The Risk of Third-Party Payment and Its Prevention

Chunxue Liu, Ji Ling*

School of Accounting and Finance, Anhui Xinhua University, Hefei 230088, Anhui, China

Abstract: With the rapid development of the Internet, the third-party payment industry has evolved from scratch, moving slowly from an immature stage to its current gradually stable phase. It must be said that the emergence of third-party payment has fundamentally changed people's lives, evolving from the traditional "cash on delivery" model to the current e-commerce model of online shopping and merchant shipping. At the present stage, the development of third-party payment is in full swing, and its market share is continuously increasing. However, with the expansion of third-party payment resources and business operations, various risks have emerged, which are closely related to consumer rights and interests. Therefore, this article first explains the necessity of studying third-party payment risks. Secondly, based on found data and content regarding third-party payment risks, it systematically analyzes the various types of risks existing in third-party payments. Finally, corresponding solutions are proposed based on these risks to enable the healthy and stable development of the third-party industry.

***Keywords*:** third-party payment; risk; prevention

1. Introduction

With the development of Internet technology, traditional sales methods obviously cannot meet people's needs, making the emergence of third-party payment inevitable. The appearance of the third-party payment industry not only solves the disadvantages of long queuing times and inconvenience in banks but also meets people's payment demands, making life more convenient and efficient.

The vigorous development of third-party payment is determined by its unique characteristics. It utilizes Internet technology to transform traditional offline transaction payments into convenient online payments, changing the traditional "pay while receiving goods" model into the current e-commerce model. Although third-party payment is essentially a monetary transaction, it innovates the transaction model, enriches people's payment methods, and brings new experiences. However, as the market share of the third-party payment industry continues to expand, the risks of third-party payment institutions are becoming increasingly prominent. Due to the particularity of third-party payment, its risk manifestations are very unique. This not only concerns consumer rights and the development of the financial environment but also relates to the stable development of the national economic environment. Therefore, researching and preventing third-party payment risks is necessary for the third-party payment industry and even the entire market.

2. The Necessity of Preventing Third-Party Payment Risks

Third-party payment institutions serve as independent platforms bridging buyers and sellers. Third-party payment refers to consumers selecting goods when shopping online and paying through a third-party platform. Meanwhile, the merchant accepts the order and ships the goods. When the consumer receives the goods and provides no feedback to the seller within the specified time, the third-party institution transfers the funds to the seller's account. Because third-party payment possesses characteristics such as speed, security, payment flexibility, and fund guarantees, it can not only improve the supervision of product quality but also provide a solid foundation for commodity transactions.

Third-party payment makes life faster for people. Before its emergence, consumers had to go to a bank to activate online banking functions with a bank card to shop online. With third-party payment, consumers only need to register an account on a third-party payment platform and bind their bank card to consume directly, greatly accelerating the shopping speed. Third-party payment also has the characteristic of fund guarantees. During the process of purchasing goods, funds stay on the third-party payment platform for a period. During this time, the third-party platform must ensure the safety of the funds to guarantee that transactions between buyers and sellers proceed normally.

The relationship between third-party payment and banks is one of both cooperation and competition. Since the third-party payment model is largely similar to bank business models, the emergence of third-party payment has captured a significant portion of the banking sector, greatly reducing bank business volume. Through the above analysis, it is evident

that every industry requires business innovation over time and cannot remain static.

2.1 Standardizing the Business Operations of Third-Party Payment Institutions

It is well known that third-party payment is an emerging industry, and its rapid development was unexpected. Because the regulatory intensity and legal constraints on third-party institutions do not match their level of development, the state should promptly improve and refine relevant laws and regulations for the third-party payment industry. This ensures that third-party institutions have laws to follow and traces to track in their business operations, avoiding detours. The business operations of third-party institutions should also be supervised by relevant agencies. If a third-party institution operates unstably, it will affect consumer rights and, more seriously, may impact the automatic adjustment of the economic market, thereby affecting the stability of the national economy. The following sections will analyze a series of risks brought by third-party payment. These risks will affect consumers, merchants, third-party payment institutions, and even the entire financial market order, ultimately impacting national economic life. Therefore, to safeguard the healthy development of the entire economy, it is essential to strictly standardize the business operations of third-party payment institutions.

