Economics, Law and Policy
ISSN 2576-2060 (Print) ISSN 2576-2052 (Online)
Vol. 9, No. 1, 2026
www.scholink.org/ojs/index.php/elp

Original Paper

Research on Legal Regulation of Data Security in the Context of Financial Data Sharing

Rui Zhu[1]

[1] Grandway Law Shanghai Offices, Shanghai 200010, China

Received: May 20, 2026 Accepted: June 3, 2026 Online Published: June 16, 2026

doi:10.22158/elp.v9n1p376 URL: http://dx.doi.org/10.22158/elp.v9n1p376

Abstract

Financial data sharing can improve risk analysis, reduce information asymmetry, and enhance the efficiency of financial services, but it may also give rise to risks such as personal financial information leakage, superficial user authorization, excessive data sharing, unclear third-party responsibilities, algorithmic discrimination, and cross-border compliance risks. The existing legal system has established a basic protection framework through rules on personal information protection, data security, cybersecurity, and financial regulation. However, there remain significant challenges in financial data sharing, such as insufficient rule agreements, blurred sharing boundaries, unclear responsibility allocation, and inadequate technology governance. Based on the main scenarios and risk structures of financial data sharing, as well as recent research on open banking, financial privacy, digital lending, and financial security, this paper proposes that legal regulation should be built on classification and grading, substantive consent, accountability, security assessment, algorithmic governance, and cross-border governance. This paper argues that financial data-sharing regulation should shift from post-event accountability to full-process, scenario-based, and risk-driven governance, so as to balance data security, financial innovation, and consumer rights.

Keywords

financial data sharing, data security, legal regulation, personal financial information, open banking, fintech regulation

1. Introduction

Data have become one of the most important productive resources of financial institutions. Financial institutions use identity, account, transaction, credit, asset, and risk information to conduct financial transactions and business activities. Data processing plays a key role in customer identification, credit management, risk control and compliance. Research on open banking shows that connecting account

information with third-party services can support payment innovation, more accurate credit granting, and digital financial services, provided that user trust, privacy protection, and secure interfaces are institutionally guaranteed (Xie, C., & Hu, S., 2024, pp. 73-82). Financial data sharing commonly occurs among traditional financial institutions. Banks, securities, insurance, payment, credit reporting, Internet service providers, algorithm service providers, and regulatory authorities generate data and have a multi-subject, multi-interface, multi-purpose, and multi-level data processing chain. Consumers' acceptance of open banking and financial technology is closely related to perceived privacy risks, trust, and security (Chan, R., Troshani, I., Rao Hill, S., & Hoffmann, A., 2022, pp. 886-917). If financial data sharing lacks clear boundaries, data-driven innovation may turn into forced authorization and implicit profiling under conditions of severe information asymmetry.

From a legal perspective, financial data are sensitive, correlated, commercially valuable, and at risk of spillover. An individual's purchase records may reflect consumption habits, continuous account flows may indicate income levels and lifestyle patterns, and credit information may affect financing opportunities and social evaluation. UK open banking applications (as in tenant credit review) show that when financial data are incorporated into new evaluation practices, they may reshape trust between users and institutions and raises issues such as data protection, usage constraints, and interpretation responsibilities (Ciocanel, A., Wallace, A., Beer, D. G., Cussens, J., & Burrows, R. J., 2024, pp. 1810-1825). Financial data sharing should not be understood as opening the door to technical interfaces; instead, financial data should be considered part of rights protection and responsibility management.

This study explores the legal regulation of data security in financial data sharing and the issues that must be considered. The questions are as follows: (1) What are the main cases and risks associated with financial data sharing? (2) What are the limitations of current legal regulations regarding the sharing of boundaries, consent mechanisms, liability allocation, and technology governance? (3) How can legal regulations be designed to balance data security and risk with financial innovation and consumer rights? The remainder of this paper is organised as follows: Part II defines the meaning and situations of financial sharing; Part III considers the legal risks of sharing; Part IV reviews the limitations of current regulations; Part V proposes improvements; and finally, the research conclusions are presented.

