Proceedings of the 4th International Conference on International Law and Legal Policy
DOI: 10.54254/2753-7048/2025.30725

Research on Privacy Protection of Express Payment from the Perspective of Economic Law

Yang Han

China University of Political Science and Law, Beijing, China
631219491@qq.com

Abstract. Under the general trend of digital transformation, express payment has occupied a key position in modern financial transactions due to its characteristics of convenience and high efficiency. However, with the widespread application of express payment systems, incidents of user privacy leakage occur frequently, posing a serious challenge to the security of personal information. Based on this, this study attempts to explore the privacy protection mechanism of express payment from the perspective of economic law, analyze privacy risks, and propose corresponding protection strategies. Firstly, this paper presents the development background of express payment and its role in contemporary finance, analyzes the current situation of privacy protection in express payment systems, and points out the logic and existing problems in the collection and processing of user information. Then, from the perspective of economic law, the paper constructs a legal framework for privacy protection, combines international experience with the current situation of domestic laws, and elaborates on the legal basis of the right to privacy and the specific norms of economic law for privacy protection. On this basis, this study conducts an in-depth analysis of various types of privacy risks in express payment, uses Quantitative Risk Analysis for individual case risk assessment through case studies, and conducts in-depth analysis with the Critical Incident Technique to present the current privacy vulnerabilities in express payment. In response to these risks and deficiencies, this paper proposes a set of privacy protection solutions integrating technology and management, and advocates the simultaneous optimization of legislation and law enforcement. The paper discusses in detail the privacy protection measures based on database encryption technology, the application of the principles of data minimization and persistence in express payment, and conducts in-depth analysis of relevant management strategies such as data permission management and de-identification. On this basis, the paper also puts forward legislative and law enforcement suggestions on how to optimize the existing legal system and strengthen the law enforcement capacity of privacy protection. In summary, this study theoretically constructs an economic law framework for privacy protection of express payment, and proposes feasible privacy protection measures, providing key research perspectives and practical guidance for the innovative development of financial technology and the security of user privacy.

Keywords: Express Payment, Privacy Protection, Economic Law, Risk Assessment, Legal Framework

1. Introduction

With the rapid development of information technology, express payment has become one of the main modes of modern financial transactions due to its efficiency and convenience, exerting a profound impact on people's consumption habits and the financial ecology. However, with the widespread application of express payment, the problem of user privacy protection has become increasingly prominent. Frequent privacy leakage incidents have posed a severe threat to the security of personal information. The privacy risks behind various convenient services have made consumers pay more attention to their own information security, and such risks are more prominent when technology and law fail to effectively coordinate. Privacy violations in express payment not only affect user experience but also trigger extensive social discussions on user rights, financial security, and social trust. Against this background, it is crucial to conduct an in-depth analysis of the privacy protection mechanism of express payment from the perspective of economic law. This study aims to analyze the risks of information security from a technical perspective and, more importantly, explore and construct an effective privacy protection framework from a legal perspective to cope with the increasingly complex financial technology environment.

From the perspective of economic law, the legal basis of the right to privacy, the norms made by economic law for privacy protection, and how to closely link these laws and regulations with the actual operation of express payment are all key points that urgently need to be discussed. The right to privacy is not only a key component of personal freedom but also a crucial factor in the process of economic development. With the continuous increase of consumer data, how to ensure the security and privacy of personal information within the framework of economic law has become a major problem facing legislative and judicial practice. Although some achievements have been made in research in this field at home and abroad, most studies are limited to theoretical discussions, lacking self-reflection and practical exploration for practical applications in the current era. In view of this, this paper attempts to propose the principles of privacy protection from the perspective of economic law through in-depth analysis of the development status and current situation of express payment, analyze the legal basis of the right to privacy, and elaborate on the specific norms of economic law for privacy issues, laying a solid foundation for subsequent research.

