooperate to improve regulations, strengthen technical prevention and control and publicity and education to prevent and manage fraud and protect public property.

# 3 THE CURRENT SITUATIONS AND PROBLEMS OF FINANCIAL NETWORK FRAUD

## 3.1 Current Status of Financial Network Fraud

The rapid development of science and technology in recent years, network financial fraud technology, scene, and hidden trends are obvious, bringing great challenges to society. Sharing screen fraud has become a new type of means, and the amount of money involved in the first half of 2024 increased by 67% year-on-year; AI face-switching and mimicry technology is used for fraud, such as a marriage platform that cheated away 470 million yuan; false investment and financial management fraud is rampant, and a certain platform ran off the road after absorbing more than 2 billion yuan of funds in 2023 (The State General Administration, 2024).

Analysis shows that in 2023, the average age of victims of telecom network fraud is 37 years old, and the proportion of people aged 18-40 is 62.1%. Brush single rebate type of fraud is the largest volume of cases, accounting for 28.7%, such as Jiangsu Cao was cheated 420,000; false network investment and finance fraud cases with large losses, such as Anhui Zhang's investment foreign exchange losses of more than 1.4 million (Ministry of Public Security, 2024).

The online loan fraud problem is serious, 2025 A short video platform exposure of 23 illegal online lending platforms, involving 630 million yuan, habitually "unsecured", "violent collection" means, there is a "write-off of school loans". The increase in scams, the frequent appearance of false APP, cross-border money laundering difficult to track and other characteristics, cross-border crime is prominent, the

amount of money involved in 2024 increased significantly. Preventing financial fraud requires a multi-pronged approach to technology, regulations, and public awareness.

### 3.2 Problems Posed by Financial Network Fraud

First of all, in the digital era, network financial fraud means technologization, covert, and mainly technology-driven. Fraudsters set up a scheme with the help of AI face-swapping and other technologies, such as a dating platform that cheated 470 million in 2024 by relying on an AI virtual tutor (Zhang, 2024). New types of fraud penetrate emerging fields such as the meta-universe and iterate quickly (Xu, 2023).

Secondly, there are structural contradictions in the current regulatory system. Legal norms are lagging, and the Cybersecurity Law lacks detailed provisions on new cybercrime(Zhang, 2024); cross-border collaboration mechanisms are missing, and it is difficult to collect evidence from outside the country; and financial institutions' technological prevention and control are lagging, which increases the risk of loss (Yang, 2024).

Finally, network financial fraud affects individual victims, but also deepens the financial market trust crisis, 23% of Internet users due to fraud reduce online financial activities, a bank loss of more than 500 million. At the same time, the cost of social governance climbed, and the hidden social cost of telecom fraud in 2023 reached 2.8 trillion, the problem is widespread and serious (Chen, 2023).

In summary, in the face of increasingly complex online financial fraud, effective prevention and governance mechanisms need to be constructed from technology, law, public education, international cooperation and other levels.

## 4 ANALYSIS OF THE CAUSES OF THE PROBLEM OF FINANCIAL NETWORK FRAUD

### 4.1 Technology-Driven Escalation of Crime

In the digital age, the rapid development of technology has changed the means of online financial fraud. Fraudsters use AI face-swapping and deep forgery technology to build "full simulation" fraud scenarios, increasing the difficulty of identification. For example, in 2024, in the case of a dating platform, the fraud gang cheated 470 million yuan through the AI virtual investment mentor, and the difficulty of identification increased by 300%. 2023, the account theft cases caused by AI disguise surged by 147% year-on-year, which is a serious threat to financial security (Zhang, 2024).

The darknet ecology and vulnerability economy provide a hotbed for cybercrime, and the average price of financial vulnerabilities on darknet trading platforms reaches $150,000, leading to frequent cyberattacks (Xu, 2023). Technical outsourcing promotes the specialized division of labor of criminal groups, forming the "development - theft - money laundering" industry chain. Virtual currency money laundering technology is becoming increasingly complex, cross-border fraud funds after multi-layer currency mixing operation, the recovery rate is less than 5%. Criminals use privacy coins and cross-chain technology to hide traces, making it difficult for law enforcement authorities to track and combat.

Technological advances have made online financial fraud more efficient and covert, challenging financial security and social stability, and urgently requiring a tripartite synergy of technological upgrades, legal improvements and public education to reduce the incidence of crime.

### 4.2 The Governance Dilemma of Internet Fraud

In the digital age, telecommunications network fraud is rampant, posing a serious threat to the rights and interests of citizens and social stability, and because of the popularization of the Internet and smart devices, fraudulent means are varied, and governance is urgent.

China has built a legal framework with the Anti-Telecommunications Network Fraud Law, adopting full-chain governance, real-name system and multi-sectoral synergy, with heavy sentences of up to life imprisonment and sentencing based on the amount of money, and the joint formation of relevant laws to deter. However, there are problems such as vague norms in legal governance, poor cross-sectoral cooperation, insufficient corporate support, loopholes in the protection of personal information, and non-transparent anti-fraud technology.

Cross-border crime is difficult to combat, and international cooperation is urgently needed. Public

awareness of prevention is weak, education and publicity are scarce, compensation channels are poor, and some enterprises violate the law to assist fraud, increasing social security risks.