2. The Connotation and Main Scenarios of Financial Data Sharing

Financial data sharing refers to financial institutions, credit reporting agencies, payment institutions, fintech companies, outsourcing service providers, and regulatory agencies reporting, opening, calling, exchanging, and reusing financial data through cooperation, risk control, customer service, compliance or public governance. Most open banking systems operate on account opening, third-party access, API standards, user authorisation, and data security (Casolaro, A. M. B., Rauber, G. N., & de Lima, U. S. M., 2025, pp. 340-355). In China, financial data sharing in digital finance may also involve joint credit granting, anti-fraud modelling, regulatory reporting, anti-money laundering, cross-border payments, and fintech outsourcing.

Financial information includes customer identity information such as name, ID numbers, and contact numbers; account balances; transaction records; payment history; lending information; credit scores; investment preferences; device information; behavioural patterns; and risk labels. Some of this information is highly sensitive, while other data may generate inference risks when cross-analysed with additional information. For example, payment frequency, spending locations, counterparties, fund flows, and even seemingly simple fields can, through continuous observation, reveal an individual's income level, living situation, and repayment capacity.

Financial data sharing involves five scenarios: joint credit granting and risk control for financial institutions; intelligent risk control, cloud computing, and customer service between financial institutions and technology companies; credit assessment between financial institutions and credit reporting agencies; anti-money laundering, anti-fraud, and prudential supervision between financial institutions and regulators; and cross-border sharing for cross-border payments, international clearing, and cooperation with foreign financial institutions. Table 1 summarises these scenarios in detail.

Table 1. Main Scenarios, Data Types, and Legal Concerns Regarding Financial Data Sharing

Shared Scene	Main data types	Main risks	Key points of legal regulation
Sharing among financial institutions	Identity information, account information, transaction information, credit information	Sharing beyond the scope, duplicate collection, and unclear responsibility	The purpose of sharing should be clearly defined, data should be minimised, and responsibilities should be established.
Financial institutions and technology companies share	Behavioral data, risk control tags, model scores, and device information	Third-party abuse, API leaks, and opaque algorithms	Outsourcing compliance, contractual constraints, and security audits
Financial institutions and credit reporting agencies share	Loan history, credit score, default information	Insufficient authorization, difficulty in correcting erroneous data	Individual authorization, objection handling, retention period
Financial institutions and regulatory authorities share	Suspicious transactions, risk data, and reported data	Excessive reporting and expansion of application	Legal obligations, principle of proportionality, supervision and confidentiality
Cross-border financial data sharing	Payment information, account information, customer data	Jurisdiction conflicts, abuse abroad, and difficulties in obtaining relief	Outbound assessment, standard contracts, and ongoing supervision

To illustrate this regulatory logic, we divided governance into six categories: legal rules, regulatory coordination, technological control, institutional compliance, consumer rights, and cross-border governance. Figure 1 depicts the overall architecture, where risk assessment is emphasized as the core mechanism, and legal responsibility, regulatory tools, and technological measures are embedded into the data-sharing process.