In the process of analyzing privacy risks, this paper will examine various privacy risks existing in express payment. These risks may arise from technical vulnerabilities, improper user operations, third-party information sharing, and other factors. Through the analysis of multiple practical cases, this study uses quantitative risk assessment methods to evaluate these privacy risks and combines the Critical Incident Technique for discussion. This process can not only intuitively present the complexity of privacy issues but also reveal the specific challenges and response measures faced by privacy vulnerabilities, providing data support for legal rectification and system optimization.

Regarding the research on privacy protection countermeasures, this paper will propose a comprehensive solution combining technology and management, evaluate and optimize the existing laws and regulations, introduce advanced technical means such as database encryption technology, and focus on the application of the principles of data minimization and persistence in the process of express payment to improve the security of user information. In addition, it will analyze relevant management strategies such as data permission management and de-identification, and construct a comprehensive privacy protection system to provide effective guarantee for information security in financial technology.

This paper combines theory with practice, conducts a systematic study on the privacy protection mechanism of express payment from the perspective of economic law, and proposes feasible privacy protection measures, providing key research perspectives and practical guidance for the innovative development of financial technology. This study advocates strengthening the effective connection between legislation and law enforcement, awakening the whole society's attention to privacy protection, and building a sound ecological environment that can promote economic development through express payment while effectively protecting user privacy and information security.

2. Overview of express payment systems

2.1. Development and current situation of express payment

As an emerging payment method, express payment has developed rapidly since the 2010s with the widespread popularization of mobile Internet and smart phones. According to statistical data, China's express payment market has shown exponential growth in recent years, with its market size reaching nearly 40 trillion yuan in 2019 and is expected to exceed 100 trillion yuan by 2025. This payment method relies on the seamless connection of various third-party payment platforms and fast transaction processes. Users can complete payments by providing their mobile phone numbers or scanning QR codes without using traditional bank cards. Express payment has provided great convenience to consumers and has become an indispensable transaction method in e-commerce, offline retail, and the sharing economy.

With the rise of express payment, people have paid extensive attention to user privacy. Express payment involves personal sensitive information such as mobile phone numbers, bank card information, and shopping records, making the problem of user privacy protection increasingly prominent. According to a report from the cybersecurity industry, more than 60% of users are worried that their payment information will be leaked [1]. In the context of frequent hacker attacks and data leakage incidents, enterprises need to build an efficient privacy protection mechanism while achieving convenient transactions to prevent information from being abused and stolen.

At present, there are multiple express payment service platforms at home and abroad, and these platforms have implemented a series of measures to protect user privacy. For example, a well-known payment platform has introduced data encryption technology, using advanced algorithms such as AES-256 and RSA to encrypt user information to ensure data security during transactions. The platform has also adopted a multi-factor authentication mechanism, such as fingerprint recognition, facial recognition, and dynamic passwords, to improve the security of account access. Such measures have reduced the risk of user privacy leakage at the technical level, but they still face legal and ethical challenges.

Within the current legal framework, the actual situation of privacy protection faced by express payment is relatively complex. From the perspective of economic law, the privacy protection laws and regulations specifically targeting the express payment field are not yet perfect. Most of the existing relevant laws are derived from the Personal Information Protection Law and the Consumer Rights Protection Law. These laws and regulations stipulate the principles that payment platforms should follow in the process of information collection, use, and sharing, but they lack detailed content and enforcement power in specific operations and accountability, resulting in unsatisfactory privacy protection effects [2]. How to find an adaptive solution between the rapidly developing payment technology and the imperfect legal environment will become a key direction for future research.

The continuous development of express payment has promoted the innovation of financial technology and highlighted the urgency of user privacy protection. With the dual evolution of technology and law, the market demand for privacy protection will become increasingly urgent, prompting the continuous improvement of relevant legal systems and the strengthening of corporate

DOI: 10.54254/2753-7048/2025.30725

self-discipline. For researchers, exploring this field is not only of theoretical significance but also can help form a more reasonable and effective privacy protection mechanism in practice.