2.2 Protecting Consumer Interests

Consumers are the main subjects of third-party institution businesses. After registering an account on a third-party payment platform using their identity information, they deposit a certain amount of settled funds to conduct business or shop online. However, third-party institutions sometimes leak consumers' private information, causing serious impacts on their private lives. Settled funds essentially belong to consumers' property; third-party institutions only temporarily hold these funds and have no other rights. In reality, a large proportion of third-party institutions invest or lend out these settled funds to earn profits. The profits earned from funds that originally belonged to consumers are not given to the consumers. Even if they were distributed, the method and process of distribution would be a massive undertaking. Finally, the internal security technology of third-party institutions may not meet standards, leading to consumer accounts being hijacked, causing huge infringements on consumers' funds and personal information. From the above analysis, we know that consumers are the weaker party in third-party payments, so various measures should be taken to protect their interests.

2.3 Promoting the Healthy Development of Third-Party Payment Network Transactions

The third-party payment industry is flourishing, bringing visible benefits. However, technology is a double-edged sword, and third-party payment also introduces negative factors. While it brings much convenience to consumers' lives and promotes national economic development, incidents show that internal hacks of third-party institutions can leak consumers' funds and private information, causing huge losses. Furthermore, as the industry expands rapidly, more problems become apparent, such as the misappropriation of reserve funds and money laundering. This highlights the necessity of preventing third-party payment risks. Ensuring the safe and healthy development of third-party payment transactions protects consumer rights and ultimately promotes the healthy development of the third-party industry.

3. Risks Existing in Third-Party Payment

3.1 Traditional Risks of Third-Party Payment

3.1.1 Weak Fund Management

Unlike traditional transaction methods, when buyers use third-party payment for related commodity fund transactions, funds are first stored on the third-party payment platform. Only after the seller ships the goods and the buyer receives and confirms them as intact are the funds transferred to the seller's account. Therefore, funds stay on the third-party payment platform for a period. During large events like "Double 11" or "Double 12," the funds on these platforms are substantial. Looking at a broader scale, such as the annual payment scale of the third-party industry, it reached as high as 577 trillion yuan in 2025. Due to imperfect national management in this area and the difficulty for bank regulatory agencies to effectively manage the fund flows of these intermediaries, weak fund management issues inevitably arise.

Funds temporarily staying on the third-party payment platform paid by consumers are called "settled funds." Settled funds can be divided into "funds in transit" and "deposit funds." Funds in transit refer to the time lag between business processing and fund circulation during the purchase process; to ensure safety, these funds are temporarily custodied by the third-party payment platform. Deposit funds refer to the balance function opened by third-party platforms for quick consumption, where consumers transfer small amounts from their bank cards to the platform balance to spend directly.

Settled funds on third-party payment platforms generate significant potential risks. As long as funds stay briefly, third-party platforms may use them for investment. Investment inevitably carries risk, and the higher the return, the greater the risk. Therefore, to ensure the stable operation of the national economy, effective supervision of third-party payment

platforms is necessary.

3.1.2 Lack of Credit Risk

Although third-party payment has brought many changes to consumers' lives, some innovative steps have also introduced a series of problems, such as credit risk. In real life, credit risk refers to the losses caused by individuals or enterprises associated with third-party payment failing to complete their tasks on time [1].

Typically, buyer credit risk refers to the risk formed when a buyer places an order but fails to pay on time. Seller credit risk refers to the risk where, after the buyer places an order and pays, the seller fails to ship on time or ships damaged goods, leading the buyer to request a return because the goods do not match expectations or are of poor quality. Such risks not only increase operating costs for sellers but also reduce corporate reputation, leading to resource waste and environmental pollution. The credit risk of third-party payment institutions refers to the risk caused by the institution failing to perform agreed operations on time, such as investing funds and encountering risks that prevent recovery, causing unnecessary losses to consumers and merchants. Bank credit risk refers to banks failing to transfer funds in time, reducing fund liquidity, lowering user and merchant trust in third-party payment, and inhibiting its development [2].

Although third-party payment platforms have a credit guarantee function, transaction participants include not only the third-party institution but also consumers and merchants. Clearly, the functions currently possessed by third-party payment institutions cannot completely eliminate the credit risks existing between consumers and merchants. Therefore, there is a greater need to optimize the functions of third-party payment platforms to minimize existing risks as much as possible.

3.1.3 Decentralized Management of Reserve Funds

Reserve funds consist of two aspects: balances stored in third-party payment accounts by consumers, and funds temporarily held on the third-party payment platform due to the time lag between consumers and merchants completing transactions. Money deposited by consumers in banks and invested by banks to earn interest is legal. However, reserve funds differ from fixed deposits; they belong to consumers or merchants, not the third-party institution. It is illegal for third-party institutions to directly misappropriate reserve funds.

With economic development in recent years, the number of financing institutions has increased, and the scale of reserve funds has grown accordingly. Data shows that as of December 2025, reserve fund deposits reached 2.526022 trillion yuan [3]. A single third-party institution may control hundreds of millions or even tens of billions in reserve funds. Using these settled funds for investment can account for one-tenth of a company's total revenue, which is why there are increasingly more third-party institutions. However, investment inevitably involves risk, especially when clients are unaware. Once reserve fund investments fail, the resulting risks are enormous.

In practice, the management of reserve funds by third-party institutions is decentralized, and regulatory intensity is insufficient. For example, a single third-party institution may have anywhere from a dozen to over seventy accounts. Too many accounts increase regulatory difficulty. Although reserve funds make life more convenient and ensure transaction security, phenomena such as employees privately misappropriating funds occur. Therefore, the negative impacts of reserve funds require our serious attention.

3.2 Contemporary Risks of Third-Party Payment

3.2.1 Mobile System Security Design Flaws

With the rapid development of third-party payment, mobile payment is becoming increasingly popular. The development of smartphones and mobile payment makes life more convenient. Technology is double-edged, so third-party payment inevitably brings risks [4].

First is payment risk. On one hand, imperfect mobile system payment functions or completing payments due to input errors can cause huge losses to consumers. On the other hand, mobile payment allows direct transfers by simply entering the recipient's account number; if the number is entered incorrectly, who compensates for the mistaken transfer?

Second is performance risk. When a mobile terminal needs to handle a large volume of payment rates and business numbers in a certain period, it requires extremely high technical support. If mobile payment functions and business processing cannot be completed in a short time, it will affect user evaluation of the mobile terminal and even endanger user fund security.

Finally, there is security risk. On one hand, criminals believe mobile payment has a low security coefficient and use viruses to attack mobile internals to obtain and sell user information or commit fraud directly. On the other hand, hackers attack mobile internals to steal user balances, causing immeasurable losses to users.

3.2.2 Hardware Equipment Failures

Hardware equipment failure in third-party payment refers to risks where systems cannot complete work due to untimely updates or natural disasters. When hardware fails, transactions cannot proceed. For example, during Alibaba's annual "Double 11" event, especially the midnight rush, customers often report being unable to place orders or complete payments in time

due to system issues, missing the flash sale window. Hardware risks can be categorized as follows:

First, hardware intrinsic problems. Weak hardware capacity and processing power are direct causes; when business demand is high, the hardware itself cannot cope.

Second, hardware equipment management. Hardware should be inspected and maintained regularly. Research shows that JD.com has over 60,000 servers in the China Unicom Langfang Data Center. Managing and inspecting these servers requires significant effort. Slight mismanagement can lead to poor user experiences, affecting the future development of third-party institutions.

Third, backup hardware equipment management. In the event of natural disasters such as earthquakes, floods, or volcanic eruptions, the role of backup hardware systems becomes evident. Backup hardware should be established separately from main hardware, not in the same region. Additionally, backup hardware should be capable of sharing the load of the main hardware. When the main hardware faces high business demand and payment pressure, backup equipment can share the burden. If a third-party institution lacks backup equipment in such situations, users will doubt its operational capabilities, leading to a decline in reputation.

3.2.3 Rampant Telecom Fraud

With the development of the Internet and third-party payment, criminals have shifted their focus to the Internet industry. They send attractive links on websites containing Trojan horses to steal private information from network users. Worse, they impersonate merchants sending links similar to products; these links contain viruses that steal consumer information for sale or direct fraud. Logistics in online shopping have also become a focal point for fraud. Criminals falsely claim that a consumer's package is lost or contains contraband, sending SMS messages or making phone calls to defraud consumers, causing financial losses [5].

4. Countermeasures for Preventing Third-Party Payment Risks

4.1 Strengthening Commercial Banks' Risk Control over Third-Party Payment Business

4.1.1 Strengthening Legal and Regulatory Management

With the rapid development of the economy and science and technology, in an era where third-party payment prevails, its regulatory intensity and level have not kept pace with its application level. Although third-party payment is functionally similar to first-party payment (banks), various aspects of third-party payment are not as developed. Therefore, it is necessary to first position third-party payment correctly in the market and then strengthen and improve relevant laws and regulations [6-7].

First, relevant laws must be refined. We cannot vaguely apply general laws and regulations to risks arising from third-party payment; every detail must be regulated. For instance, strict measures must be issued for fund risks, especially cracking down on the private misappropriation of settled funds.