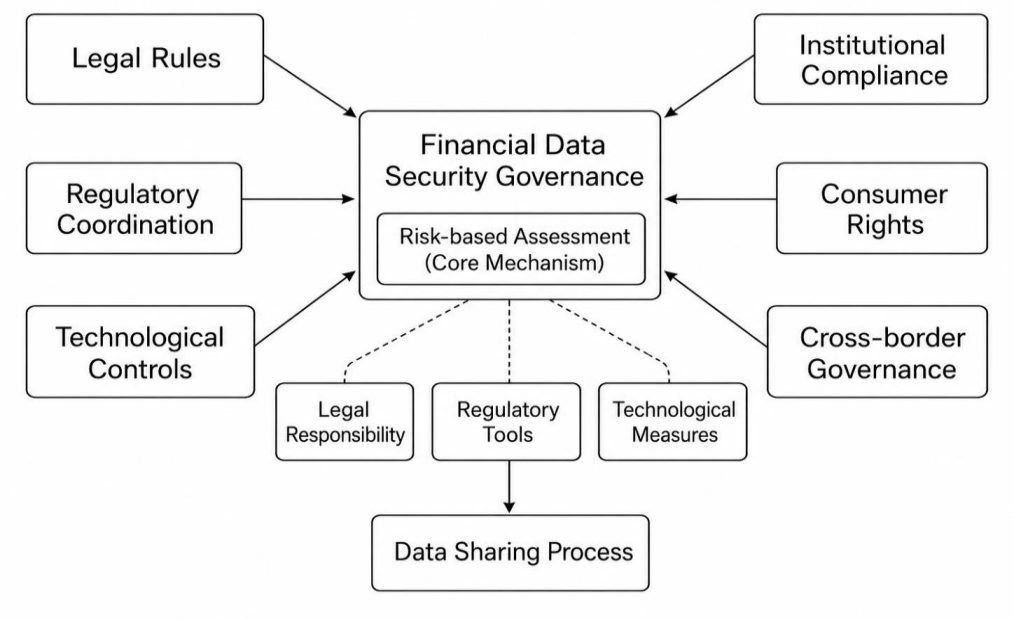

Figure 1. Overall Legal Governance Framework for Financial Data Sharing

3. Legal Risks Related to Data Security in Financial Data Sharing

An overview of open banking systems indicates that related work has moved from business openness to privacy protection, identity authentication, risk management, trust, and regulation (Preziuso, M., Koefer, F., & Ehrenhard, M., 2023). Financial data-sharing risks are based on data collection, transfer, processing, modelling, output, and deletion, as shown in Figure 2.

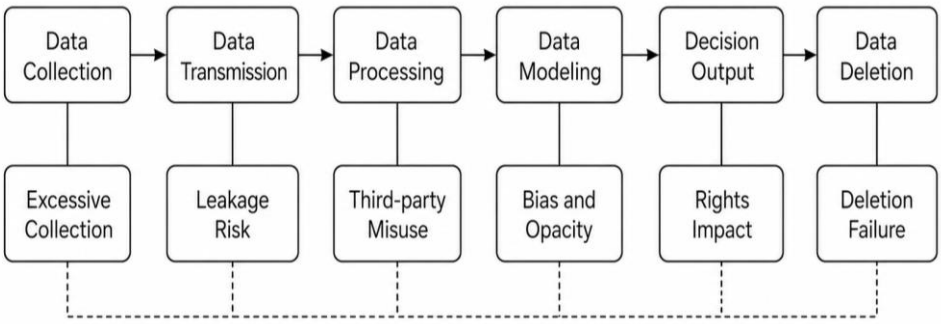

Figure 2. Risk Transmission Mechanism in Financial Data Sharing

First, personal financial information may be lost. Financial data sharing requires interface calls, docking, permission, and external messages. If encryption, desensitisation, access control, or log audits are unavailable, it may cause property loss, identity theft, illegal loans, and credit damage. Fintech cybersecurity research has found that platforms suffer from identity authentication, leakage, system intrusions, and a lack of control (AlBenJasim, S., Dargahi, T., Takruri, H., & Al-Zaidi, R., 2024, pp. 835-851).

Second, it is problematic to formally impose informed consent on participants. Financial consumers often have rather long privacy policies and complex authorization rules, and some institutions offer general authorizations under the condition of "optimizing risk control" or "personalized recommendations." Research on digital credit data privacy shows that data subjects, credit institutions, and regulators have inconsistent understandings of privacy, and rules may affect consumer trust (Koul, S., Verma, R., & Ajaygopal, K. V., 2025).

Third, there is the potential for misuse of the technology. Institutions can still consider account opening, payment, or credit data to create, recruit, train, and price differentials for AI models. In an algorithm, data can be considered as tags, ratings, or model parameters, and they have an impact even if the data are deleted.

Fourth, it is unclear whether people are responsible for one another. Data providers, recipients, entrusted processors, cloud service providers, and algorithm service providers share data, and users cannot decide whether someone is responsible for leakage or misuse. KYC data governance studies can facilitate identity data traceability through blockchain and access management (Kulkarni, A. V., Mondal, T., & Modi, D., 2025).

Fifth, there is a risk of algorithmic decisions and users' actions. Shared data are often used for credit scoring, loan approval, insurance pricing, and marketing. If the data are opaque, variable selection is biased, or the output is not interpretable, it may lead to loan rejection, differential pricing, marketing, and unfair transaction.

Sixth, cross-border financial data flow. Cross-border payments, international clearing, and global anti money laundering cooperation may all involve data left the country. Different countries have different regulations on financial privacy, data localisation, access, and relief, that can sometimes result in jurisdictional conflict and abuse abroad. Digital currency privacy researchers also warn that centralized processing of payment data might lead to surveillance and privacy risks (Kaur, G., Lashkari, Z. H., & Lashkari, A. H., 2024, pp. 1-37).