2.2. Analysis of the current situation of privacy protection

With the continuous development of science and technology and the rapid rise of Internet finance, express payment systems have become an indispensable part of people's daily lives. This payment method has gradually replaced traditional payment methods due to its convenience and efficiency, attracting a large number of users. However, the resulting privacy protection problems have become increasingly serious and have become the focus of social attention. According to the "2021 China Express Payment Market Research Report", the transaction scale of China's express payment reached 60 trillion yuan in 2020 and is expected to exceed 130 trillion yuan by 2025 [3]. Such a huge market scale has brought severe challenges to privacy protection while promoting economic development.

The current situation of privacy protection in express payment shows limitations in various aspects. On the one hand, enterprises lack transparency in the process of data collection and processing. Most users do not fully perceive the hidden dangers to their right to privacy when applying for and using express payment. According to the "2022 Network Security and Privacy Protection Survey Report", about 70% of users stated that they hold a passive attitude towards the collection of personal information during express payment and lack the initiative to understand relevant privacy policies [4]. In terms of the notification of the right to privacy and the user consent mechanism, the privacy clauses provided by many express payment platforms are relatively complex and lack comprehensibility, making users unknowingly give up control over their personal information [5].

On the other hand, the existing privacy protection legal system is insufficient in protecting express payment data. Although the Personal Information Protection Law came into effect in 2021 and set a series of behavioral standards for the processing of personal information, in the specific implementation level, there is a lack of clear legal norms and industry self-discipline standards for the specific scenario of express payment [6]. This situation has led to frequent occurrences of problems such as leakage and abuse of user privacy data during express payment, and users' trust in privacy information protection has continued to decline. According to the "2023 Digital Economy Development Report" released by the Cyberspace Administration of China, only 39% of users believe that express payment platforms can properly protect their personal information, and 43% of users have reduced the frequency of using express payment due to privacy risks [7].

The severity of the current situation of privacy protection is also reflected by the frequent occurrence of data leakage and hacker attack incidents. According to statistical data from Cybersecurity Ventures in 2022, the annual losses caused by cyber attack incidents have exceeded 600 billion US dollars, a large part of which is closely related to information leakage associated with user privacy. In the field of express payment, the consequences of incidents such as data theft and user information leakage will not only affect users' economic interests but may even trigger crises in their financial security. Several data leakage incidents encountered by payment platforms in recent years have sounded the alarm for the public, making people have a deeper understanding of the urgency of privacy protection [8].

While bringing convenience to users' lives, express payment has also brought many challenges to the field of privacy protection. Although national laws and regulations have begun to pay attention to and protect personal privacy information, there are still deficiencies in specific implementation. Faced with the increasingly complex situation of privacy protection, it is crucial to improve the

DOI: 10.54254/2753-7048/2025.30725

relevant legal system, enhance users' awareness of privacy protection, and increase the transparency of enterprise data processing. With the continuous progress of technology, building a comprehensive and systematic privacy protection mechanism will be an inevitable requirement for the development of express payment in the future.

3. Principles of privacy protection under economic law

3.1. Legal basis of the right to privacy

The right to privacy belongs to the category of basic personal rights and occupies a key position in the legal system. At the international level, Article 12 of the Universal Declaration of Human Rights clearly states that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence", which provides theoretical support for the legal basis of the right to privacy in various countries [9]. China's Constitution also stipulates the protection of citizens' personal freedom and the right to privacy, reflecting the state's emphasis on personal privacy rights. Articles 1032 and 1033 of the Civil Code clearly regulate the right to privacy and the protection of personal information, building a more specific framework for legal theory [10].

The connotation of the right to privacy includes the protection of personal information, family life, personal image, and other private fields. According to the provisions of the Civil Code, the infringement of the right to privacy includes the unauthorized collection and use of citizens' personal information. It can be seen that the basis for the legal protection of the right to privacy is citizens' control over their personal information. This control allows individuals to decide when, how, and under what circumstances to share their private information with others, thereby protecting their autonomy and personal dignity [11].

As a key legal tool for regulating market economic activities, economic law emphasizes the fairness and transparency of information in the transaction process. This principle extends to the protection of personal privacy rights in the field of economic activities, ensuring that consumers can fully understand how their information will be used and shared when conducting financial transactions. One of the legal bases in this field is the information asymmetry theory, which states that the unequal relationship between market subjects in information acquisition and use may lead to the infringement of the right to privacy. Therefore, legal intervention is crucial.

For express payment systems, with the rapid development and widespread application of technology, the purpose of the system is to improve the convenience of transactions. However, during the express payment process, data such as users' personal information, account information, and transaction records are likely to become targets of infringement of the right to privacy. In such cases, the legal basis of the right to privacy requires that institutions capable of providing legal protection have the ability to maintain information security, and also clearly defines the boundaries and exercise of the right to privacy [12].

In practical applications, the protection of the right to privacy needs to balance the relationship between transaction security and privacy protection. For consumers, relying solely on legal protection is insufficient. Economic law should refine relevant regulations, clarify the responsibilities and obligations of payment institutions in processing personal data, and ensure that users' personal privacy is not damaged while enjoying convenient services. The value of law lies in building a safe transaction environment through transparent rules and regulations, which not only enhances the public's trust in express payment systems but also reduces legal disputes caused by privacy issues.

DOI: 10.54254/2753-7048/2025.30725

Within the scope of economic law, the legal basis of the right to privacy has built a multi-level protection framework through international law, domestic law, and the particularity of economic activities themselves. Only by improving and implementing legal policies can we effectively ensure that personal privacy rights are fully protected in the field of express payment, and maintain the normal conduct of economic activities and the legitimate rights and interests of consumers.

3.2. Norms of economic law for privacy protection

The norms of economic law for privacy protection are mainly reflected in the management of the collection, use, storage, and transmission of personal information, emphasizing the principles of transparency, legality, and security. As a legal norm for adjusting economic relations between market subjects, economic law also needs to attach importance to the protection of personal privacy rights. With express payment increasingly becoming the mainstream payment method, its privacy risks have become more significant [13]. The norms of economic law for privacy protection can be analyzed from the following aspects.

Economic law clearly defines the definition and scope of personal information. According to the relevant provisions of the Civil Code, personal information includes name, date of birth, ID card number, phone number, address, and other aspects. Economic law needs to be based on a clear definition of personal information. When enterprises use personal information in the process of express payment, they must ensure its legality and follow the "minimum necessary" principle, that is, only collect personal information that is essential to achieve the transaction purpose, so as to avoid unnecessary information acquisition [2].

Express payment involves the collection and use of personal information. Economic law stipulates that the right to know and the right to choose of the information subject should be realized. When conducting express payment, consumers should be informed of the purpose of information collection, the method of use, and possible disclosure objects. Merchants and payment platforms need to clearly inform users through privacy policies to ensure that users agree to the collection and use of information with full knowledge [5]. The requirement of economic law for transparency has key normative significance.

In addition, economic law pays attention to information security protection measures. With the rapid development of Internet technology, personal information is vulnerable to the threat of hacker attacks and data leakage. Economic law clearly stipulates that information processors must take corresponding technical and management measures to ensure information security. For example, measures such as data encryption, identity authentication, and access control should be reasonably configured to improve the overall level of information security protection. For enterprises that experience data leakage incidents, economic law requires them to take timely remedial measures and assume corresponding legal responsibilities to protect the legitimate rights and interests of consumers [9].

In addition, economic law has also strengthened regulatory requirements in the transmission of personal information. When it comes to cross-border data transmission, economic law stipulates that corresponding international standards and domestic legal constraints should be followed. For cross-border transmission involving sensitive information, enterprises should evaluate the information protection level of the destination country to ensure that the information can be used legally and safely. This norm not only protects consumers' data privacy but also provides a guarantee for improving the country's information security level [9].

Economic law promotes the effective implementation of privacy protection through administrative supervision mechanisms. In the process of supervising the implementation of laws

DOI: 10.54254/2753-7048/2025.30725

and regulations, government regulatory authorities should strengthen compliance inspections of express payment enterprises, investigate and punish improper information use and privacy leakage incidents. By increasing law enforcement efforts, enterprises' legal awareness can be improved, and they can be ensured to act in accordance with relevant privacy protection regulations in their business operations [8].

Economic law has formulated regulations around the definition of the right to privacy, the collection and use of personal information, information security protection, cross-border transmission supervision, and administrative supervision, building a relatively comprehensive privacy protection norm system. In the rapidly developing field of express payment, continuously strengthening the implementation and improvement of laws and regulations to ensure consumers' privacy security will be a key direction for economic law to focus on in the future.

4. Privacy risks in express payment

4.1. Types of privacy risks in express payment

The privacy risks existing in express payment systems can be mainly summarized into the following types: data leakage risk, identity theft risk, transaction monitoring risk, and risks arising from service providers' data processing.

In express payment systems, data leakage risk is one of the common types of privacy risks. When users perform payment operations, they need to enter a lot of personal information, such as bank card numbers, mobile phone numbers, and addresses. Once this information is leaked due to system vulnerabilities or hacker attacks, users' privacy security will face a serious threat. According to some studies, data leakage incidents of payment platforms have occurred frequently in recent years, leading to an upward trend in the number of cases of user information leakage [4], affecting a large number of users.

Identity theft risk is also a major hidden danger in express payment. Once users' personal information is obtained by criminals, this information may be used to conduct unauthorized transactions, resulting in direct loss of users' funds. Moreover, identity theft may also cause users to bear unnecessary responsibilities when facing legal issues. According to statistics from the U.S. Federal Trade Commission, in 2019, the losses suffered by consumers due to identity theft reached 15 billion US dollars, and as many as 110 million users were affected [14].

Transaction monitoring risk refers to the possibility that third-party service providers may monitor users' transaction behaviors in real-time and collect users' consumption data during the express payment process. If these data are not strictly protected and processed, they may be used for big data analysis, affecting users' normal consumption activities. Users may not have sufficient right to know and right to choose regarding the collection of their privacy information, leading to an increase in distrust of the platform [12].

The risks existing in service providers' data processing cannot be ignored. In the era of express payment, payment service providers generally involve multiple participants, including payment gateways, banks, and third-party payment platforms. If these participants do not follow the corresponding data protection laws and regulations or take appropriate security measures when processing user data, it may lead to the leakage or abuse of user information. According to the provisions of the General Data Protection Regulation (GDPR) of the European Union, data controllers and processors are legally responsible for user data, otherwise, they will face heavy fines [9].

DOI: 10.54254/2753-7048/2025.30725

Overall, the types of privacy risks faced by express payment systems are diverse, and various risks are intertwined, which poses challenges to the protection of users' privacy. Strengthening user privacy protection measures, improving system security, and acting in accordance with relevant regulations are necessary conditions for ensuring the privacy security of express payment.

4.2. Individual case risk assessment and analysis

Individual case privacy risk assessment is an analysis carried out on real cases in express payment systems to identify and evaluate potential privacy risks. In this process, first, several representative express payment platforms, such as Alipay, WeChat Pay, and UnionPay Cloud QuickPass, are selected, and a systematic assessment is conducted on the privacy leakage incidents occurring on these platforms. The assessment content mainly focuses on the four key links of collection, storage, transmission, and use of users' personal information.

In the user information collection link, the widely used parameters include sensitive information such as users' names, phone numbers, addresses, and payment passwords. By comparing many incident cases, it can be found that a certain payment platform excessively collects personal information without clearly informing users, leading to data exposure. For example, some users reported that their transaction information was used in third-party advertising, and the platform did not follow the "minimum necessity" principle, which increased the risk of privacy leakage [2].

