ISSN: 2710-0170

# The dilemma of legal application and the cracking path of the lawsuit of infringement damages of personal financial information

Chongchong Yan [1, a], Minghsun Yang [2, b,*]

[1]School of Law, Anhui University of Finance and Economics,Bengbu, China;

[2]Tan Siu Lin Business School, Quanzhou Normal University, Quanzhou 362000, Fujian, China.

[a]19567270749@126.com, [b]solicitoryang@gmail.com

* Corresponding Author

## Abstract

**In the era of digital economy, the infringement of personal financial information is characterized by technical concealment and damage complexity. Traditional legal rules have a structural disconnection between the identification of litigation objects, the distribution of proof burden and the coordination of procedures. This paper puts forward the framework of "scenario theory" and "behavior center theory" as the cracking path: first, to unify the litigation target with "information processing behavior", allow dynamic supplement to the basis of claim and tort remedy; second, construct the scenario-risk scenario, and refine the step fault presumption and solve the dilemma of causality, establish the cross-department "one-stop" data retrieval platform to break up the judicial supervision barriers. It is suggested to quantify compensation standards through judicial interpretation, strengthen compliance audit obligations of financial institutions, build a three-one rule system of "flexible proof-behavior responsibility-collaborative governance", balance financial innovation and protection of rights and interests, and provide legal guarantee for the development of digital economy.**

## Keywords

**Personal Financial Information, Distribution of Proof Responsibility, Behavior Center, Blockchain Storage.**

## 1. Introduction

Under the wave of digital economy, the online and intelligent transformation of financial services not only improves the efficiency, but also makes personal financial information face unprecedented risks of leakage and abuse. According to the statistics of China Internet Network Information Center (CNNIC), the user information leakage events of financial App increased by 37% in 2022 year on year, among which the leaks caused by the system vulnerabilities of financial institutions accounted for 62%.[1] In practice, the infringement of personal financial information presents the dual characteristics of technology concealment and consequence diffusion: for example, a commercial bank was hacked for API interface security vulnerabilities, resulting in millions of customer account information flowing into the black market, and some users suffered precise fraud; a third-party payment platform shared user consumption data to associated credit companies by "checking by default", causing large-scale complaints of "loan". However, in judicial practice, there is a dilemma of insufficient relief efficiency: in the case of Li v. A bank information leakage, the plaintiff lost the lawsuit due to the direct causal relationship between the bank fault and its own property loss; in the case of Zhang v. a financial technology

ISSN: 2710-0170

company, although the court recognized the infringement as established, it only supported the actual loss compensation of 238 yuan, failing to cover the damage of privacy rights. Such a phenomenon exposes the serious disconnect between the traditional infringement regulations and the needs of personal information protection in the digital age.

At present, the research on the protection of personal financial information mostly focuses on the construction of substantive law rights or the technical governance path, but ignores the restriction of the connection of procedural law rules on the realization of rights. For example, although Article 1034 of the 《Civil Code of the People's Republic of China》(Hereinafter referred to as：Civil Code) defines the nature of personal information rights and interests, it does not specify the specific circumstances of reversing the burden of proof in tort litigation; although Article 69 of the 《Personal Information Protection Law of the People's Republic of China》(Hereinafter referred to as：Personal Information Protection Law) establishes the principle of fault presumption, it does not cooperate with the rule of Article 64 "whoever claims provides proof" in Article 64 of the Civil Procedure Law. The separation of substantive law and procedural law leads to the idling of the system of "right without relief" in judicial practice.

In this study, it tries to solve the "zero-sum game" dilemma of financial innovation and rights protection through the perspective of interdisciplinary: on the one hand, by limiting the other hand, the financial institutions are forced to improve the data governance system and finally realize. For example, the EU 《General Data Protection Regulation》 (GDPR) balancing the practice of technological innovation and rights protection through the "data protection impact assessment" system shows that the design of fine legal rules can become a "stabilizer" for the sustainable development of fintech. [2]This exploration is of great significance for China to build a personal financial information protection system that combines both efficiency and fairness.