4. Inadequacies of Current Legal Regulations

My country has protected personal information, information security, security, and financial rules, such as legality, clear purpose, minimum necessity, classification and grading, cross-border data management, and rights protection. Financial industry rules impose higher compliance requirements on personal financial information, credit reporting, anti-money laundering, and fintech outsourcing.

However, data-sharing scenarios can have different purposes, chains, and dispersed entities, and current laws lack proper practices. First, the boundaries of sharing are unknown, and the necessity does not have adequate safety management and customer service standards. Second, classification vs grading. Sharing access is not correct; sharing conditions, approval procedures, and security for different kinds of data remain to be refined. Third, user authorizations are not formal, and financial customers prefer to accept only general authorisations on complex agreements. Fourth, responsibilities between multiple sources are insufficient; the boundaries of joint processing, delegated processing, and re-sharing cannot be resolved. Fifth, algorithm management and data-sharing regulations cannot be understood, and model interpretation, manual inspection, and fairness testing still need to be improved. Sixth, rules for cross-country financial flows must incorporate financial business characteristics.

5. Pathways to Improve Legal Regulation of Financial Data Security

First, a scenario-based classification and grading system was established. Classification and grading should consider sensitivity, identifiability, relevance, processing size, sharing recipients, and risk impacts. General financial business data may be shared in limited amounts; personal financial data will be subject to consent and necessity analysis; important financial data must be checked for security and institutional approval; and core data can only be shared in limited amounts.

Second, legal and purpose boundaries for financial data sharing should be clarified. Financial data sharing should be legal, legitimate, and required, and trustworthy. Data sharing based on contract performance should only be limited to financial services. Data sharing based on user consent should be clear about sharing recipients, data type, processing, and lifetime. Data shared based on legal obligations should only cover legal purposes, such as reporting of regulatory data, anti-money laundering, or court support.

Third, better informed consent and dynamic authorisation are required. Customers should be able to understand the sharing goals, purposes, and withdrawals. Sensitive financial information should be subject to consent, tiered prompts, and a visual authorisation manager. A Malaysian bank's compliance with privacy policies showed that privacy rules are both transparent and consistent in terms of personal data protection (Alibeigi, A., Munir, A. B., & Asemi, A., 2021, pp. 365-394).

Fourth, the roles of multiple parties should be defined and traceability established. Financial institutions should serve as legal collections, necessity checks, partner selection, and supervision; recipients should not expand their use area beyond consent; responsible processing parties will act according to the agreement; and joint processing parties should define their roles. Authorisation records, interface logs, security reports, and audit reports can be shared among parties.

Fifth, an audit system should be established. For large-scale personal financial data, sensitive information, important data, cross-border transmission, and algorithm modelling, pre-assessment, in-process monitoring, and post-audits are the most important processes of audit systems. Blockchain applications in banking have shown that distributed ledgers may be useful for identity authentication,

transactions, audit trails, and trusted sharing (Rahman, S. M. M., Yii, K.-J., Masli, E. K., & Voon, M. L., 2024).

Sixth, algorithms and automated decision-making should be better regulated. For credit scores, credit credit, insurance price, targeted marketing based on shared information, explanation of algorithms, manual review, review, correction, and fairness test, institutions should explain the main data sources and factors for automatic decision making, and should not use shared financial data to apply price discrimination, credit discrimination, or unfair transactions.

Fourth, cross-border financial data flows should be controlled. For transfers that involve personal financial information, consent must be obtained in accordance with the law, and the overseas payment must be aware of the information, processing, and rights. For transfers that generate money from financial information, a security evaluation must be conducted, and the obligations of overseas payments should be specified in a contract. Cross-border transfers of financial data should support financial openness and data security without weakening the role of domestic payments for business convenience.

Eighth, legal regulations and technological governance should be included in the framework. Privacy computing, federated learning, multiparty secure computing, desensitisation, differential privacy, blockchain notarization, and access control can minimise the risk of raw data exposure. Information security policy compliance research shows that in organizations, members perceive threat severity, efficacy of responses, and enforceability of systems as important aspects of rule enforcement (Alrawhani, E. M., Romli, A., & Al-Sharafi, M. A., 2025).

6. Conclusion

Financial data sharing is an important tool for advancing digital financial innovation, risk control, and regulatory technology development. Because financial data relate to personal assets, credit ratings, and market orders, financial data sharing cannot rely on institutional self-regulation or technological convenience. Instead, a law-based law-in-regulation with data security, consumer rights, and financial stability should be established. