International Journal of Education and Humanities
ISSN: 2770-6702 | Vol. 15, No. 1, 2024

Personal Financial Data Sharing Mechanisms within the Open Banking Framework

Ye Ju[1, *], Haoran Liu[2], Xinlin Zhang[3]

[1] Faculty of Law, College of Applied Arts and Science, Beijing Union University, Beijing, China
[2] Faculty of Law, GuiZhou MinZu University, Guiyang, China
[3] Faculty of Economics, Beijing Technology and Business University, Beijing, China
[*] ajuye@buu.edu.cn

Abstract: The development model of open banking is a necessary condition for commercial banks to achieve stable development in the digital era, and it can make data as a resource coupled with finance deeply. However, in practice, due to the relevant rules of open banking personal financial data sharing , there is a gap in legislation, inadequate implementation of relevant regulatory systems, the urgent of improving data privacy protection and many other practical difficulties. Therefore, there is an urgent needs to build a system for China's open banking financial data sharing system, which can be designed by drawing on the relevant rules of other countries and combining with China's specific realities, contrapuntally, through the establishment of a classification and grading authorization mechanism, the improvement of the "common vote" mechanism, and the sharing of black and white lists of the target bidirectional co-ordination model and other system designs, to facilitate the digital transformation and upgrade of financial institutions, and ultimately foster the development of new trends centered around consumer-centric personal financial data protection and open banking.

Keywords: Open Banking, Personal Financial Data Sharing, Data Privacy Protection, Regulatory Regimes.

1. Introduction

Driven by the advancements of FinTech 3.0 and Banking 4.0, the new development model of open banking has emerged as a mainstream trend in the global banking industry. This model breaks down data silos and facilitates the digitization and convenience of transactions. The open banking paradigm shifts away from traditional, physical banking towards a "de-physicalized" approach, aiming to maximize convenience and benefits for the public, thereby creating a "ubiquitous bank" accessible from anywhere. Within the framework of open banking, key challenges include preventing and mitigating major financial risks, preventing data leakage during data exchange, balancing macroeconomic control with individual autonomy, and legally regulating unauthorized sharing of personal financial data and preventing overreach in data sharing rights. Addressing these challenges is crucial for fostering innovation, synergy, and openness in the era of the digital economy.

2. Jurisprudence and Framework Explanation of Personal Financial Data Sharing within the Context of Open Banking in the Digital Age

Under the framework of open banking in the digital age, jurisprudence and the explanation of the regulatory framework for personal financial data sharing become paramount. The digital era is characterized by highly advanced information technology, which enhances the convenience and efficiency of all aspects of traditional social life. As a central component of commercial activities, the banking industry must lead in implementing the principles of convenience and efficiency within commercial transactions. Open banking, a novel banking model, focuses on the sharing of user financial data with third-party platforms. This model involves three legal entities, leading to more complex legal relationships and necessitating a robust regulatory mechanism. To safeguard the rights and interests of financial consumers, it is essential to first clarify the conceptual relationship between open banking and personal financial data sharing.

2.1. Concepts and Characteristics of the Digital Age

Digitization refers to a developmental model that integrates all aspects of human social life with digital technology, enabling the interconnection of all entities. The most significant characteristics of the digital era are openness, sharing, and compatibility. The sharing of personal financial data by open banks is a product of the digital era and is essential to realizing the core principle of sharing in this age. It plays a crucial role in the transformation and upgrading of the financial industry, accelerating the creation of a unified financial market and ecosystem, and helping the financial sector advance towards a more diversified and open new stage of development in the digital era.

2.2. Open Banking: Origins, Concepts and Characteristics

Open Banking represents a new development model in the banking sector where banks share user data with third parties within the business ecosystem. This model is characterized by the integration of various scenarios, platform-based services, and the shift towards de-physicalization. [1] The legal relationships under the Open Banking model differ from the traditional "bank-customer" linear, two-way relationships and involve three legal entities: banks, financial consumers, and third-party organizations. There are two types of tripartite relationships in this context (Figure 1). One is the "triangular relationship," and the other is the "linear relationship." The

linear relationship can further be divided into a bank-centered one-way contractual relationship and a customer-centered one-way contractual relationship, depending on the central entity involved.

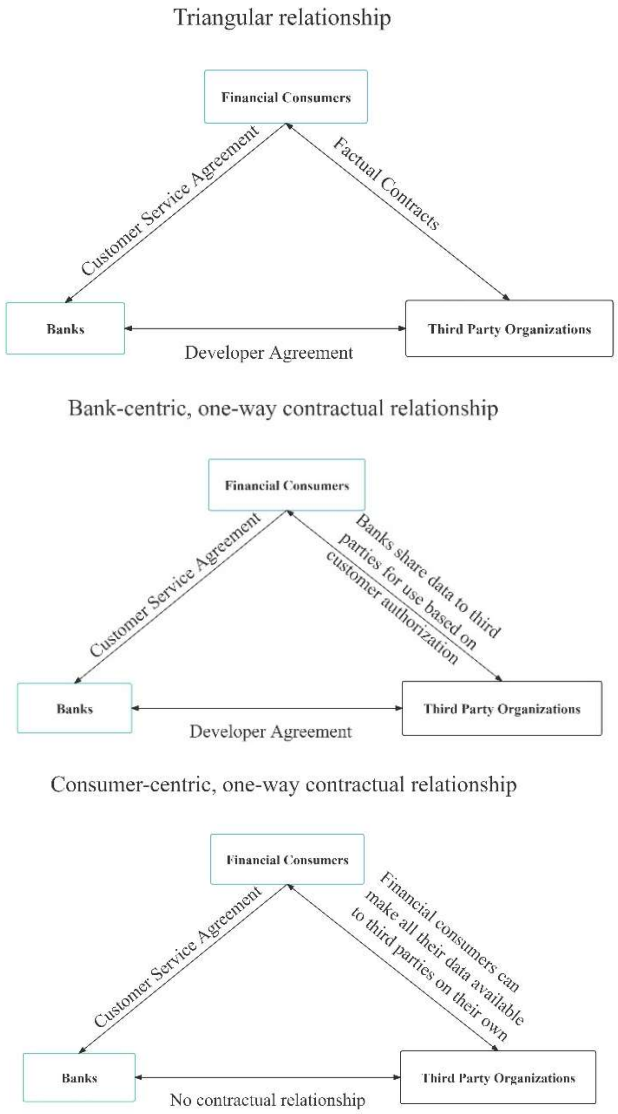

Fig.1 The relationship between three legal entities in Open Banking

Open Banking can be categorized into three stages of development based on time (Table 1): the nascent period from 2004 to 2013, the emergence period from 2013 to 2016, and the period of rapid development since 2016. There are two main development models of open banking in the world, one is the "top-down" regulation-driven development model represented by the United Kingdom, and the other is the "bottom-up" market-driven development model represented by the United States. China's open banking practice adopts a "bottom-up" market-driven mechanism.[2] The so-called "bottom-up" market-driven mechanism refers to the fact that China does not intervene in the operation of open banking practices through the introduction of mandatory standards by public authorities, but more through the delegation of power to the market, so that the market is able to summarize the specific norms and standards that are suitable for the operation of open banking in practice through its market players, industry associations, etc. This approach fully respects the autonomy of the private subject's will and the autonomy of private law.

Table 1. Stages of development of extra-territorial open banks

Time	Stage	Specific Performance
2004-2013	Nascent Period	Open Banking was kicked off with the promotion and application of PayPal API.
2013-2016	Emergence Period	The UK, the EU, and others have regulated the new model of open banking and the sharing of personal financial data under this model, either mandatorily or non-mandatorily, in order to ensure the long-term stability of open banking.
2016-present	Rapid Development Period	The United States, Japan, Singapore, Australia and other countries are also starting to layout open banking.

2.3. Personal Financial Data Sharing: Concepts, Scope and Types

Table 2. Classification of personal financial data

Classification and Scope of Personal Financial Data		
First-class Classification	Second-class Classification	Scope
Personally Identifiable Data	Personal natural information (except personal property information)	Name, gender, ID number, nature of work, home address, contact information, geographic location, etc.
	Personally Identifiable Information(Personal Identity Authentication Information)	Face, voice print, gait, ear print, bank card password, payment password, etc.
	Personal Situation Information(except personal credit information)	Information on defaulted executee, court session announcement information, case announcement information, etc.
	Personal Relationship Information	Recorded data used to describe the relationship between an individual and a related party
	Personal Behavior Information	Time of logging in to Internet banking, access time, web browsing history, etc.
Personal Financial Data	Personal Property Information	Personal income status, real estate status, vehicle ownership status, tax payments, etc.
	Personal Credit Information	Personal loan information, repayment information, etc.
Value Added Data	Personal Label Information	Personalized financial data generated by banks through big data analysis of financial consumers

Personal financial data encompasses all financial information generated during the process of receiving or using financial services by a specific natural person, which can identify the individual in a particular manner. Personal financial data can be categorized into three groups based on sensitivity: personal identity data, personal financial data, and value-added data.[2] Referring to the categorization outlined in the "Financial Data Security Data Security Classification Guidelines" issued by the People's Bank of China, personal financial data can be further subdivided into specific categories (Table 2).