In the data storage link, it is necessary to focus on analyzing the database security measures of payment platforms. Through case analysis, it can be seen that a platform failed to use data encryption technology, resulting in the user information stored on the server being maliciously obtained after a cyber attack, and this information was not desensitized. The results of the risk assessment show that unencrypted data has a high exposure probability, and it is recommended that payment platforms adopt advanced encryption standards such as AES-256.

In the process of information transmission, encrypted transmission is crucial for protecting users' privacy. During the investigation, it was found that some payment platforms rely on unencrypted SSL/TLS protocols for data transmission, which greatly increases the risk of information being intercepted during transmission. In addition, some individual cases show that users make payments using public Wi-Fi without their knowledge, resulting in the illegal acquisition of their real-name information in the network and increasing the risk of abuse of personal information [8].

In the information use link, payment platforms need to formulate strict standards for the access control and subsequent use of user data. For example, a platform provided users' consumption records to third parties without the users' consent in order to cooperate with market research institutions, and these data involving users' privacy show great legal and ethical risks [5]. The risk assessment concludes that it is necessary to strengthen users' control over data use, and improve users' right to know and right to choose regarding such operations through the transparency of privacy policies and the user consent mechanism.

Using a risk matrix constructed by scenario analysis, a systematic assessment can be conducted on the occurrence probability and impact degree of different types of privacy risks. By classifying historical data events and deriving risk levels, it can provide a basis for formulating reasonable privacy protection strategies. In future research, quantitative indicators such as event occurrence frequency and impact scope can be considered to more effectively predict and prevent privacy risks, and ensure the security and compliance of the express payment environment.

5. Research on privacy protection countermeasures

5.1. A solution combining technology and management

The solution combining technology and management needs to improve the privacy protection level of express payment systems through multi-level comprehensive measures. At the technical level, methods such as data encryption, anonymization, and access control can be used to improve information security. Specifically, during data transmission, the use of AES 256-bit encryption algorithm can ensure the confidentiality of user information. In the data storage stage, hash algorithms such as SHA-256 are used to digest data, irreversibly converting sensitive information into a set of fixed-length characters, thereby reducing the risk of information being cracked. In addition, introducing multi-factor authentication technology to improve account security. Users are required to provide multiple identity verifications when conducting transactions, such as SMS verification codes, fingerprint recognition, or facial recognition, which can effectively reduce privacy leakage caused by account theft.

In the field of enterprise management, enterprises need to build strict information protection policies and privacy management frameworks. An effective privacy policy should cover the entire process of data collection, use, storage, and destruction, clearly define users' right to informed consent, and ensure that users can clearly understand the nature of the use of their personal information and potential risks during the registration and payment processes. Use Privacy Impact Assessment (PIA) as a decision support tool to build a risk management system to identify and evaluate potential privacy risks caused by data processing activities [5]. Formulate data leakage emergency plans. Once a data leakage occurs, emergency measures can be quickly activated to reduce losses, including timely notification of users and regulatory authorities.

In building a collaborative mechanism between technology and management, enterprises can use big data analysis to monitor user behaviors, analyze potential privacy risks through data mining technology, and promptly detect abnormal transaction activities to achieve real-time risk control. For example, machine learning algorithms can continuously learn user transaction behaviors and issue early warnings for suspicious activities. At the same time, management should regularly conduct privacy protection training for employees to improve their security awareness and ensure the effective implementation of various privacy protection measures.

Enterprises can cooperate with the payment industry to establish industry standards and cooperation mechanisms, and share best practices in privacy protection. Through cross-industry cooperation platforms, promote the interoperability and standardization of privacy protection tools, so as to maintain a consistent level of privacy protection for consumers across different payment platforms. Use blockchain technology to build a decentralized identity authentication mechanism, strengthen users' control over personal information, and improve transparency and trust [12].

The solution combining technology and management provides a systematic approach to privacy protection in express payment. By integrating advanced technical means and practical management measures, it can effectively reduce the risk of privacy leakage, protect users' legitimate rights and interests, and promote the whole society to attach importance to privacy protection, which is helpful for establishing a good market credit environment.

5.2. Suggestions for optimizing legislation and law enforcement

In the express payment environment, the importance of privacy protection is increasing. With the rapid development of technology and the continuous expansion of financial business, the

DOI: 10.54254/2753-7048/2025.30725

contradiction between convenience and privacy protection has become more prominent. In view of the current lack of privacy protection, the legislative mechanism and law enforcement mechanism need to be optimized to more effectively protect users' privacy rights [13].

At the legislative level, the primary task is to strengthen the legal framework and improve laws and regulations related to privacy protection. Although China's current Civil Code and Cybersecurity Law have initially defined the right to privacy, there are still deficiencies in the actual operation links. Therefore, it is recommended to formulate a special Privacy Protection Law, which clearly specifies the specific requirements for the collection, storage, use, and transfer of personal information during express payment [6]. This law should include clear user consent principles, data minimization principles, and information transparency requirements to ensure that personal information beyond the scope of business needs will not be collected without the user's explicit consent. Introduce a privacy impact assessment mechanism. Before the launch of any new technology or service, a privacy risk assessment must be conducted to fully protect users' privacy.

At the law enforcement level, it is necessary to strengthen the supervision and law enforcement of privacy protection. At present, the penalties for acts of infringing on the right to privacy are relatively low, which is difficult to form a sufficient deterrent effect. Therefore, it is proposed to establish a special privacy protection regulatory authority, which is responsible for conducting regular inspections on the privacy protection measures of express payment platforms and imposing penalties for illegal acts. The regulatory authority should have sufficient resources and authority to carry out on-site inspections, data audits, and user complaint investigations [8]. By establishing a rapid response mechanism, information leakage incidents can be handled more quickly, and the risk of user information being abused can be reduced.

It is necessary to establish an inter-departmental cooperation mechanism. Strengthening information sharing can improve the overall law enforcement efficiency of privacy protection. Regulatory authorities in various industries should share data related to express payment and privacy protection, promptly notify potential privacy risks and illegal acts, and increase the joint punishment for enterprises that violate regulations multiple times [5].

In the field of public education, the optimization of legislation and law enforcement must be accompanied by the improvement of consumers' awareness of privacy protection. By regularly releasing annual reports on privacy protection, popularize the significance of privacy protection to the public, enhance their understanding of privacy rights, and cultivate users' awareness of actively safeguarding their own right to privacy, forming a good social atmosphere.

Optimizing the legislation and law enforcement of privacy protection not only needs to start from the refinement of legal provisions but also should be promoted simultaneously in multiple fields such as law enforcement intensity, inter-departmental cooperation, and public education. Such comprehensive measures can build a safe and reliable user privacy protection network in the rapidly developing express payment system, protect the legitimate rights and interests of consumers, and promote the healthy development of financial technology.

6. Conclusion and outlook

With the prosperity of the digital economy, as a key component of financial technology, express payment has profoundly changed people's payment methods and consumption habits. However, the resulting privacy leakage and data security issues have become increasingly serious, becoming a core problem that needs to be solved. By systematically analyzing the current situation of privacy protection of express payment, this paper examines the application of economic law in privacy protection, and proposes a series of feasible privacy protection strategies, providing theoretical support and practical guidance for improving the security of express payment systems and the protection of user privacy.

The conclusion part first clearly states that express payment plays a key role in financial transactions. Its convenient and efficient characteristics have attracted a large number of users and promoted its rapid development. With this development trend, users' personal information and privacy are facing unprecedented risks. Research shows that there are deficiencies in the privacy protection measures in the current express payment systems, which increases the potential safety hazards of user information during data collection, storage, and processing [8]. From a legal perspective, although relevant laws and regulations are continuously improving, a systematic privacy protection framework has not yet been built. In this case, economic law is crucial.