Second, previous legal penalties need to be increased. Criminal penalties should be added. Heavier punishments on top of civil penalties better reflect the authority of the law, instilling fear in third-party institutions. Alternatively, civil penalty amounts could be doubled, making the fine for misappropriation several times the amount misappropriated.

Third, protect vulnerable users. When settled funds are misappropriated and losses occur, if the third-party institution's capital is insufficient to repay these funds, users suffer the most. We must strive to protect vulnerable users. Regardless of the situation, users have the right to know how their funds are used. Therefore, while drafting legal charters, we must reflect legal fairness and also provide appropriate tilted protection for users in special circumstances.

4.1.2 Improving the Credit System

With the rapid development of third-party payment, the number of registered users is increasing, leading to higher business volumes for third-party institutions. To protect the rapid and healthy development of this industry, we need to accelerate the improvement of the credit system. Although domestic credit system construction started late, we can reference foreign systems, taking the essence and discarding the dregs, to learn and introduce gradually [8].

Domestically, there are no commercial rating agencies, only the personal credit reporting system established by the People's Bank of China (PBOC). Moreover, this system only records loan history for buying cars and houses. Apart from this, there are no other credit records. However, third-party payment users generate vast amounts of credit data. Combining PBOC data with third-party institution data would create a complete credit database, beneficial for the development of various industries and the national economy [9].

China can also establish a personal credit scoring mechanism based on a national credit big data foundation. For example, everyone could have a base score. Based on data, users could be classified into "good credit" and "poor credit," eliminating bad-faith consumers. Good credit users could be further divided into risk-lovers, risk-neutrals, and risk-avoiders.

This would help evaluate consumer spending levels in industries like the Internet, insurance, funds, and stocks, promoting the healthy development of the third-party industry, safeguarding basic consumer rights, and fostering healthier and faster national economic life.

4.1.3 Perfecting Internal Control Systems

Strengthen supervision and management of reserve fund accounts. Reserve funds belong to consumers; they are liabilities, not assets, of third-party institutions. The priority payment rights of consumers must be guaranteed.

First, separate the funds of third-party institutions from consumer reserve funds. Prohibit the private misappropriation of reserve funds for investment, lending, etc. If discovered, punish the third-party institution immediately.

Second, third-party institutions should pay a certain proportion of risk margin to the PBOC based on the reserve fund amount. This risk margin must be mandatorily submitted. Without PBOC permission, third-party institutions have no right to use it. The risk margin serves as compensation for consumer losses when the institution suffers asset losses. This not only guarantees consumer rights but also helps regulate market interest rates.

Third, third-party institutions should establish their own internal management systems, such as rules and regulations to manage the enterprise, risk control indices, and improving employee quality to standardize daily operations. These regulations can avoid various risks caused by improper operations, forming a good management mechanism. Improving employee quality not only enhances service attitudes toward consumers but also ensures the confidentiality of user personal information held by the institution, preventing leaks. More importantly, it prevents employees from privately misappropriating reserve funds for investment or personal spending.

4.2 Building Self-Improvement Mechanisms for Third-Party Payment Institutions

4.2.1 Artificial Intelligence Promoting the Development of the Payment Industry

The third-party payment industry is inherently composed of technology. Therefore, with future technological developments, the industry will see huge growth. Intelligent credit and intelligent investment advisory, bolstered by AI, are constantly surpassing old patterns, and the payment industry is gradually embracing artificial intelligence [10] [2].

Internet giants like Apple have already begun investing in and utilizing AI. As AI continues to develop, the financial sector will undergo new changes. Meanwhile, if the third-party payment industry wants to occupy a favorable position in the Internet, it must utilize AI technology. As long as basic scientific technology is sound and innovation continues, the third-party industry will become increasingly thriving. AI promotes the development of the third-party industry in three aspects:

First, AI can improve computing power. AI contains massive computing functions, enabling rapid data calculation and reducing computing costs.

Second, AI can improve algorithmic capabilities. In the third-party payment industry, users purchase various financial products. Improved algorithms can timely calculate what type of buyer a consumer is and recommend appropriate financial products, avoiding mismatches between products and consumer preferences.

Third, AI has data management and intelligent analysis capabilities. In the future, data protection is an area companies should focus on. How to manage data safely and effectively is a problem to be solved. However, deep neural network learning provides the greatest convenience for AI in data management and intelligent analysis. AI can also gain insight into and analyze a company's future development and decisions.

4.2.2 Big Data Enhancing the Advantages of Third-Party Payment Institutions

While preventing third-party payment risks, institutions can use big data technology to record users' browsing and consumption behaviors on mobile terminals on cloud servers, conducting continuous and comprehensive observations of user behavior. Such big data holds great value for third-party payment institutions.

First, big data can improve operational efficiency. Due to its timeliness and continuity, big data helps determine consumer preferences and the consumption status of third-party institutions, providing suitable products to consumers in a timely manner, improving sales rates, and increasing market share. This not only provides precise marketing value-added services but also offers valuable decision-making support for future business operations.

Second, third-party institutions can use big data to increase operating profits. By combining consumer consumption behaviors with merchant sales behaviors using big data, and then performing deep analysis and mining experiences, institutions can sell these materials as value-added services to merchants in need. This allows third-party payment institutions to gain extra value-added service fees, increasing corporate profits.

Finally, third-party payment institutions can use big data to build an ecosystem. By organizing and analyzing consumer consumption traces and browsing records, conclusions can be provided to merchants on the platform to improve their operational status, enhance the overall production and operation level of the third-party payment platform, and significantly increase the advantages of third-party payment institutions.

4.2.3 Biometric Recognition Ensuring the Security of Third-Party Payment

Following the widespread promotion of barcode and QR code payments, biometric payment may enter the next opportunity period. Biometric payments such as fingerprint, facial recognition, and voiceprint can better ensure payment security and speed.

For example, current facial recognition technology allows users to complete payments quickly by simply scanning their face like taking a photo, without needing to enter a payment password as before. Faces possess uniqueness and a user-friendly identification process. If third-party institutions link photos scanned on their platforms with authoritative photos from the public security system, they can more effectively prevent risks associated with third-party payment, making payments faster and more secure.

4.3 Increasing Protection for Consumers

4.3.1 Rationally Choosing Third-Party Payment Platforms

Facing so many third-party payment institutions in the market, consumers might be overwhelmed. However, to protect their rights from damage, consumers should choose platforms rationally. For instance, check if the platform has a high reputation, large scale, and how it compensates consumers if risks occur [11] [12]. Currently, many platforms offer cash gifts or coupons to attract users. When registering, consumers must protect their private information and not leak it for small gains.

Platforms with high reputations, large scales, and complete software/hardware facilities are suitable choices. With these elements in place, if risks occur, there will be comprehensive prevention and response strategies. These aspects demonstrate that the third-party platform is doing its utmost to reduce risks encountered by consumers, ensuring their rights are protected.

4.3.2 Strengthening Security Payment Awareness

As third-party payment platforms become more popular, incidents of fund theft from consumer accounts are countless. Consumer funds circulate between banks and third-party platforms; while these two platforms rarely experience fund theft, consumers still need to strengthen their security awareness.

First, do not click on various links seen online out of curiosity or inability to resist temptation, as they may lead to phishing sites and financial theft. Also, try to avoid logging into third-party payment accounts in public places like internet cafes, where Trojans installed on public computers can easily record account numbers and passwords to steal money.

Second, installing security protection software on mobile or computer terminals can prevent third-party payment risks. For example, using "360 Security Guardian": when consumers shop on shopping webpages, if they encounter fake shopping sites, the software will alert and intercept them, safeguarding consumer property security. It not only resolves dangers during shopping but also kills viruses during regular browsing or mobile infections. Recently, 360 Security Guardian has launched an online shopping compensation feature; if consumers suffer losses from Trojan viruses while shopping under the software's protection, the software provides appropriate compensation.

Finally, consumers should try not to preload excessive funds on third-party payment platforms. Regularly log in to check account balance dynamics. Pocket money can be kept on the platform for consumption, but larger sums should remain in bank cards to prevent third-party payment risks.

4.3.3 Properly Safeguarding Personal Information

When registering accounts on third-party payment platforms, some platforms require ID card numbers or bank card numbers. SMS verification is needed to activate third-party payment functions. Consider this example: a consumer discarded an unused mobile phone number, which entered the market for resale. The buyer used the previous owner's number information and SMS verification codes to log into the previous user's third-party account and made purchases, causing severe asset losses to the previous user. This highlights the importance of properly safeguarding personal information [13]. Before discontinuing a mobile number, cancel all associated third-party payment accounts, then cancel the number itself to protect consumer privacy. During online shopping transactions, never easily leak verification codes to anyone. Verification codes in online shopping act as one-time passwords; remain vigilant against anyone requesting them. After logging out of third-party accounts in public places like internet cafes, delete all account numbers and passwords to leave no traces for the next user. Ideally, change passwords on your mobile device after logging in at public places. Before discarding a mobile phone, remove the SIM card and erase all personal information from the device.

In the prevention of third-party payment risks, if consumer information is not leaked, there will be no channels for spreading such information, similarly reducing many related rights protection cases.

5. Conclusion

With the continuous development of technology, third-party payment has emerged. Actually, third-party payment

originated abroad, but in recent years, domestic third-party payment technology has made significant progress. The appearance of third-party payment has changed people's lifestyles, transforming shopping from "cash on delivery" to the e-commerce model, fundamentally altering how people shop. Technology is a double-edged sword; third-party payment brings both convenience and risks to people's lives. To safeguard the rights of all consumers and enterprises, corresponding suggestions must be proposed for existing risks to ensure the healthy development of the economic market and even the entire national economy. Through the analysis in this article, the following conclusions can be drawn:

First, third-party payment is an industry with huge development potential. Its development relates to the entire financial market and even the national economy. Therefore, studying third-party payment risks and how to solve them is highly meaningful for individuals or enterprises participating in transactions.

Second, through this article's analysis, we know that third-party payment not only faces issues like weak fund management, lack of credit risk, and decentralized reserve fund management but also problems such as mobile system security design flaws, hardware equipment failures, and rampant telecom fraud.

Third, this article proposes solutions to the various risks mentioned above to reduce risks on third-party payment platforms and maintain the safe development of the national economy.

Acknowledgments

This paper was supported by the following Funding Reimbursement Item: 2024 University-level Key Research Project of the Centre for Quality Education Research: “A Study on the Practice of Ideological and Political Education through University Curricula in the New Era: A Case Study of “International Finance A” (Project Number IFQE202407, Presenter: Wang Dandan).

References

[1] Deng Tao. Major Risks and Prevention of Third-Party Payment in China [J]. Finance and Finance, 2020, (05): 1-6.
[2] Zheng Sujuan, Zheng Kaiyan, Guo Junmo. Development and Risk Analysis of Third-Party Payment in China — Taking Alipay as an Example [J]. Financial Theory and Teaching, 2019, (05): 31-35.
[3] Fan Yehui. Research on Risk Control and Policy Suggestions of China's Third-Party Payment Industry [J]. Enterprise Technology and Development, 2021, (09): 195-197.
[4] Sun Liang. Research on Information Security Issues of Third-Party Payment under the Background of E-commerce [J]. Shanxi Agricultural Economics, 2019, (14): 165-166.
[5] Zhong Jie. Analysis of Current Status and Risk Prevention of Cross-Border Payment in China [J]. Marketing Circle, 2020, (52): 190-192.
[6] Li Wenmin. Analysis on the Application and Risk Management of Third-Party Payment in Public Hospitals [J]. Vitality, 2024, 42(06): 46-48.
[7] Guo Yang, Xie Yumin. Research on Risk Prevention and Control of Third-Party Payment Application in Public Hospitals from the Perspective of Internal Control [J]. Administrative Career Assets and Finance, 2024, (05): 115-117.
[8] Zhang Lin. Research on Risk Analysis and Prevention and Control of Third-Party Payment in China [J]. Think Tank Era, 2020, (08): 34-36.
[9] Xia Xumei, Pang Xuele. Research on Risk Analysis and Control of Third-Party Payment Based on Multi-Party Perspectives [J]. Commercial Accounting, 2019, (04): 92-94.
[10] Zhao Limin, Chen Hao, Li Liangliang. Risk Analysis and Prevention of Internet Finance Ecosystem Based on Financial Regulation Perspective [J]. Investment and Cooperation, 2024, (02): 1-3.
[11] Huang Saie. Risk Analysis of Third-Party Payment — Taking Alipay as an Example [J]. Industrial Innovation Research, 2021, (13): 47-49.
[12] Jiang Xiuhong. Brief Talk on Risk Prevention of Third-Party Payment [J]. Chinese and Foreign Entrepreneurs, 2020, (13): 84.
[13] Hu Jinfei. Research on Legal Risks of Third-Party Payment and Its Prevention Measures [J]. Journal of Harbin University, 2018, 39(07): 75-77.

Author Bio

Chunxue Liu (March 1999), Female, Han ethnicity, Postgraduate, Master's degree,Teaching Assistant, Green Finance.

Ji Ling (June 2000), Female, Han ethnicity, Postgraduate, Teaching Assistant, Financial Technology and Corporate Investment and Financing.