2.4. The Relationship between Open Banking and Personal Financial Data Sharing: Carrier and Kernel

The relationship between open banking and personal financial data sharing is one of form and substance. Open banking serves as the carrier for personal financial data sharing, while the operational mode of open banking facilitates the transformation of personal financial data into a form of digitized property rights in a faster and more efficient manner. Personal financial data sharing constitutes the specific content within the operational framework of open banking and is a critical aspect of the new open banking model, essential for achieving significant development and digital transformation. The two are interdependent and mutually constraining.

2.5. Open Banking Personal Financial Data Sharing Framework Architecture

Within the framework of the open banking system, personal financial data are shared through a process whereby customers authorize the bank to circulate their personal financial information to third-party institutions by signing an agreement with the bank. Third-party organizations, such as third-party payment companies, platform-based Internet companies and consumer finance companies, obtain users' financial data primarily through the technical support of APIs (Application Programming Interfaces) and SDKs (Software Development Kits) (Figure 2).

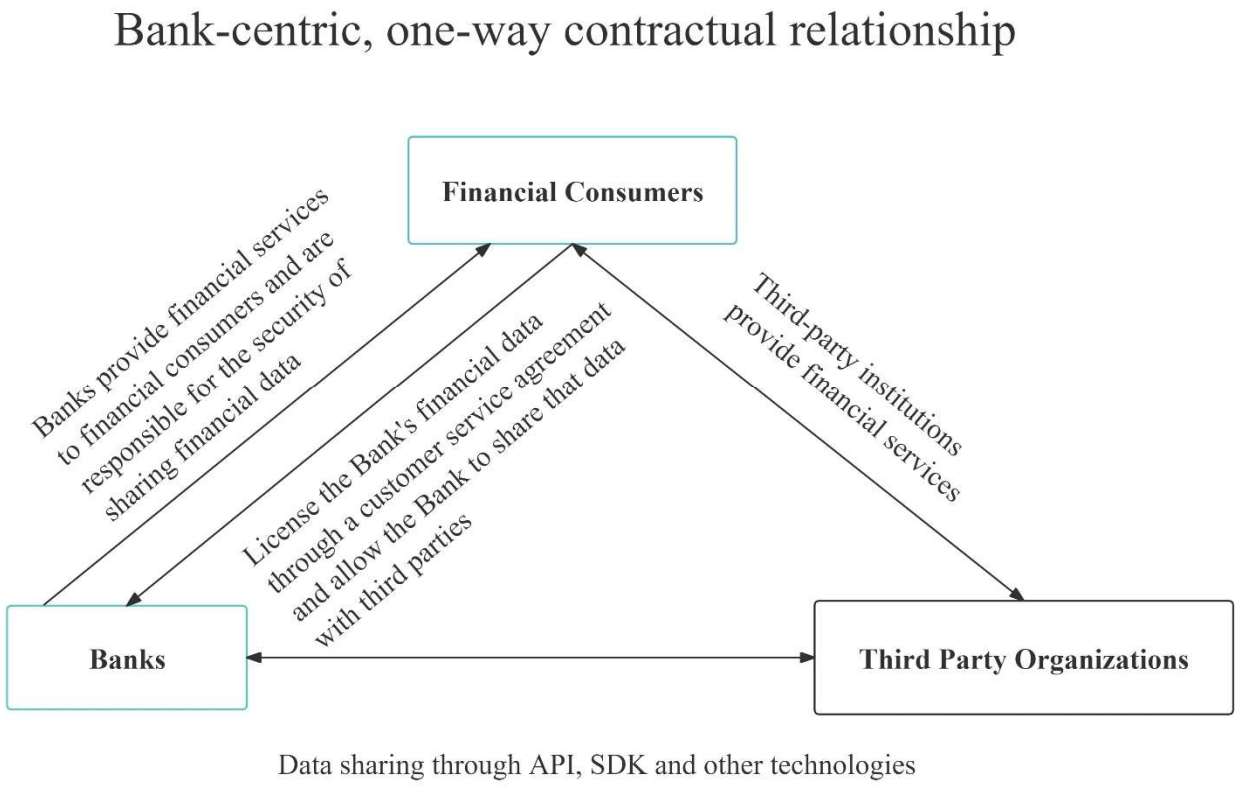

Fig.2 Shared Framework - Tripartite Subjects

The financial ecosystem of open banks is primarily divided into three levels (Figure 3). The primary components of the commercial ecosystem are third-party financial institutions, which include fintech companies and e-commerce platforms. At the middle level, there are two types of open banking platforms: self-built platforms and third-party platforms. The lower level consists of banks, which act as data providers. Banks can classify their existing data according to a unified logic, thereby efficiently transferring it to the middle level. This allows for the direct sharing of financial data through the open banking platform, enabling fintech companies and e-commerce platforms within the commercial ecosystem to directly access the personal financial data they require through the platform.[3]

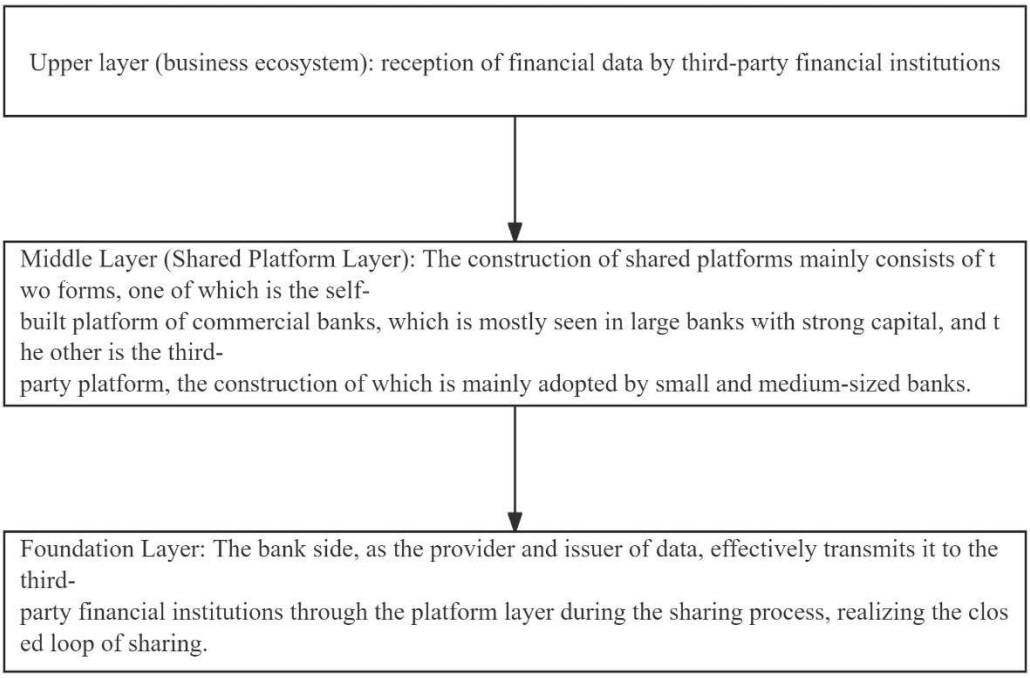

Fig.3 Shared Framework - Three Levels

3. Problems, Pitfalls, and Causes of China's Open Banking Personal Financial Data Sharing System

China has adopted a market-driven mechanism for constructing financial data sharing systems for open banks. The inherent contradictions of this mechanism, combined with China's legal practices and technological capabilities, have led to issues such as the "one-size-fits-all" application of the "informed consent" rule, inconsistent standards for data sharing and platformization, and unclear delineation of the rights and responsibilities of the three parties involved in financial data sharing. The emergence of these problems raises concerns about the development of open banking.

3.1. Institutional Dilemmas and Pitfalls of Personal Financial Data Sharing in China's Open Banking

Open banking has indeed introduced new "digital" dynamics into the development of China's financial ecosystem. However, there are still shortcomings in the implementation of the sharing system and the regulation of overarching laws.