Economic law has laid a legal foundation for the protection of the right to privacy, emphasizing the security of information and users' right to know, which is the key to building an effective privacy protection mechanism. Relevant legal norms should pay attention to data processing principles, use responsibilities, and protection measures for user privacy. Learning from international experience can provide useful references for China in the field of privacy protection, such as GDPR and its application in personal information protection practices [9]. After summarizing the analysis of existing cases, the paper finds that privacy risks are diverse, covering identity theft, data leakage, etc. These problems not only affect users' trust but also pose a threat to the development of the financial market.

In the suggestion part, considering the insufficient privacy protection of express payment, a dual strategy integrating technology and management is proposed. At the technical level, the security of user information can be improved by using advanced technical means such as database encryption and data de-identification. At the management level, it is necessary to strengthen data permission control and monitoring systems to ensure the legality and compliance of users' privacy information. The improvement of the legislative level is also urgent. On the basis of the existing legal framework, combined with market demand, special privacy protection laws and policies for express payment should be formulated to improve the enforcement of privacy protection [11].

There are deficiencies in the research process, specifically, there are certain limitations in the selection and analysis of some cases. Future research can consider a wider range of representative cases, which can deepen the understanding of privacy risks and formulate corresponding countermeasures. In addition, the interactive relationship between law and technology provides a broad space for exploration for subsequent research. It is necessary to conduct an in-depth analysis of the dynamic balance between the two to achieve effective privacy protection.

Looking forward to the future development trend, with the continuous advancement of science and technology and the gradual improvement of people's awareness of privacy protection, privacy protection in the field of express payment will face more opportunities and challenges. Multiple parties should be encouraged to participate, including financial institutions, technology providers, and legislative bodies, to cooperate and pool their efforts to promote the comprehensive implementation of privacy protection. Regarding the application of emerging technologies, such as blockchain and artificial intelligence, how to ensure user privacy while maintaining their technical advantages will become a key research direction [12].

Against the background of global digital transformation, examining the issue of privacy protection of express payment from the perspective of economic law is not only a challenge related to law and technology but also a very crucial topic in the process of social development. Conducting in-depth research and practice on privacy protection can promote the healthy development of financial technology and create a safer and more reliable payment environment for society. This

DOI: 10.54254/2753-7048/2025.30725

paper discusses this topic, which has theoretical contributions, and also hopes to provide practical guidance for society, helping the express payment field achieve sustainable development. It is expected that future research can go deeper into multiple dimensions such as the legal system, technical means, and user education of privacy protection, and promote the establishment of a more comprehensive privacy protection mechanism.

References

[1] China Cybersecurity Review Technology and Certification Center. (2022). Cybersecurity and privacy protection survey report [R].

[2] Liu, D. L. (2020). Legislative purposes and institutional construction of the Personal Information Protection Law. Chinese Journal of Law, 42(3), 102-119.

[3] China Payment and Clearing Association. (2021). Research report on China's express payment market [R].

[4] Cybersecurity Ventures. (2022). 2022 cybersecurity statistics report [R].

[5] Ding, X. D. (2022). A pluralistic governance model for personal information protection. Chinese Journal of Law, 44(1), 133-150.

[6] Zhou, H. H. (2020). Legislative positioning and major systems of the Personal Information Protection Law. Chinese Journal of Law, 42(4), 3-24.

[7] Cyberspace Administration of China. (2023). Digital economy development report [R].

[8] Li, M. (2021). Privacy risks and legal regulation of express payment in the era of financial technology. Studies in Law and Business, 38(2), 110-121.

[9] European Union. (2016). General Data Protection Regulation (GDPR) [S].

[10] Wang, L. M. (2020). Legislative highlights and application of the personality rights chapter of the Civil Code. China Legal Science, (4), 25-42.

[11] Zhang, X. B. (2021). Personal information protection: From personal control to social control. Social Sciences in China, (1), 106-127+207.

[12] Chen, S. (2022). Privacy protection and data utilization in the era of digital economy. China Legal Science, (2), 5-24.

[13] Huang, Y. Antimonopoly regulation of platform economy. China Legal Science.

[14] Federal Trade Commission. (2020). FTC consumer sentinel network data book 2019 [R].