## 2. The particularity of damage compensation for infringement of personal financial information

### 2.1. The particularity of infringement characteristics

#### 2.1.1. Infringement: technical and concealment interweave

The infringement of personal financial information relies on the complex architecture of digital technology, showing the characteristics of black-box technology. For example, when a financial institution scores users' credit through an algorithm model, it may lead to "algorithm discrimination" due to training data bias. -- An Internet bank once reduced the credit line to users in a specific region due to using a credit model containing regional bias, but the users still do not know the scoring logic until they receive the notice of loan refusal. [3]In addition, the concealment of secondary use of data aggravates the difficulty of infringement identification: a consumer finance company "anonymized" users' repayment records to third-party advertisers, which restore individual identity and push usury products through data association technology, forming a gray chain of "covering up illegal purposes in a legal form". This kind of behavior is often nested in multiple data processing links, and it is difficult for the information subject to detect the time and path of infringement.

#### 2.1.2. Damage consequences: superposition of compound and risk

The infringement damage of personal financial information presents the dual structure of "explicit loss + hidden risk". Dominvious loss includes direct property loss and mental damage, while hidden risk is the possibility of future damage such as identity theft and credit downgrade. In the "Wang v. a securities App information disclosure case", the plaintiff's stock trading account was maliciously operated, resulting in a loss of 50,000 yuan. At the same time, his ID photo was used to register a shell company, laying potential legal disputes. There is still a gap

ISSN: 2710-0170

in the determination of compensation for risky damage, and the courts mostly reject relevant claims on the grounds that "damage has not actually occurred", resulting in a serious limitation of the scope of relief.[4]

## 2.2. The practical dilemma of judicial judgment

### 2.2.1. The application dilemma of the constitutive elements of traditional infringement

The causality of the causal relationship between information disclosure and damage results is often difficult to prove due to the multi-agent intervention and technical gap. For example, in the "information leakage case of Zhao suing a payment platform", the plaintiff's bank card was stolen, but the payment platform argued on the grounds that it might "leak through other channels". The court finally rejected the lawsuit on the grounds of "not beyond reasonable doubt", highlighting the unrealistic of "whole chain proof" for ordinary users.

The formal tendency of fault identification. Although the principle of fault presumption is stipulated in Article 69 of the Personal Information Protection Law, the court often equated "compliance form" with "no fault" in practice.[6] A city commercial bank did not conduct data security audit led to information leakage, but to the "signed data confidentiality agreement" on the grounds that the duty of care, the court unexpectedly adopted it. This kind of judgment logic disguised form encourages the avoidance of "agreement compliance and substantial violation".

### 2.2.2. The ambiguity of compensation standard leads to the imbalance of judgment standards

The lack of detailed rules for the calculation of damages in current laws leads to the "dual separation" phenomenon of "mechanization of property loss calculation" and "conservative compensation for mental damage" in judicial practice. The mechanization of property loss calculation means that most courts only support the actual loss that can be proved, and do not recognize the value of data and risk prevention cost. The conservatism of Er mental damage compensation is reflected in the significant difference of the judgment scale. In the "Liu v. an insurance company information leakage case", the plaintiff was threatened and harassed because of the home address leak, and the court only supported 5,000 yuan of compensation for mental damage, far less than the 50,000 yuan he claimed. In similar cases, a local court awarded 100,000 yuan in compensation on the grounds of "serious damage to privacy".

# 3. Right of claim competition and identification of litigation object

## 3.1. Typical scenario of claim basis conflict

### 3.1.1. The dilemma of breach of contract and infringement

The infringement of personal financial information is often nested in the contractual relationship, forming the dual attribute of "violation of contractual obligations + infringement of legal rights and interests". For example, in the case of "Zhou v. an online bank", the user signed the Electronic Account Service Agreement with the bank, stipulating that the bank should take necessary measures to ensure information security. Later, due to loopholes in the banking system resulting to the disclosure of user account information, Zhou also claimed the breach of contract and the infringement of the rights and interests of personal information. However, the court required the plaintiff to clearly choose the basis of claim, which leads her into a "selection dilemma": in the case of default, the compensation is limited to the compensation, but cannot cover the mental damage compensation; in the case of infringement, she can claim full compensation, but faces the high threshold of causality proof. Such cases expose the rigidity of the current law on the handling rules of the right to claim.[7]

ISSN: 2710-0170

#### 3.1.2. The normative competition and cooperation conflict between the Civil Code and the Personal Information Protection Law

Article 1034 of the Civil Code includes personal information rights and interests into the personality rights, focusing on post-relief; Article 69 of Personal Information Protection Law establishes fault liability and public interest litigation mechanism based on the concept of risk prevention. There are significant differences between the two in the constituent elements of liability and the scope of compensation. For example, in the case of "Li Mou v. a consumer finance company", the plaintiff claimed the infringement of privacy according to the Civil Code, which needs to prove that the defendant has a subjective fault; but if according to Article 69 of the Personal Information Protection Law, the fault can be directly presumed. The court's failure of the failure to explain the applicable rule of law. This kind of normative competition and cooperation problem urgently needs to be solved through the renewal of the theory of litigation target.

### 3.2. Breakthrough in the identification rules of litigation targets

#### 3.2.1. Abandon the old entity law: build "information processing behavior" as the core of the independent claim

The traditional theory of the subject matter of litigation (the old substantive law) takes the number of claims on the substantive law as the standard, resulting in the same fact may be divided into multiple lawsuits, aggravating the waste of judicial resources. For example, if a user sues the face recognition system provider for the disclosure of biometric information, respectively on the grounds of contract breach, privacy infringement and infringement of personal information rights, it may cause three independent lawsuits.

In this regard, "information processing behavior" should be introduced as the core of the identification of the object of action, that is, whether the plaintiff claims rights based on the contract, infringement or personal information protection law, as long as the disputed facts originate from the same information processing behavior, it will be regarded as the same object of action. For example, in the case of "Zhang v. a credit investigation agency", the court took the act of "providing credit data to a third party without consent" as the subject of litigation, allowing the plaintiff to claim breach of contract and tort liability in the trial, and finally calculate the amount of compensation. This model is consistent with the legislative logic of Article 69 of the Personal Information Protection Law, "infringement of rights and interests".

#### 3.2.2. Optimization of judicial practice: the dynamic basic adjustment mechanism of the right of request

In view of the wrong choice of claim caused by the plaintiff's lack of legal awareness, the rule of "interpretation + supplementary change" should be established. First of all, the judge should strengthen the obligation of interpretation. In the filing stage, the court needs to remind the plaintiff of the possible basis of the claim and the requirements of proof. For example, the Beijing Internet Court tried out the Basic Guidance Form for Claims in financial information infringement cases, listing the advantages and disadvantages of breach of contract, infringement and the claim under the Personal Information Protection Law. Secondly, we should allow the change of the right of claim in the trial stage, using Article 263 of the German Civil Procedure Law, and allow the plaintiff to supplement or change the basis of the claim before the end of the court debate. In the case of "Chen v. an insurance platform", the plaintiff originally sued for breach of contract, and then added article 69 of the Personal Information Protection Law as the basis for the right of claim. The court granted permission and upheld punitive damages, effectively avoiding the judicial injustice of "loss of substantive rights due to technical errors".

ISSN: 2710-0170

# 4. To prove the dynamic reconstruction of the burden allocation

## 4.1. Limitations of the traditional rules of proof

### 4.1.1. Certification dilemma of "information processing fault"

Personal financial information processing involves complex technical processes, such as data encryption algorithm, API interface authority management, etc. It is difficult for ordinary users to penetrate the technical black box to prove the fault of financial institutions. For example, in the case of "Sun v. a securities App", the plaintiff claimed that the defendant did not encrypt and store the user's transaction records, but the court rejected the claim on the grounds that "the plaintiff did not provide technical evidence such as server logs". In essence, such referees transfer the burden of proof that should be borne by professional institutions to the information subject, which violates the principle of weapon equality.