3.1.1. Obligations and Responsibilities of the Three Main Parties are Not Yet Clear

In open banking financial data sharing, the intent to safeguard the rights of data subjects and prevent data privacy breaches must be achieved through the application of more stringent mandatory provisions on data processing and user rights. However, in practice, financial institutions may seek private gains by excluding or restricting the rights of data subjects or unreasonably mitigating their own obligations. Moreover, the operations of open banking are highly specialized, making it difficult for the general public to understand its operational logic. Therefore, the information disclosure obligations of data processors are particularly crucial. Nonetheless, there remains a legislative gap in practice regarding the imposition of obligations and the requirements for disclosure. When data leakage and data infringement occur, there is also a lack of clear legislative guidelines on remedial measures and liability determination mechanisms. This gap has contributed to the increasing number of data breaches and a mixed data market in reality.

3.1.2. Data Security Mechanisms are Not Yet Complete

Before personal financial data can be circulated for sharing, they must be subject to dual regulation by an authorization mechanism and a recipient selection mechanism to ensure the security of information flow and the data rights of financial consumers. Legislation in various countries mandates that data and information sharing must be authorized by the right holder in advance. In China, the authorization mechanism for personal financial data sharing follows a uniform "informed consent" approach. Regarding the recipient selection mechanism, China practices a "licensed" model.

The "informed consent" rule is applied in a "one-size-fits-all" manner. For different types of personal financial data, China's current laws, regulations, and industry guidelines still employ a uniform "informed consent" authorization mechanism. However, if distinct authorization mechanisms are not established for different types of data, it will be challenging to realize the true value of each data type.

The rigidity of the recipient selection mechanism is evident. The selection of third-party institutions in the open banking ecosystem follows a "licensed" model. That is, third-party institutions wishing to access financial consumers' data held by commercial banks through open banking must have their qualifications examined and approved by the state before a license is issued. However, from the original intent of constructing the open banking industry, the efficiency of granting uniform qualifications is relatively low and overly general.

3.1.3. There are Real Barriers to Data Flow

In the realm of data circulation, there are objective barriers to sharing practices. Data storage requires certain format

standards, and before sharing and opening up has been concretely implemented, the data format has not been standardized. This inconsistency has led various banks and financial institutions to store data in disparate formats.[4] Moreover, platform standards also exhibit significant variability. The lack of uniform standards creates obstacles for the interconnection and sharing of financial data under the open banking framework, forcing third-party institutions and commercial banks to spend additional time unifying data formats and creating a unified sharing platform. In some cases, different third-party institutions and the same commercial bank may adopt different data format and platform requirements. This results in a paradox where the cumbersome sharing practices contradict the intended convenience of the sharing concept. The inconsistency of domestic data standards and platform standards, coupled with the urgent need for improved de-identification technology and imperfect security assessment standards, highlights a disconnect between China's approach to data localization and the inherently international nature of data and ease of transactions.

Due to the wide variety of personal data, data formats are also diverse, such as XML, CSV, and JSON. The General Data Protection Regulation (GDPR) does not provide a standardized format to resolve this contradictory deadlock.[5] Additionally, the unification of platform standards faces similar issues, primarily reflected in the non-uniformity of API interfaces.

Moreover, the Cybersecurity Law of the People's Republic of China stipulates that personal information can exit the country only when there is a genuine business need to provide it externally and the criteria for a security assessment are met.[6] However, the criteria for security assessment remain undefined. This is due to the high transmissibility and unpredictability of risks in the financial industry and the fact that data is closely tied to national sovereignty, security, and livelihoods.

3.1.4. The Urgent Need to Regulate Personal Financial Data Sharing Practices

In practice, there are issues of ineffective implementation of regulatory systems. When addressing the risks associated with open banking data sharing, single regulatory approaches tend to create regulatory loopholes, while multiple regulatory approaches face the challenge of determining the primary regulator.[7] Additionally, since open banking financial data sharing is a dynamic process, it requires regulation through a dynamic and systematic approach. However, the regulatory model in practice still follows traditional financial industry regulatory frameworks, which can lead to correlated financial risks and trust risks that have a more significant impact due to ineffective regulation.

At the same time, the quality of data varies widely. The Personal Information Protection Law of the People's Republic of China clearly states that the quality, integrity, and consistency of data should be ensured when handling personal information.[8] Nevertheless, due to the need for encryption and de-identification in practice, there is a risk that personal data may be lost because of inadequate implementation of technical measures in personal data sharing.

3.2. Reasons for the Dilemma of the Personal Financial Data Sharing System in Open Banks in China

The systemic dilemma and associated concerns stem from the market-driven mechanism employed for the development of open banking in China, which has inherent limitations. Additionally, the inherent risks, as well as technical and legal constraints in the financial sector, have contributed to the emergence of institutional dilemmas and concerns.

3.2.1. Market-Driven Mechanisms Complicate the Application of Mandatory Standards

The rationale behind adopting market-driven mechanisms for developing open banks in China is deeply rooted in the country's financial practices. The financial market in China is characterized by autonomy, innovation, and market orientation. Implementing the regulatory-driven approach used by the United Kingdom and the European Union in China's financial market could stifle financial data sharing. From the perspective of competition law, regulation-driven open banking would compel all banks to share their financial data. While this might be more advantageous than disadvantageous in developed countries, China's financial industry is still in its nascent stages and has significant growth potential. Most banks in China are small and medium-sized, with insufficient capital and limited financial data.[9]Therefore, imposing an across-the-board liberalization would subject these banks to intense competition, potentially weakening them and exacerbating monopolistic tendencies. To protect the financial activities of small and medium-sized enterprises, China must continue to rely on market-driven mechanisms. However, the market-driven approach inherently lacks the standards needed for sharing financial data, and without government incentives, businesses are less motivated to participate in open banking. This is a critical reason for the numerous gaps in China's legislation regarding open banking.

3.2.2. Rigidity of Mechanisms Due to the Inherent Contagious Risks of Finance

Financial risks are inherently uncertain and highly contagious. Banks, as financial institutions, engage in a wide range of activities beyond just creating open banking platforms. Although open banking is essential for their transformation and modernization, traditional functions and services like credit, capital storage, and currency circulation cannot be abandoned. The goal of transformation and upgrading is not to break away from traditional practices but to infuse them with new growth momentum through the digitalization of modern technology. Within the framework of open banking, third-party organizations, which are also financial institutions, play a critical role. However, these institutions face several limitations. Firstly, they possess varying capacities for preventing and managing financial risks. If the third-party financial institutions involved in open banking have inherent risks or lack sufficient risk-bearing capabilities, it can lead to hidden data security issues throughout the entire process. Moreover, third-party financial institutions are profit-driven entities, and their profit-seeking behavior will be evident throughout the development of open banking. Consequently, the limitations of third-party financial institutions also weaken the financial system. This is why the government strictly regulates the sharing of personal financial data in open banks.

3.2.3. Objective Contradictions between Traditional Regulatory Models and Open Banking Data Sharing

With the rise of financial technology, tools such as big data, cloud computing, blockchain, and the Internet of Things can be leveraged to facilitate open banking practices. However, due to the technical shortcomings of these technologies, hastily applying them to regulatory procedures can result in inadequate implementation of the regulatory system, leading to heightened financial security risks. Therefore, the regulation of financial data sharing in open banks through digital technology is insufficiently applied in practice.

Currently, regulation primarily relies on the traditional financial industry model, with the China Banking and Insurance Regulatory Commission (CBIRC) overseeing the overall operation and implementation of open banking. This is supplemented by internal autonomous regulation and social supervision within the financial industry. However, the business model of open banks differs significantly from traditional financial operations, as it involves integrating data as a new production factor alongside traditional factors. Data itself has high liquidity and significant social attributes, making traditional regulatory mechanisms insufficient for ensuring the efficient flow of financial data. This mismatch leads to ineffective implementation of regulatory systems.

3.2.4. The Law Itself has Limitations

The law itself inherently has limitations, marking the boundaries of its role in social life. While the idea of legal omnipotence should not be advocated, neither should legal nihilism be favored. Specifically, the limitations of the law in the context of financial data sharing are reflected in the following ways: Firstly, the scope of the law's adjustment is limited. There exists an extrajudicial space within financial life that the law cannot govern entirely. Therefore, the law cannot manage every aspect of the financial data sharing process. Secondly, there is a contradiction between the characteristics of the law and the realities of financial life. The law is general in nature, while financial life is highly specific. This disparity leads to rigidity in the law's application. In addition, the law must be stable; as an embodiment of the state's coercive power, it achieves stability through the consistent application of legal provisions to maintain the existing basis of governance. Frequent adjustments to legal texts can lead to public mistrust, while financial life is continuously evolving. In the practice of open banking, China adopts a "practice before system" approach, resulting in inherent discrepancies between the law and financial realities. Thirdly, the formulation of the law is constrained by human factors. Legislators are not omnipotent, and the legislative process may not exhaustively consider all circumstances. This limitation means that the law may not fully account for the dynamic and complex nature of financial activities. Fourthly, there are inherent limitations within the law itself, including gaps in legislation and legislative loopholes. Such loopholes are inevitable because financial life, and social life more broadly, are constantly changing. Additionally, the law often contains ambiguities at the semantic and textual levels, which complicates the implementation of rights such as data portability in financial data sharing.

These limitations are not flaws in the law; they are insurmountable realities that highlight the need for targeted relief for each specific manifestation. Rather than seeing these limitations as defects, it is crucial to understand them as inherent characteristics of legal systems that require thoughtful and adaptive solutions in practice.

4. Examining and Learning from the Legal Regime of Personal Financial Data Sharing of Open Banks in the Extraterritorial Area

4.1. U.S.: Financial Consumer Protection and Open Banking Personal Financial Data Sharing Regulatory Model

Table 3. The Regulatory Framework and Content of Open Banking in the United States

Uniform Money Services Ac(UMSA)	Licensing of money transfers (including money transfers, sales of payment vouchers and certain types of Internet payment services);
	Licensing system for check cashing and currency exchange
	Offers new ways to manage top-ups and e-money
Dodd-Frank Wall Street Reform and Consumer Protection Act	Expanding the authority and scope of supervision of regulatory agencies and conducting risk regulation measurement
	Appropriately expand the regulatory responsibilities of the Federal Reserve to supervise all systemically important banks and non-bank financial institutions
	Strengthening consumer and investor protection
	Strengthening the supervision of the banking derivatives market
Electronic Funds Transfer Act(EFTA) and Regulation E	Detailed regulations on fund allocation, consumer liability, and financial institution liability
	Allocation of responsibilities in the allocation of funds according to different perspectives such as civil, criminal and administrative
Principles of Consumer Finance Data Sharing and Integration	Dispute resolution and liability for access to personal data, data control or consent, authorized payments, security, transparency, accuracy and unauthorized access to data

The U.S. government empowers consumers with the right to choose and the right to know as much as possible, and realizes the protection of financial consumers' rights and interests through the Principles for the Sharing and Integration of Consumer Financial Data.[10] In addition, the U.S. regulatory model for open banking is also worthy of China's reference (Table 3).[11]

The United States adopts non-mandatory rules for open banking financial data sharing, i.e., it gives the market the greatest degree of self-regulation and empowers banks to make adjustments to the relevant specific systems. At the same time, the U.S. government also gives consumers the right to choose and the right to know as much as possible, and realizes the protection of consumer rights and interests at the level of financial data through the Principles for the Sharing and Integration of Consumer Financial Data. In addition, through the enactment of the Dodd-Frank Wall Street Reform and Consumer Protection Act, the U.S. has expanded the authority and scope of regulatory agencies, making the scope of its supervision broader, the number of regulatory matters has increased accordingly, and risk supervision and

evaluation, and the U.S. has also expanded the supervisory responsibilities of the Federal Reserve through the Act, so as to make it more convenient for the exercise of supervisory rights and fulfillment of supervisory obligations. Regulatory Obligations. At the same time, the U.S. through the Electronic Funds Transfer Act and the promulgation of Regulation E, the consumer responsibility and the responsibility of financial institutions to carry out detailed provisions, so that the responsibility is clearer, but also indirectly accelerate the quality and efficiency of the construction of open banking.

4.2. EU: Dual Regulatory System for Open Banking Personal Financial Data Sharing

The EU's GDPR attaches great importance to network and digital security. The GDPR clearly stipulates that third-party financial institutions shall not store users' sensitive personal information and defines the scope of sensitive personal information, requiring third-party organizations to clear it when it is used up and not to retain it.[12] The protection of financial data in the EU has evolved from the era of "The Data Protection Directive" to the era of "The General Data Protection Regulation," and the EU has gradually built up a dual normative system (industry code of conduct + mandatory rules of law). The specific application of the dual normative system in practice is mainly manifested in the following ways: on the one hand, the EU clearly stipulates in the GDPR that all data can only be disclosed and shared with the consent of the customer, and any sharing without the customer's authorization is considered a data infringement,[13] which is an extremely stringent mandatory rule. Through this approach, the safety and stability of financial data sharing can be fully guaranteed, and the high level of legislation also highlights the EU's rigorous attitude towards the sharing of financial data.[14] On the other hand, the EU has delineated the scope of competence of financial institutions through general and overarching provisions, without completely restricting their activities.[15]Specifically, the relevant financial industries of EU member states can further refine the original overarching provisions through the formulation of industry standards and carry out flexible legislation on specific issues of data sharing. This approach gives full play to the flexibility and initiative of the market, making open banking financial data sharing more efficient and convenient.[16] This regulatory framework ensures that data security issues are addressed, it also maintains the original vitality of the financial market by effectively balancing decentralization with control.

4.3. UK: Differential Access Rights for Third-Party Institutions and Implementation Architecture for Open Banking Personal Financial Data Sharing

The UK Competition and Markets Authority (CMA) launched the Financial Sharing Initiative in 2015, and in 2016, the Open Banking Working Group (OBWG) issued the Open Banking Standards Framework. This framework categorizes bank data, including open data, customer transaction data, customer reference data, aggregated data, and commercially sensitive data. These five categories, depending on the degree of sensitivity, allow the bank side to set differentiated read access rights for third-party organizations. The implementation structure of open banking financial data sharing in the UK is also more focused on government macro-control. Specifically, the implementation of the UK open banking industry is outlined first by the CMA through top-level system design, followed by the formation of the "Open Banking" program Implementation Entity (OBIE) led by the CMA, which is centrally responsible for the system design of open banking financial data sharing. Under the organization and coordination of OBIE, the major banks have successively formed groups to implement the plan. In addition, in terms of regulation, the UK government has adopted a "regulatory sandbox" model, i.e., the UK Treasury, the CMA, the Financial Conduct Authority (FCA) and the Payment Systems Regulator (PSR) have formed a Joint Regulatory Oversight Committee (JROC) to oversee the practice of open banking financial data sharing.

4.4. Lessons and Insights

Comprehensive Regulatory Frameworks: The EU's GDPR serves as a model for developing comprehensive regulatory frameworks that balance stringent data protection with the need for innovation in financial services. The integration of mandatory legal requirements with industry-specific guidelines ensures high levels of data security while allowing for regulatory flexibility and adaptability.Balancing Innovation with Regulation: The UK's regulatory sandbox approach underscores the importance of fostering an environment that encourages innovation while maintaining robust oversight. This model facilitates the testing of new technologies and business models within a controlled regulatory setting, which is crucial for advancing the financial sector.

Emphasizing Consumer Consent and Control: A common thread in the regulatory frameworks of the EU, UK, and US is the emphasis on consumer consent and control over personal financial data. Ensuring that consumers are informed about and agree to how their data is used is essential for maintaining trust and compliance with data protection regulations.

The Need for Unified Regulatory Approaches: The diverse regulatory landscape in the US highlights the challenges posed by having multiple regulatory bodies and varying state-level regulations. A more unified regulatory approach, similar to that of the EU, could provide clearer guidelines for financial institutions and enhance the protection of personal financial data across different regions.

Flexibility and Industry Participation: The EU's dual regulatory system and the UK's differentiated access rights approach demonstrate the benefits of involving industry stakeholders in the regulatory process. This ensures that regulations are practical and can be effectively implemented across various sectors, maintaining the flexibility required for industry-specific needs.

Adapting to Technological Advancements: All three regions recognize the necessity of adapting regulatory frameworks to keep pace with technological advancements in financial services. Ensuring that regulations are flexible enough to accommodate new technologies while maintaining stringent data protection standards is crucial for the future of open banking.

By examining the policies and regulations of the EU, UK and US, it is clear that a balanced approach integrating robust data protection measures with the flexibility to foster innovation is essential for the successful implementation of open banking and the secure sharing of personal financial data. Each region's regulatory experiences offer valuable insights for developing effective and comprehensive frameworks

globally.

5. Suggestions for the Personal Financial Data Sharing System under the Open Banking Framework in China

China's current open banking framework still faces significant challenges, such as ineffective regulatory enforcement and varying data quality. To fully align with contemporary trends and propel the financial ecosystem into its next golden era, these issues must be thoroughly addressed.

