Open Banking Personal Financial Data Governance: Framework, Dilemmas and Strategies

Zhongqi Jiang
Xi'an Jiaotong University School of Law, Xi'an, Shaanxi, China

Abstract: The essence of "Open Banking", as a representative of digital transformation in the financial industry, is data sharing. At present, with the continuous development of Open Banking practice, there are many challenges in Open Banking personal financial data governance, such as the risk of data authorization, data leakage, the lack of industry norms, and the lack of industry supervision. In this regard, on the basis of sorting out China's Open Banking personal financial data governance framework, a scientific data governance mechanism should be constructed, a strict supervisory and regulatory system should be established, and the dual objectives of data sharing and risk prevention should be taken into account.

Keywords: Open Banking; Personal Financial Data; Data Sharing; Legal Regulation

1. Introduction

The concept of "Open Banking" can be traced back to Brett King, known as the "future expert of the global banking industry", in his book "Bank 4.0" published in 2018[1]. Essentially, Open Banking is a "banking platform development model", where banks utilize technologies such as API, SDK, etc., based on data sharing, to share data resources with third-party institutions, enabling banks to deeply integrate into various user scenarios, and jointly build a digitalized, comprehensive banking financial ecosystem. PayPal's introduction of the "PayPal API" to developers in 2004 is regarded as the beginning of global Open Banking. The China Bank's Open Platform launched in 2013 can be seen as the embryonic form of Open Banking development in China. Under the premise of ensuring data security, Open Banking, through data sharing, helps to enhance user service experience, reduce operating costs for both financial and non-financial institutions, break the data monopoly of traditional financial institutions, and promote innovation and development in the banking industry. However, it is necessary to be vigilant about various risks arising from data sharing, such as unauthorized data collection, data leakage, denial-of-service attacks, and man-in-the-middle attacks[2]. Due to the involvement of multiple stakeholders, if Open Banking is disrupted or flawed, it will affect the overall stability of banks and may even lead to paralysis, posing a threat to financial stability and economic security, resulting in significant losses to the public interest.

2. Open Banking Personal Financial Data Governance Framework

Since the launch of China's first API Bank by Shanghai Pudong Development Bank in 2018, China has entered the preliminary development stage of Open Banking. Subsequently, dozens of large and medium-sized commercial banks such as ICBC and CCB have successively launched API open platforms. In 2015, "Guiding Opinions on Strengthening the Protection of Financial Consumer Rights and Interests" established for the first time the "right to information security" for financial consumers. In 2019, "Financial Technology Development Plan (2019-2021)" proposed to utilize means such as API and SDK for cross-border cooperation, aiming to build an open, cooperative, and win-win financial services ecosystem. In 2020, "Security Management Specification for API of Commercial Banks" detailed the security technology and security protection requirements for the types, security levels, security design, and deployment of API for commercial banks. In 2020, "Technical Specifications for Personal Financial Information Protection" clarified the security protection requirements for the collection, transmission, storage, and use of personal financial information from the perspectives of security technology and security management. In 2021, "Regulations on the Scope of Necessary Personal Information for

Common Types of Mobile Internet Applications" explicitly stated that applications may not forcibly collect unnecessary personal information. In 2022, "Financial Technology Development Plan (2022-2025)" proposed to use financial technology reasonably to enrich the hierarchy of financial markets, optimize the supply of financial products, and bridge the digital divide between regions, groups, and institutions. In 2022, "Guiding Opinions on the Digital Transformation of the Banking and Insurance Industries" emphasized the active development of industrial digital finance, the establishment of digital financial service platforms, the promotion of open banking construction, and the strengthening of scenario aggregation and ecological integration.

In addition, laws such as Cybersecurity Law, Data Security Law, Personal Information Protection Law, and Measures for the Implementation of the Protection of Financial Consumer Rights and Interests all involve the sharing of personal financial data. The current situation of development where "practice precedes regulation" in development banks has provided a relaxed practical environment for various commercial banks in China to build Open Banking. However, it has also led to the absence of relevant standards for Open Banking in China, further hindering the deep development of Open Banking in China[3].

3. Open Banking Personal Financial Data Governance Dilemma

3.1 Risk of Authorisation of Personal Financial Data

In the data acquisition stage of Open Banking, large commercial banks may refuse reasonable sharing requests either due to considerations of possessing massive data, or due to an inherent mindset of "owner's data", or based on market competition needs. Meanwhile, small and medium-sized commercial banks, due to their small data holdings and weak competitive abilities, typically, for certain profit considerations, excessively collect personal financial data without proper authorization from the data subjects or beyond what is authorized, in order to seek partial economic benefits. Large financial technology companies have rapidly accumulated a large amount of data in a short period by leveraging their platform traffic advantages and network effects. Their influence in markets such as mobile payments, money market funds, and small loans continues to grow. They also face the issue of collecting and abusing user data without authorization or beyond authorization, which must be taken seriously. Additionally, due to the lack of precise rights over data, the absence of clear authorization mechanisms, effective tracking mechanisms, and access mechanisms for data recipients, coupled with potential design flaws in Open Banking technical systems and business processes, as well as the lack of security protection capabilities and willingness of third-party institutions, malicious attackers can illegally obtain personal financial data, exacerbating the risks in the process of personal financial data authorization in Open Banking.

3.2 Risk of Personal Financial Data Leakage

Open Banking relies on a data sharing mechanism established with third-party institutions based on data interfaces. API or SDK, as crucial channels connecting data, become key targets for malicious attackers to steal data. Data openness in Open Banking not only elongates the chain of data storage, transmission, and usage but also extends the chain of risks. Personal financial data originally stored only in banks is handed over to third-party institutions during the process of sharing data interfaces. Especially, considering the limited operational and data protection capabilities of certain third-party institutions, along with the continuous increase in data volume, lacking corresponding technical coping abilities and management mechanisms, coupled with potential defects in interface design and permission settings, will significantly increase the risk of personal financial data leakage, thereby triggering more significant data security issues. Currently, in the construction process of Open Banking, commercial banks in China are limited to providing basic information and services at a preliminary level. There has not been a broad consensus reached between them and large financial technology companies regarding data sharing. Small and medium-sized commercial banks generally find themselves in a disadvantaged position during cooperation with large financial technology companies. They are unable to effectively address data leakage issues under the guise of financial service innovation claimed by large financial technology companies[4].

3.3 Risk of Lack of Industry Regulation

China's Open Banking is still in its early stages of development, differing from both the mandatory regulatory model in the UK and the laissez-faire development model in the US. The legal system in China still relies on relevant laws and regulations regarding the protection of personal financial data, such as the Personal Information Protection Law, the Data Security Law, and the Consumer Rights Protection Law. However, these laws mostly consist of principled provisions, lacking operability. Additionally, administrative regulations and departmental rules with practical guidance are relatively scattered. Moreover, regarding the collection, processing, and handling of personal financial data, the content of the traditional legal system significantly lags behind the development of Open Banking. Take the "informed - consent" clause as an example. Open Banking cannot inform users of the entire scope of data collection at the initial collection of personal financial data, and Chinese law does not allow for "generalized notification", so Open Banking cannot achieve "complete notification" fundamentally. In Open Banking, due to the existence of third-party institutions, the "informed - consent" clause may not effectively constrain these institutions. Furthermore, most data collectors integrate the "informed - consent" clause with the entire user agreement. Users often find themselves confined by the lengthy and complex terms and tend to simply skim through them or even consent without reading. Therefore, the "informed - consent" clause not only fails to fully protect the legitimate rights and interests of data subjects but also provides a pathway for banks and third-party institutions to evade their responsibilities[5].

3.4 Risk of Lack of Industry Regulation

Open Banking, as a platform development model involving multiple entities and the integration of "technology + finance", spans various domains such as finance, technology, and commerce. Consequently, it will be subject to multiple regulations, including oversight from market regulatory authorities, financial regulatory authorities, national internet security authorities, consumer rights protection organizations, and others. With regulatory entities being so fragmented, each entity possesses incomplete regulatory authority. The ambiguity of regulatory agencies and functions may lead to regulatory overlaps or gaps. Moreover, a single regulatory framework may face the dilemma of which type of regulatory agency should take precedence and which regulatory measures to adopt. This situation is highly disadvantageous for the protection of personal financial data[6]. Additionally, data sharing in Open Banking fundamentally pertains to technical issues and may give rise to the problem of "algorithmic black boxes". This can leave users unaware of the purpose and intent of Open Banking algorithms, leading to information asymmetry between regulators and the regulated, thereby creating significant regulatory loopholes. Therefore, the existing regulatory framework is still unable to effectively regulate the risks associated with personal financial data sharing in Open Banking. Furthermore, as data volume and the extent of data sharing deepen, it may lead to systemic risks in the banking industry.

4. Open Banking Personal Financial Data Governance Strategy

4.1 Building Scientific Data Governance Mechanisms

Establish a comprehensive data risk prevention and control system. Data sharing has extended the data transmission chain of Open Banking, increasing the systemic risks of bank data protection. To address potential issues such as data leakage, misuse of data, and data rights during the open data process, it is necessary for banks to actively explore the application of technologies such as big data and blockchain in risk prevention and control. Additionally, third-party institutions need to conscientiously fulfill their risk prevention and control obligations, constructing a comprehensive data risk prevention and control system that aligns with platform operations, thereby providing a secure and reliable operating environment for Open Banking[7].

Establish unified Open Banking API technical standards. Regulations such as "Commercial Bank Application Programming Interface Security Management Specification" and "Mobile Financial Client Application Software Security Management Specification" require accelerating the establishment of a standardized data system for Open Banking, clarifying the scope and mode of openness, application

interface standards, and cooperation access standards. Regulatory authorities should promote the establishment of a sound and unified Open Banking API technical standard, enhancing the operability and convenience of data transmission between banks and third-party institutions. This will reduce the redundancy of personal financial data collection, lower the construction and transaction costs of Open Banking, enhance its risk prevention and control capabilities, and fully unleash the value of data.

Establish a data classification management mechanism. China can draw lessons from the UK's OBIE in classifying data based on different levels of confidentiality. Building upon existing data inventory catalogs, factors such as national security, social security, and individual privacy should be considered to develop data classification standards that meet the needs of Open Banking development. Differential regulatory measures should be adopted for data at different security levels. Additionally, technical means should be employed for continuous monitoring of sensitive data in API data transmission, providing basic standards for the flow of data in Open Banking. Although the "Technical Specification for Personal Financial Information Protection" serves as a recommended industry standard and lacks enforceability, its graded classification management of data based on sensitivity can guide future relevant legislation in China[8].

4.2 Establishment of a Tight Data Regulatory Regime

Enhance relevant legislation. On the one hand, it is necessary to ensure the practical implementation of the "data portability right", which serves as the foundation of Open Banking. Article 45 of the "Personal Information Protection Law" concerning the data portability right only has declarative significance in principle, lacking practical operability. Therefore, regulatory authorities need to promptly introduce detailed implementation guidelines, including methods, types, and conditions for data portability. On the other hand, further refinement of the "informed - consent" clauses in the sharing of personal financial data is needed. Banks and third-party institutions must obtain explicit consent from users when collecting, storing, transmitting, and processing personal financial data. If during this period, banks share data with another third-party institution, users must grant authorization again, and clauses stating "refusal to provide services if the user does not consent to authorization" are prohibited. Furthermore, it is essential to implement the strict adherence to the "informed - consent" rule for sharing personal identity information as outlined in the "Notice on Banking and Financial Institutions' Protection of Personal Financial Information". This includes anonymizing property, account, credit, and transaction information, and exempting the sharing of derivative information from notification obligations.

Utilize the self-disciplinary supervision role of banks and third-party institutions. On one hand, establish an internal third-party institution audit mechanism within banks. Although the "Commercial Bank Application Programming Interface Security Management Specification" delegates the power of third-party institution audits to banks, there are no restrictive regulations in Chinese law regarding the scope and conditions of third-party institutions. China can emulate a "whitelist" system, where banks establish whitelists for third-party institutions holding financial licenses, passing security tests, or endorsed by national credit, thereby reducing the audit process. Conversely, strict admission criteria should be set for third-party institutions engaged in activities such as data abuse or leakage, potentially even placing them on a blacklist. On the other hand, optimize the operational mechanism for data sharing between banks and third-party institutions. Both banks and third-party institutions need to develop sound data security management systems and specific processes, clarify responsibilities, define clear data openness scopes, establish data sharing logs to prevent malicious data tampering, provide traceability for data breaches, enhance data anonymization and encryption efforts, and prevent data loss due to technical deficiencies or internal reasons, safeguarding the legitimate rights and interests of users[9].

Strengthen government regulatory functions. On one hand, establish a diversified regulatory model with a single leading agency, multi-agency cooperation, and encouragement of private sector participation. Currently, in China, the People's Bank of China takes the lead, with cooperation from national financial regulatory authorities, the national cyberspace administration, market supervision departments, and encouragement for participation from

industry associations, enterprises, universities, and other entities. However, it's essential to strengthen regulatory coordination to prevent overlap or gaps in supervision. Additionally, establish a comprehensive regulatory mechanism. In the pre-stage, it is necessary to improve the data sharing authorization mechanism and establish risk warning and disaster recovery mechanisms suitable for Open Banking construction. In the mid-stage, establish risk monitoring and emergency mechanisms, conduct regular security monitoring of banks and third-party institutions, and enhance the analysis and response capabilities for risk events. In the post-stage, establish crisis public relations and relief mechanisms, promptly report risk events to higher authorities, implement a "burden of proof reversal", and tendentially increase the burden of proof for banks and third-party institutions to fulfill data protection obligations. Finally, pilot the "regulatory sandbox" mechanism. The "regulatory sandbox" places open banking products in a real but restricted environment for testing, providing an environment for open banking to develop freely under controlled risks. Additionally, the "regulatory sandbox" allows regulatory authorities to monitor the entire process, prompting them to continuously develop and improve regulatory rules in line with the development trends of Open Banking[10].

5. Conclusion

The emergence of Open Banking provides opportunities for the transformation and upgrading of the banking industry, and is closely related to the process of financial openness and innovation in China[11]. The development of Open Banking in China is still in its early stages. By analyzing the governance challenges of personal financial data in Open Banking, summarizing the current situation of personal financial data governance related to Open Banking in China, and based on this, proposing two aspects of recommendations: constructing a scientific data governance mechanism and establishing a rigorous data regulatory mechanism. The aim is to establish the correct development direction for the development of Open Banking in China, while fully unlocking the economic value of personal financial data, promoting the digital transformation of the banking industry, advancing the development of inclusive finance, and comprehensively enhancing the overall strength and core competitiveness of China's financial industry[12].

References

[1] Brett King, Bank 4.0 ,Marshall Cavendish International (Asia) Pte Ltd ,2018.

[2] Omarini A E. Banks and FinTechs: How to develop a digital open banking approach for the bank's future[J]. International Business Research, 2018, 11(9): 23-36.

[3] Boot A W A, Thakor A V. Can relationship banking survive competition?[J]. The journal of Finance, 2000, 55(2): 679-713.

[4] Ding Xiaoqiang, The "Yang" and "Yin" of Consent Rules in Personal Data Protection - A Study of Rule Configurations in the Perspective of the Kame Framework,Law Review , 2020,4 (130):130-143.

[5] Xuan Di, Fang Yan, Risk Challenges and Legal Regulation of Open Banking Data Sharing in China,Credit Collection, 2022,7(39):39-44.

[6] Zhu Wenhui, Practical Dilemmas and Improvement Paths of Personal Financial Data Protection under Open Banking,Heilongjiang Finance,2023,6(61):61-65.

[7] Zhou Yourong, The Role and Countermeasures of Digital Inclusive Finance in Assisting the Development of Small and Micro Enterprises, Finance Zonghengheng 2021.1(24):24-31.

[8] Gu Shenjun, Research on Open Bank Construction Mode and Its Regulatory Path - Taking Jiangsu Province as an Example, Fintech Times,2022,7(87): 87-90.

[9] Wen Shuying, The British Experience and Implications of Open Banking Regulation, Journal of Shanxi University, 2023,2(152):152-160.

[10] Chris Naskin, Internet Banking: The Digital New Financial Era ,CITIC Press ,2015.

[11] Xu Ke, Yin Zhentao, Financial Data Open Circulation and Sharing, China Finance,2019,4(90).

[12] Zhao Yin, Legal Regulation of Personal Data Sharing under the Open Banking Model,Modern Law, 2020, 3(138):138-150.