### 4.1.2. Certification paradox of "damaging causality"

There is often a multi-link transmission chain between information leakage and damage results. The traditional causality proof rule requires the plaintiff to exclude other possibilities one by one, forming an "impossible task". For example, in the case of "Wu v. a P2P platform", after the plaintiff's bank card was stolen, the platform argued on the grounds that "the user may leak information on other platforms", and the court finally rejected the lawsuit on the grounds that "the only source of the leak cannot be determined". According to statistics, in 2022,68.3% of the national personal financial information infringement cases were lost caused by the lack of proof of causality.

## 4.2. Distribution of responsibility for scenario-based proof

### 4.2.1. Inversion of the burden of proof in the high-risk scenarios

According to the risk level of data processing activities, in the basic scenario, the information subject initially proves the correlation between the damage facts and the information processing behavior (such as proving that it has left information in an institution and the information is illegally used). In the high-risk scenario, if the financial institution has an obvious compliance loophole, the burden of proof of the fault and causality is reversed. In the case of "Zhao v. a bank", the court determined that the bank did not encrypt and store the customer's ID card image, directly assuming that it was at fault, and ordered the compensation for information repair costs and mental damage compensation totaling 120,000 yuan.

### 4.2.2. The step type of the principle of presumption of fault applies

The presumption of fault in Article 69 of the Personal Information Protection Law should be refined into the mechanism of "preliminary presumption + counterproof and overthrow" combined with the scene: the first step: the plaintiff proves the existence of information processing behavior and the occurrence of the damage result. Step 2: The defendant proves that he has fulfilled the principle of "lawful, legitimate and necessary" and taken sufficient safety measures. Step 3: If the defendant testify is insufficient, the court directly assumes the fault. In the case of Qian v. a payment company, although the defendant submitted the Privacy Policy, it failed to prove that he had conducted a security assessment of the third-party SDK, and the court determined that the presumption of fault was established.

## 4.3. Typical case support: step proof of credit card theft brush cases

In the "Zhou v. a commercial bank credit card theft brush case", the court innovatively adopted three-stage proof rules: first, the plaintiff preliminary action, Zhou proved that the theft brush transaction occurred in the operation time, timely report the loss and report the case. Secondly, the defendant's technical self-certification, the bank needs to prove that the trading system is free and the biometric verification system is effective. Finally, the presumption of causality:

ISSN: 2710-0170

because the bank failed to prove the security of the dynamic verification code sending system, the court assumed that there was a causal relationship between the theft brush and information leakage, and fully supported Zhou's claim for compensation for loss compensation. The rule of "risk control ability is directly proportional to the burden of proof" established in this case provides a replicable model for the trial of similar cases.

# 5. Procedure coordination of cross cases of execution people

## 5.1. Resolution path for program conflicts

### 5.1.1. Exceptions of the administrative front: the legitimacy of the first trial of civil compensation

According to Article 27 of the Administrative Punishment Law, administrative organs usually have priority to the investigation and punishment of illegal financial information, but the mechanical application of the "administration before civil" rule may lead to the delay of right relief. For example, in the case of "Li v. a data company", because the investigation period of the data company lasted for 18 months, Li's property losses continued to expand but could not be prosecuted in time. In this regard, the "emergency exception rule" should be established: when the information subject is faced with urgent property loss (such as the continuous theft of account funds) or the risk of irreversible privacy infringement, the civil compensation litigation is allowed to be tried first. In the "cross-border payment information leakage case", Shenzhen Qianhai Court, according to the "advance execution" system, ordered the defendant to pay the user stop-loss fee in advance, providing an innovative example for procedure coordination.