5.1. Concept and Framework for the Construction of a Personal Financial Data Sharing System for Open Banking in China

China has traditionally adopted a "bottom-up" approach in constructing its open banking framework. This market-driven approach can continue to be utilized in building an open banking financial system, but it should be complemented by macro-level intervention. Such intervention is necessary to rectify market inaction and misconduct, and to delineate clear boundaries of rights and mandatory obligations. This dual approach will ensure a more stable and robust construction of the open banking model in China.[17]

Specifically, the system can be structured at the following three levels (Figure 4). The combined efforts of the state, society, and individuals will better align the open banking personal financial data sharing system with China's practical development needs.

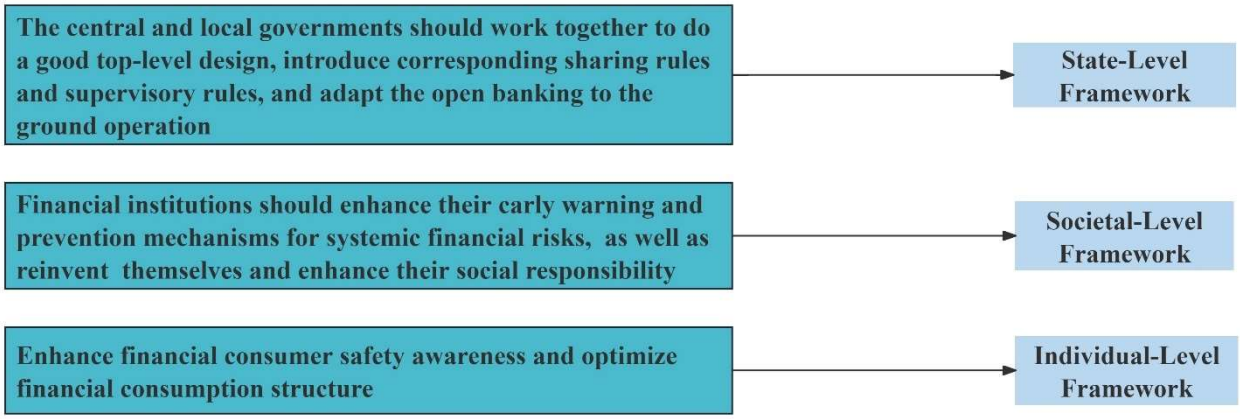

Fig.4 Personal Financial Data Sharing System Construction Model

5.2. Proposed Specific Rules for Open Banking Personal Financial Data Sharing in China

The systemic challenges that arise within the framework of open banking in China are interconnected rather than isolated issues. Therefore, these challenges must be comprehensively analyzed to understand their causes and potential pitfalls, ensuring that solutions address the root causes. Specific measures include establishing a robust classification and authorization mechanism, unifying data standards and platform standards, and fully applying legal norms to clarify the rights and responsibilities of all parties involved.[18]

5.2.1. Establishment of Interoperability Data Standards and Harmonized Platform Standards

Experience has shown that allowing data standards to be freely applied in the marketplace is not compatible with the trends of the digital economy. Article 20 of the General Data Protection Regulation (GDPR) requires data subjects to receive their data in a "structured, commonly used, and machine-readable format" when exercising their right to data portability, while Article 68 of the preamble to the GDPR advocates for data formats to be "interoperable". Given the diverse nature of personal data, the GDPR does not prescribe specific data formats but allows various industries to choose the most suitable formats. For the specific context of open banking, countries and regions recommend adopting unified parameter standards.[19] In 2020, the People's Bank of China issued the "Security Management Code for Application Program Interfaces of Commercial Banks", which provides technical specifications and security standards for open banking. To enhance the practical benefits of open banking, China needs to establish unified data formats and legally mandated data standards to minimize unnecessary format conversion during actual data sharing.[20]

Additionally, since China does not have a unified open banking platform, third-party financial institutions face the challenge of interfacing with different platforms. To address this, two strategies can be implemented: one is to standardize API interfaces through either mandatory national regulations or industry association guidelines;[21] the other is to establish a nationally unified open banking platform, requiring cooperation among all banks and financial institutions involved in open banking, guided by national policy.

5.2.2. Full Use of Legal Norms to Clarify the Rights and Responsibilities of All Parties

To regulate the right to data portability legally, China should further refine its data-related legislation, clearly defining the scope of the right to data portability and balancing the interests of individuals and data processors.[22] It's important to note that research on the legitimacy and protection of corporate data property rights is still in its early stages in China, as the position of personal information rights ownership remains unclear.[23] To this end, three steps should be taken: firstly, improve legislation on data

portability rights, excluding derivative data from personal data, and prohibiting data subjects from transferring derivative data or exercising corresponding data rights.[24] secondly, carefully classify data and allocate data rights according to each party's contribution in data processing and usage;[25] thirdly, establish a data property rights system for enterprises and define data ownership.[26]

Further, the obligations among the parties involved in personal financial data sharing within open banking need to be clarified. To genuinely remove cooperation barriers among data users, it is crucial to reasonably allocate the responsibilities and obligations of financial institutions and third parties. Specifically, the parties in each segment of open banking should undertake the following obligations. First, commercial banks and third-party organizations should establish a data security management system, create detailed security management procedures, and assign specific responsibilities to personnel. Second, they should control the risk of financial information leakage based on the level of information disclosure. Third, an effective data storage mechanism should be established to prevent malicious tampering. Fourth, the capability of commercial banks and third-party organizations to control data risks should be enhanced, with data being classified and encrypted to prevent network attacks and information loss. Fifth, commercial banks and third-party organizations should manage, process, and protect users' financial data. If personal data leakage occurs due to internal issues or technical defects, causing customer losses, they are liable for compensation to ensure the safety of customers' personal financial information.[27]

The information disclosure obligations of banks are primarily focused on the pre-authorization stage and should cover aspects such as the purpose of data sharing, recipient information, type of data shared, duration of sharing, and potential risks. Regarding third-party institutions, the obligations mainly concern post-sharing stages, where they should keep real-time records of the time of data acquisition, the purpose of data usage, and the security measures taken for data protection.[28] Additionally, banks and third-party financial institutions should disclose foreseeable risk information, and in the event of data breaches, they must notify the data owner and regulatory authorities promptly to assist in protecting the data owner's rights and clearly inform them of available remedies. Banks and third-party financial institutions should also ensure that their customer notification obligations are effectively fulfilled, prominently highlighting key terms and conditions to users.

To effectively implement the main responsibilities of all parties based on the type of dispute, it is important to differentiate and address the four common situations of data infringement arising from open banking financial data sharing (Figure 5). Civil liabilities should be recognized separately for each situation to ensure clear accountability and resolution.[29]

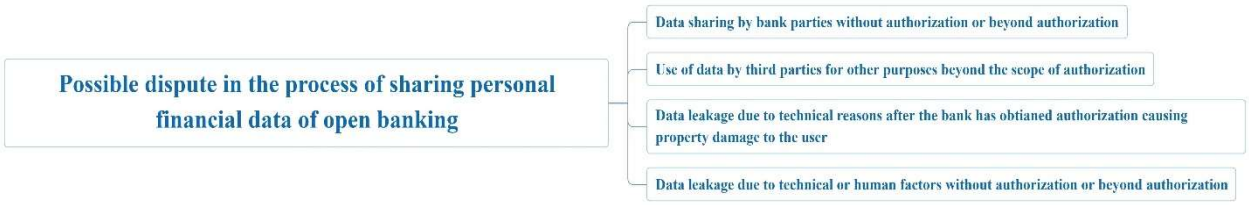

Fig.5 Types of Disputes in the Process of Sharing Personal Financial Data

In the first scenario, when a bank, acting as the data controller, shares data without authorization or exceeds its authority, it should be liable for breach of contract or tort based on the contractual agreement. The type of liability is chosen by the user and constitutes the primary liability. The third-party institution, which benefits from the data sharing process, should also bear liability to the customer for this benefit.

In the second scenario, since the primary fault lies with the third-party organization, in a triangular model relationship, a factual contract between the third-party organization and the financial consumer has been established. Consequently, the financial consumer can demand that the third-party organization be liable for breach of contract or tort. In a linear model, where there is no contractual relationship between the third-party organization and the individual user, the user can only claim that the third-party organization is liable for the return of unjust enrichment or for tort liability. In this situation, whether the bank is liable depends on whether it has fulfilled its duty of review according to the contract.

In the third scenario, if the technical problem is caused by the bank, the bank should be liable to the affected individual for breach of contract or copyright infringement. Conversely, if a third-party organization's access technology is faulty and leads to data leakage, the type of liability will depend on the existence of a factual contractual relationship between the third-party organization and the user. If such a relationship exists, the user should be responsible for breach of contract or copyright infringement. If no contractual relationship exists, the injured party can only request that the aggressor assume tort liability. Similarly, if the bank fails to fulfill its obligation to review whether the access technology is adequate, it should be liable for breach of contract to the extent of this failure.

In the fourth scenario, for data leakage due to technical problems, the assumption and distribution of responsibility apply as in the third scenario. However, in the absence of data misuse, if the leakage is caused by the actions of the bank's or third-party institution's staff, a distinction must be made between functional and non-functional behavior. If the leakage results from functional behavior, the bank or the third-party institution should assume liability for breach of contract or for infringement, and the organization can seek recourse from the at-fault staff member. If the leakage is due to non-functional acts, the staff member should be liable for the tort, and the organization they belong to should also be liable, unless it can prove it is not at fault. If the data leakage is caused by the actions of a natural or legal person other than the bank or the third-party institution, the responsible person should be held liable for the infringement, and the bank or third-party institution should bear supplementary liability if they cannot prove they are not at fault.

5.2.3. Multi-Channel Construction of a Cross-Border Regime for Data

China should initially sign data cross-border agreements with other countries to clarify the rights and obligations of each country involved in the cross-border data process. Secondly, it should establish correct data cross-border values at the national, social, and individual levels. Further, it should implement a security assessment mechanism to categorize and classify data for cross-border control and management. Finally, countries should strengthen domestic legislation and streamline the legal protection mechanism for data cross-border through contract law, tort law, competition law, and other relevant legislation.[30] In the process of open banking financial data sharing, China should pay considerable attention to the cross-border flow of data. Specifically:

China should actively advocate for the international cross-border circulation of data on the basis of data security. Based on the principle of reciprocity, it should promote the cross-border flow of information by signing bilateral or multilateral agreements with other countries. China can refer to the European Union's digital protection system and establish a "white list" to include eligible countries or companies, thereby providing more lenient export policies for data from these countries or companies.

A correct and dynamic value of financial data should be established at the national, social, and individual levels. It should not be assumed that the protection of data rights is always better than the functioning of data sharing. It should be examined through the dynamic system theory that when data rights are or will be under obvious threat or infringement, data rights should indeed be fully protected, and data sharing should be appropriately limited. However, when data rights are in a secure state, the data sharing function should be fully utilized, and data should be proactively shared across borders in compliance with the law.

The security assessment mechanism should be further implemented, and a sound and reasonable security assessment mechanism should be established to facilitate cross-border data flow. The establishment of a security assessment mechanism is urgent, but due to the different types of data, it is necessary to improve the assessment mechanism in the form of classification and grading.[31] Specifically, the National Technical Committee for Financial Standardization (NFSTC) issued the "Personal Financial Information Technology Protection Specification" (hereinafter referred to as the "Specification"). This specification clearly divides personal financial data into three levels (Figure 6).

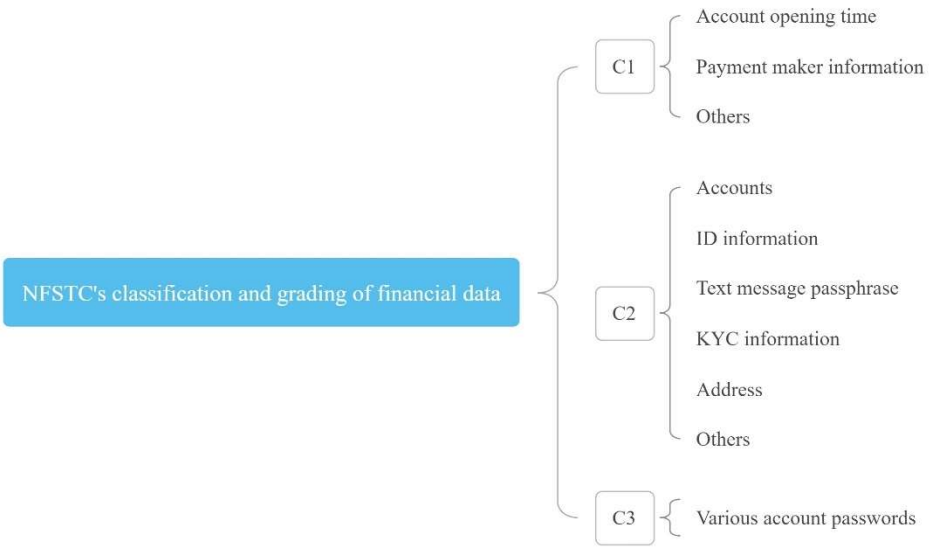

Fig.6 NFSTC's Classification and Grading of Financial Data

Due to its lower privacy level, the restrictive conditions for C1 category data should be appropriately relaxed. The cross-border transmission of such data can be achieved following the express consent of the data subject and an internal assessment by the data transmitting party. For C2 category data, which involves more sensitive information, data export can occur only after explicit consent has been obtained from the financial consumers, the existence of relevant contracts protecting personal financial data leaving the country, and validation of the security assessment mechanism through relevant departments. In the case of C3 category data, which is extremely closely related to personal privacy, it is not advisable to permit cross-border data transmission at this stage due to its high sensitivity.

The international regulatory cooperative development model must be constructed and regulated through international treaties. Countries should clearly agree on the scope and authority of regulation in such treaties to determine the effectiveness of national laws on data sharing both domestically and internationally. Additionally, it is imperative to address the inadequacies in regulating cross-border disputes over data and establish mechanisms for dispute resolution that clarify the rights and responsibilities of each country. This can be achieved through treaties and agreements, thereby incorporating the regulatory system of open banking into the framework of international law.

Protective Regulation Through Contract Law, Tort Liability Law, and Competition Law. In terms of contract law, during the cross-border transmission of data, states can provide a corresponding data cross-border contract blueprint, clearly specifying whether terms can be modified and the scope of such modifications. Parties to the contract can then adjust the terms according to their interests. Regarding tort liability law, it can be aligned with private international law

to address network infringement behavior from an international private law perspective, thus providing remedies for data sharing activities. For competition law, both the Antimonopoly Law and the Anti-Unfair Competition Law can be fully utilized to legally regulate and address issues of competition exclusion or restriction and data monopoly behaviors that may arise in the process of cross-border data sharing.

5.2.4. Breaking the Data Monopoly with Two-Way Sharing and Appropriate Mandatory Standards

Data sharing in open banking is a prerequisite for their openness. Therefore, open banks must adhere to the principle of two-way sharing to fully, effectively, and optimally leverage the benefits of data governance. Within the financial sector, data holders and providers face issues such as “data fragmentation” and “information silos”. Traditional financial institutions, including banks and securities companies, as well as traditional financial payment institutions like third-party payment platforms and e-commerce platforms, along with government departments related to finance and taxation, often exhibit imperfect data and information integration, openness, and usability. This inadequacy hampers the efficient, convenient, and comprehensive realization of the open bank’s data openness strategy. Consequently, it is not advisable to blindly emulate the “fetishism” of the foreign banking sector's “one-way sharing” model without considering domestic practices, which only addresses the data openness of financial institutions in a limited manner. Instead, from the perspective of maximizing data empowerment, we should advocate for two-way sharing across the entire value chain to achieve optimal governance effects and capabilities.

Regarding the application of mandatory standards, a certain threshold could be established. When a bank reaches this pre-set threshold, it must undertake mandatory data openness to facilitate the natural sharing and circulation of data. This approach aligns with the legislative intent of competition law, as it helps break data monopolies and prevents the formation of new financial trusts.

5.2.5. Modern Technology Enables Financial Data Risk Visualization

Emerging technologies such as artificial intelligence, big data analysis, blockchain, and smart contracts not only offer opportunities for the transformation of financial businesses but also infuse new vitality into financial risk management and supervision. Firstly, with the aid of advanced technology platforms, it is possible to establish information transmission channels from local to central levels and from open banks to regulators, thereby automating the supervisory information flow. This automation can help reduce supervisory costs and minimize the risks of underreporting, omissions, and misreporting. Secondly, big data algorithms can analyze the data standards and platform standards for open bank data sharing. The current lack of unification in data format standards and intermediary platform standards results in inefficient data transmission, severely impacting data quality and the security of the data ecosystem. The high-risk nature of financial data necessitates worldwide unification of data standards to protect national data sovereignty. Big data algorithms can propose the most suitable standards for international application, enhancing data flow efficiency and quality, ensuring the safe and reasonable sharing and circulation of data domestically and internationally, reducing the likelihood of risk occurrence. Blockchain technology can enhance the governance mechanism of common voting, optimize data authentication, prevent and resolve significant financial risks, and address financial risks at their source. Additionally, big data analysis and machine learning methods can be used to model risks associated with open banks and related financial institutions, predicting the likelihood of risks and their transmission pathways. This shift enables proactive monitoring and early warning, moving from mid-process and post-event monitoring to pre-event monitoring, achieving true “penetrative” supervision.

5.2.6. Privacy Computing Technology Fuels Data Privacy Protection

Privacy computing techniques can be employed to protect data privacy during the data-sharing process, preventing hacking and data privacy leaks. Specifically, personal data can be further encrypted using privacy computing methods such as inadvertent transmission and secret sharing. Inadvertent transmission involves both parties using obfuscation methods to transmit data, where the sender does not know the exact data being sent, and the receiver does not know the data other than what is received. Secret sharing involves splitting the original data into parts, with each participant in the open bank managing only a portion of the data. No single subject can independently recover all the data, and during data sharing, each participant exchanges only the data they possess. This privacy computing technique prevents misuse of data by both the sender and receiver, thereby avoiding privacy leakage.

5.2.7. Differential Privacy Techniques to Advance Data Quality

Article 8 of the Chinese Personal Information Protection Law stipulates that the processing of personal information must ensure the quality of the information and, as much as possible, avoid infringing on individuals' rights and interests due to inaccuracies. Data subjects have the right to request that data processors correct, delete, or supplement inaccurate information. Given the generality of these legal provisions and the practical considerations of data privacy and security, the quality of data may inevitably be compromised to some extent. Therefore, modern technological means, particularly differential privacy technology, can ensure data integrity and consistency. Differential privacy involves adding random noise to statistical data queries to maximize the accuracy and completeness of the statistical outputs while minimizing the risk of identifying individuals. By employing differential privacy techniques, data integrity and consistency can be maintained, and data privacy can be maximized while preventing data loss or distortion during transmission.

5.3. Suggestions for China's Open Banking Personal Financial Data Sharing Mechanisms

Data privacy protection is a central issue in open banking financial data sharing. Robust financial data sharing mechanisms can enable data privacy to be safeguarded more comprehensively throughout the entire lifecycle. China’s open banking financial data sharing mechanism primarily includes data sharing driving mechanisms, sharing authorization mechanisms, sharing object selection mechanisms, and data sharing supervision and management mechanisms. Through the integrated construction and enhancement of these mechanisms, the information security and data privacy protection in the process of financial data sharing of open banks can be further strengthened, aiming to

achieve a balance between individual autonomy and state coercion in the process of financial technology innovation.

Firstly, a sound mechanism for classification and authorization should be established. The improvement of the "informed consent" mechanism should make sharing transactions as convenient as possible while protecting the security of personal information. It involves the following levels. First, different authorization standards should be defined according to different data types. For personal identity data, when banks share this type of data, they should not only disclose the purpose of sharing and the type of data recipients, but also inform financial consumers of the type of sensitive data shared, the identity of the data recipients, and their ability to ensure security in a timely manner; for personal financial data, because it still belongs to the individual user, this type of data can only be shared under the explicit authorization of the individual user. If the bank has desensitized the personal financial data, the information disclosure requirements for the bank can be appropriately reduced; for value-added data, since the bank has made efforts to combine the financial users with the data, the bank can share this type of information without the user's authorization and consent, provided it is desensitized before sharing. Secondly, the prior authorization clause, which is part of the privacy protection policy, should be independent of the form contract provided by the bank when signing a written agreement with the user, and data sharing can only occur after obtaining the user's individual consent and authorization. In addition, the terms of the bank's privacy policy should also be adjusted accordingly, transitioning from traditional text to functional text, and utilizing multiple choice to allow users to select the data they want to share and exclude the data they do not want to share, thus making financial services more personalized and diverse. Considering the fragmented and scattered reading habits of today's society, the bank can provide both summary and full versions of the privacy protection clause for users to choose from. Finally, the bank can establish a "personal customer management center" within the existing platform. In this management center, the "white list" of financial institutions is presented as a check box, enabling users to authorize all at once within this center. This approach can eliminate the redundancy of single-transaction authorization and unnecessary repeated authorization.

Secondly, the rigidity of the selection mechanism should be addressed through a "black and white" two-way model and form contracts. In terms of the shared object selection mechanism, the traditional licensed model should be eliminated. By leveraging blockchain, big data, and other emerging technologies, the construction of "white lists" and "black lists" of financial institutions should be accelerated, allowing for the quick identification of trustworthy financial institutions to participate in data sharing more efficiently. This helps prevent data privacy leaks by carefully selecting target audiences. Specifically, the characteristics of form contracts, i.e., "pre-drafted for reuse," can be fully utilized. The bank can pre-draft the requirements and conditions for the selection of shared objects and fully configure the rights and obligations of the third-party financial institutions and commercial banks. Such form contracts must be filed with the relevant financial regulator, such as the CBRC, before they can produce corresponding legal effects. This approach decentralizes the specific practice standards of open banking to market players, aligning with market-driven mechanisms while fully utilizing state coercive power to prevent horizontal monopoly agreements that could damage a competitive market environment. Additionally, the "blockchain blacklist" system can be used to efficiently eliminate financial institutions with poor credit or high risk. Combined with the "white list" mechanism, the efficiency of access to financial institutions can be further improved, achieving a balance between decentralization and autonomy at the level of selection mechanisms and state coercion.

Thirdly, it is necessary to improve the regulatory mechanism: transitioning from a “regulatory sandbox mechanism” to a "common vote mechanism." In regulation, the "regulatory sandbox mechanism" can be introduced to allow regulatory agencies and open banks to innovate within the same sandbox, achieving true regulatory resonance. On this basis, regulatory agencies can integrate with the innovation chain in the sandbox, using cloud computing, big data, artificial intelligence, blockchain, and other technologies to create a dynamic system for open banking regulatory guidance, and conduct real-time risk assessments of open banking operations. In today's data-centric environment, data centralization and integration require a "regulatory" approach to data to fully utilize its potential. Therefore, introducing a "common vote mechanism" is necessary to achieve comprehensive regulation. The common vote mechanism leverages social supervision to facilitate data flow. The "common vote" mechanism can return the benefits of data sharing to users and other interested parties. As an efficient mechanism for discovering, collecting, and tracking data in real time, the "common vote," combined with features like smart contracts and blockchain’s immutable records, enables one-to-one intelligent matching of data.[32]This approach facilitates a smooth transition from "technical regulation" to "technical governance."

Finally, the market-driven mechanism can be optimized through macro-regulation. Regarding the driving mechanism of open banking financial data sharing, China has long followed a market-driven mechanism, which has significant advantages in delegating the specific application and practice of open banking to the market for self-governance, thus reducing the need for state intervention. Introducing market competition mechanisms can create a financial data sharing system and rules that adapt to the market's development. The driving mechanism must align with the characteristics of open banking practices, which are inherently autonomous and market-oriented, aligning with China's use of market-driven mechanisms. However, the market-driven mechanism has its limitations, such as market spontaneity and volatility. Excessive decentralization to the market can lead to a lack of unified standards for open banking financial data sharing, increasing the risk of disorderly competition in the open banking financial market. Ensuring the continued effectiveness of the market-driven mechanism while minimizing the risks associated with its weaknesses is crucial in reforming the mechanism. Specifically, I believe that the mechanism can be optimized without changing the market-driven approach. Macro-regulation can be used to establish general norms and guidelines, while the specific practical application of these norms and standards can be delegated to the entities involved in open banking financial data sharing for consultation and formulation. This approach allows open banking financial data sharing to operate and compete healthily within a standardized system.

6. Conclusion

The nascent model of open banking development has firmly established its presence in China. To ensure its sustainable progression, it is critical to institute robust legal frameworks that govern the data sharing practices within open banking and to augment regulatory oversight across the banking sector. The creation of a dedicated regulatory agency, tasked with the exclusive supervision of open banking operations, is essential to delineate rights and responsibilities clearly. Furthermore, there is a pressing need to facilitate cross-border data exchanges, surmount technical barriers and standardize technical specifications. These initiatives are pivotal for propelling open banking towards an advanced stage of financial ecosystem enhancement.

6.1. Conclusions of the Study

The necessity of financial data sharing in the digital economy, as both a driver of innovation and development, underscores the need for robust legal frameworks. These frameworks should support the continuous advancement and improvement of financial data sharing practices, aligning them with the principles of the rule of law while invigorating market dynamics. Specifically, the issue of the blanket application of the "informed consent" rule can be addressed by developing a classification-based and tiered authorization mechanism. Furthermore, inconsistencies in data sharing standards and platform integration can be mitigated by establishing interoperable data sharing standards and unified platformization norms. The ambiguity surrounding the rights and responsibilities of the involved parties can be resolved through overarching mandatory legal guidelines, supplemented by industry-specific norms to clarify these roles. Moreover, the rigid selection mechanisms for shared entities can be addressed through a black-and-white bidirectional model and standardized contracts.