In addition, telecom network fraud governance is also facing systemic problems: fragmentation of the regulatory system, multi-sectoral management of authority and responsibility is chaotic and poorly coordinated; technological regulation lags and data sharing is difficult (Yang, 2024); cross-border regulation is weak, and any dark-network crimes; there are insufficient incentives for corporate compliance, and the penalties are small; and the mechanism of social co-governance is deflated, with ineffective reporting incentives and a limited role for industry self-regulation.

# 5 COUNTERMEASURES IN THE FACE OF FINANCIAL NETWORK FRAUD

## 5.1 Three-Dimensional Construction of Technical Defence and Control System

The rapid development of digital finance, the complexity of fraud risk in financial institutions, and building and upgrading AI anti-fraud systems have become the core tasks of commercial banks. For example, the deployment of intelligent risk control systems based on federal learning to model user transaction behavior can improve the accuracy of risk prediction, a bank introduced the new technology after the fraud identification accuracy of 99.8%, the response time is reduced to 0.3 seconds (Hu, 2023).

Blockchain technology provides a new solution for financial security, after the promotion of payment platforms, transaction data is uploaded to the chain in real-time, the traceability time is greatly reduced, transparency is improved, tampering is effectively prevented, and it is conducive to the prevention of fraud and the protection of consumers.

Multimodal biometrics technology is used for financial security protection, and a bank piloted a three-dimensional authentication system combining iris, voiceprint recognition and vivo detection, reducing the risk of identity fraud to 92% and enhancing verification security.

Financial institutions are changing traditional financial security protection through AI anti-fraud system upgrades, blockchain applications and multimodal biometrics to enhance security and create a safer financial environment for customers.

## 5.2 Multi-Dimensional Construction of Anti-Fraud Defence

The situation of telecommunication network fraud is grim, and there is an urgent need to govern it from various aspects.

At the legal level, the ambiguous provisions of the Anti-Telecommunications Network Fraud Law should be clarified, and technical regulatory rules should be formulated; in terms of the regulatory system, a national coordination center should be set up to coordinate multiple departments, clarify responsibilities, and ensure fairness in regulation, and the government should increase its investment in technological research and development and set up a data-sharing platform.

Cross-border crime-fighting, signing treaties such as mutual legal assistance, borrowing big data and Interpol to improve the efficiency of the fight. Enterprise management, giving policy support to compliant enterprises, penalizing non-compliant third parties, reviewing the implementation of the real-name system, and rectifying non-compliant enterprises. From the perspective of social co-rule, we will innovate publicity and education, set up a compensation fund and legal aid, optimize reporting incentives, and guide the improvement of industry conventions.

Adopting the above measures will enhance governance capacity, protect citizens' rights and interests, and maintain social stability.

# 6 CONCLUSION

Financial network fraud has evolved into a complex social problem, impacting the economy of individuals and families, and also bringing psychological pressure. Because of the complexity of the network environment in which they operate, consumers' weak sense of prevention, lack of financial knowledge, and lagging laws and regulations, the risk of economic damage, personal information leakage, and identity theft has risen.

Today's common types of fraud are investment, credit and payment, and the application of new technology has made them more insidious, with young people between the ages of 18 and 40 being the

main victim group.

To deal with financial network fraud, the government and financial institutions need to increase investment in cybersecurity, strengthen regulations and popularize public financial knowledge. All sectors need to build a systematic governance model, create a technical defense and control system, improve laws and regulations, and carry out public education and psychological intervention. Internationally, it is necessary to strengthen cross-border cooperation and data sharing, enhance the ability to regulate virtual currencies and emphasize support and risk education for small and medium-sized financial institutions. Through the multi-dimensional governance framework of technological innovation, legal improvement, social co-governance and international cooperation, we can break down sectoral barriers, curb the spread of fraud, and safeguard the safety of public property and market stability.

## REFERENCES

Chen Wanlin. 2023. *Research on Telecommunication Network Fraud Problems and Countermeasures for Prevention and Control in Rural Areas of Shehong City from the Perspective of Aggrieved Party.* Master's Thesis, Sichuan Agricultural University.

China News. 2024.07.24. *State General Administration of Financial Supervision Issues Risk Tips Warning Against These New Types of Wire Fraud.* Infromation on: https://www.toutiao.com/article/7395195686922256936/.

Hu Jinlian. 2023. *Research on Prevention and Countermeasures of Telecommunication Network Fraud in Commercial Banks.* Master's Thesis, North China University of Water Resources and Hydropower.

Penguan News. 2024.06.25. *Ministry of Public Security announced ten high incidences of telecommunication network fraud types: the number of losses caused by brush single rebate topped the list.* Information on: https://www.toutiao.com/article/7384283021916127770/

Xu Jingwei. 2023. *Research and Analysis on the Problems of Network Fraud and Illegal Crimes.* Master's Thesis, China University of Political Science and Law.

Yang Shaowan. 2024. Insufficiency and Soundness of Criminal Legislation on Network Fraud. *Legal Expo, Social Sciences* 1(08), 91-93.

Zhang Yu. 2024. *Research on Difficult Issues of Telecommunication Network Fraud and Its Related Crimes.* Master's Thesis, Zhongyuan Institute of Technology.