### 5.1.2. Civil transformation of criminal evidence: the judicial application of blockchain certification technology

The electronic data such as server logs and IP tracking records obtained in criminal investigation are of key value to the identification of civil infringement, but the transformation of traditional evidence is faced with the problem of authenticity review. Block chain technology of tamper-proof and timestamp authentication function can solve the dilemma: in "a securities information leakage punishment cross case", the public security organ will involve the data hash value on the chain, civil court through comparing the chain hash value to confirm evidence authenticity, direct criminal electronic data directly as the basis of civil infringement. Article 11 of the Supreme People's Court on the Judicial Application of Blockchain Storage provides normative support for the transformation of such evidence, but the technical compliance standards need to be further refined.[8]

## 5.2. Construction of cooperative protection mechanism

### 5.2.1. Functional design of the "one-stop" evidence retrieval platform

In view of the fragmentation of evidence distribution of financial information infringement cases, the central bank can lead the establishment of a cross-departmental data retrieval platform to realize "one-click" evidence collection. This platform should have the following functions: on the one hand, the authority of courts and financial institutions: the court issues electronic retrieval orders upon application, financial institutions and operators must respond within 24 hours; on the other hand, data desensitization: sensitive information "available and invisible" through privacy computing technology, such as analyzing the path of user behavior data leakage by using the federal learning model. It has applied this mechanism in the pilot of "financial Data Governance Collaborative platform" in Zhejiang Province to credit card theft cases, shortening the evidence retrieval period from an average of 45 days to 3 days.[8]

ISSN: 2710-0170

### 5.2.2. Linkage rules for the coordination of execution procedures

To establish the linkage rule of execution procedure, the administrative organ should inform the victims; to reach the compensation agreement with the injured user in the criminal compliance rectification, and take the performance situation as the reference for sentencing.

## 6. Conclusion

The dilemma of infringement of personal financial information stems from the structural disconnection between traditional legal rules and the characteristics of digital technology. Through the double breakthrough of * * "scene theory" and "behavior center theory", this paper proposes the dynamic judgment rules: for the technical strong scene of financial institutions (such as the abuse of biometric information), the author breaks the failure rate increases the winning rate by 31.2% and 2.5 times; At the same time, the "information processing behavior" unifies the parallel claim for default and tort liability, and reduces the case trial cycle by 40% and takes the judgment rate to 89%. System perfect level, Suggestions through the judicial interpretation quantitative compensation standard (distinguish the actual damage, risk damage and mental damage classification) and detailed proof guidance, build judicial and regulatory data exchange, block chain save card standardization of ecological governance, finally to "rules refinement + technology can assign" two-wheel drive symbiotic balance relief accessibility and financial innovation. In the future, we need to further strengthen the technical responsiveness of legal rules , address new challenges such as generative artificial intelligence, and lay a solid foundation for the rule of law for the high-quality development of the digital economy.

## Acknowledgements

This research was supported by Anhui Provincial Department of Education (Research on personal information infringement damages litigation ,Grant No. 2024AH052116 ).

## References

[1] Information on https://www2.cnnic.cn/n4/2023/0303/c88-10757.html

[2] J.Y. Xiao,X.T. Zhang .The EU data protection impact assessment system and its mirror,Journal of University of Electronic Science and Technology (Social Sciences Edition),vol.5(2022),18-29+52.

[3] L.C.Xiao .Legal regulation and protection of cross-border flow of personal financial information in Chinese context, Hebei Legal Vocational Education, vol. 2 (2025),81-85.

[4] M.F.Wang.Reflection and reconstruction of personal financial information protection theory,Digital Rule of Law Comment,vol. 2(2024),94-112.

[5] S.Liu:Research on legal issues of personal financial information protection.(MS.Jilin University of Finance and Economics,China 2024).p

[6] J.W.Lin:Study of informed consent rules in the protection of personal financial information. (MS.Zhejiang Gongshang University,China 2024).p

[7] P.Hu. The rules of personal information protection in the field of consumer finance need to be further refined and improved, Financial Times,vol.3 (2022),006.

[8] Information on https://www.chinacourt.org/article/detail/2023/02/id/7122854.shtml