To support the trend towards data globalization, a cross-border data framework should be constructed through multiple channels. This would necessitate the gradual transformation of the traditional regulatory model into a phased "regulatory sandbox" approach, enabling regulatory alignment and, when appropriate, advancing towards a "common vote" mechanism to achieve comprehensive regulation centered on the rights of the data subjects. Additionally, the integration of modern technologies is essential to ensure data quality and optimize the circulation and practical application of data, all while upholding data privacy rights. When necessary, these practices should be explicitly mandated through national regulations. By respecting the autonomy of individuals and clearly distinguishing between individual autonomy and state intervention, a stable framework for personal financial data sharing within the context of open banking can be established for the new era.

6.2. Practical Implications

Open banking represents the pathway to development in the digital age. Within the framework of the sharing economy, the sharing of personal financial data is particularly critical, serving as the financial industry's lifeblood for tracking market trends and as a crucial link for achieving high-quality transformation and upgrades in the banking sector. Creating an open banking platform presents both opportunities and challenges for mitigating significant financial risks. Since 2018, leading banks such as the Pudong Development Bank, Industrial and Commercial Bank of China, China Merchants Bank, and the Construction Bank have signaled their intent to establish "de-physicalized" banks—open banks. Most banks in China have already commenced open banking operations. This operational model facilitates the more efficient and convenient flow of financial data, enabling the public to access a wider array of new financial services more inclusively. However, the lack of mandatory measures supporting personal financial data sharing under the open banking system has led to vague and broad data rights provisions and unclear ownership of specific data types. This ambiguity has resulted in novel data-related unfair competition disputes, as evidenced by cases such as Sina v. Momo and Taobao v. Meijing, where improper acquisition of user data was a central issue. It is essential to address these practical problems by analyzing China's specific circumstances and proposing targeted recommendations for system development.

6.3. Future Prospects

The development of a personal financial data sharing system for open banks must be grounded in the practical realities of data sharing and the specific operational context of open banks. The system's evolution should reflect a focus on different issues as they arise over time. In the next phase of personal financial data sharing for open banks—focused on improving the financial ecosystem—the system should not undergo significant revisions but should instead be adjusted and expanded to address practical issues while maintaining legal stability. The aim is to ensure that the personal financial data sharing framework can effectively function within the open banking context, meet public expectations and fully maximize the utilization of data.

Acknowledgments

This study is a result of the General Program of the National Social Science Foundation of China, Research on the Legal System of Financial Supervision Based on Big Data (Project No. 18BFX137).

References

[1] Miao Qianye: Unified Big Data Market and Open Banking Development, China Finance, Vol.No.983(2022), No.17, p.95.

[2] Xuan Di, Fang Yan: Risk Challenges and Legal Regulation of Open Banking Data Sharing in China, Credit Reference, Vol.40(2022) No.7, p.42.

[3] Wei Boyan, Qiang Feng, An Wensen: Application and Challenges of Privacy Computing Technology in Open Banking Data Compliance, Modern Finance Guide, Vol.No.25 (2021) No.12, p.16.

[4] Chai Ruijuan, Tian Aoni: Risk Mitigation and Institutional Construction for Introducing Data Portability in the Open banking Scenario, Credit Reference, Vol.40(2022) No.3, p.20.

[5] Yang Xueke, An Xuemei: Open Banking Practice: Data Portability and its Regulatory Logic, Financial Economics Research, Vol.36(2021) No.2, p.141.

[6] Zhou Xueting: Study on the Legal Prevention Mechanism of Open Banking Data Risks (MS., Southwest University of Finance and Economics, China 2021), p.43.

[7] Yuan Jinming: Research on Open Banking Data Sharing Model and Supervision from the Perspective of Big Data, Hainan Finance, Vol.No.390(2021) No.5, p.50.

[8] Zhao Yin: On Information Disclosure Obligations in Open Banking Data Sharing, Political Science and Law, Vol.No.309 (2021) No.2, p.96.

[9] Li Qingyue: A First Look at the Personal Data Protection Experience of Overseas Open Banking, China Banking, Vol.No.79(2020) No.7, p.91.

[10] Hao Wang, Shenglan Ma, Hong-Ning Dai, Muhammad Imran, Tongsen Wang: Blockchain-based data privacy management with Nudge theory in open banking, Future Generation Computer Systems, Vol.110(2020), p.822.

[11] Menuet M, Minea A, Villieu P, Xepapadeas A: Growth, Endogenous Environmental Cycles, And Indeterminacy, Orleans Economics Laboratory,2021(10).

[12] Suri T, Bharadwaj P, Jack W: Fintech and Household Resilience To Shocks: Evidence From Digital Loans In Kenya, Journal of Development Economics,2021(01).

[13] Somaini, L: Regulating the Dynamic Concept of Non-Personal Data in the EU: From Ownership to Portability. European Data Protection Law Review (EDPL), Vol.6(2020) No.1, p.85.

[14] Krämer J: Personal Data Portability in The Platform Economy: Economic Implications and Policy Recommendations Journal of Competition, Law &Economics, Vol.6(2020) No.17, p.308.

[15] Lauren Davis: The Impact of the California Consumer Privacy Act on financial institutions across the nation, North Carolina Banking Institute, Vol.24(2020) No.5.

[16] Janneke Gerards, Frederik Zuiderveen Borgesius, Protected grounds and the system of non-discrimination law in the context of algorithmic decision-making and artificial intelligence, Colorado Technology Law Journal Vol.20(2022) No.1.

[17] Zhao Yin: Legal Regulation of Personal Data Sharing under the Open Banking Model, Modern Law Science, Vol.42(2020) No.3, p.148.

[18] Chen Meng: Open Banking Innovation from the Perspective of Data Sharing Mechanism, New Finance, Vol.No.376(2020) No.5, p.35.

[19] Xing Huiqiang: On the Introduction of Data Portability in China - An Open Banking Perspective, Journal of Political Science and Law, Vol.No.195(2020) No.2, p.18.

[20] Luo Hang, Yang Zhuoyi: Research on the Construction of Open Banking Ecosystem from the Perspective of Data Sharing, Journal of Xihua University (Philosophy & Social Sciences), Vol.39(2020) No.1, p.76.

[21] Yang Dong, Cai Renjie: Open Banking: From Data Silos to a Data Sharing Society, Financial View, (2019) No.11, p.55.

[22] Yang Dong, Cheng Xiangwen: Research on Consumer-Centric Data Sharing Mechanism of Open Banking, Financial Regulation Research, Vol.No.94(2019) No.10, p.113.

[23] Li Yan, Cai Kailong: A First Look at Data Sharing Issues in Open Banking, China Banking, Vol.No.67(2019) No.7, p.31.

[24] Liu Youhua, Ren Zuliang: Research on the Regulation of Financial APP Data Processing in the Perspective of Consumer Rights Protection, Consumer Economics, Vol.38(2022) No.1, p.27.

[25] Lin Jie, Tian Chen: Regulation of Cross-Border Flow of Personal Financial Data, Journal of Shanghai University (Social Science Edition), Vol.38(2021) No.6, p.102.

[26] Sun Yueyuan: Study on the Objects of the Right to Data Portability: Structure, Effects and Sinicize, Journal of Henan University of Finance and Economics and Law, Vol.37(2022) No3, p.81.

[27] Xie Wei, Li Wenjing: The Path of Data Portability from the Perspective of Proportionality, Journal of Hunan University (Social Sciences), Vol.36(2022) No.1, p.143.

[28] Shang Bowen: From "Open Banking" to "Open Finance": Governance Responses to the Flow of Financial Data Elements, Research on Financial Regulation, (2023) No.11, p.61.

[29] Chen Tianhao, Xu Wei: Regulating Agile Regulation: Regulatory Challenges and Improvement Paths for Financial Data Openness, Governance Studies, Vol.39(2023) No.6, p.145.

[30] Tang Jinghai: Study on the Development of Open Banking, Modernization of Shopping Malls, (2023) No.21, p.96.

[31] OuYang Fenqiang, Zhou Yunxin, Fu Seng, etc.: Exploring the Current Status and Risks of Open Banking Applications, FinTech Era, Vol.31(2023) No.10, p.94.

[32] Yan Xiaqiu, Guo Linlin: Legal Governance of Personal Financial Data and the Way Forward - An Analysis Based on the Perspective of Dual Attributes of Personal Financial Data, Price Theory and Practice, (2023) No.5, p.32.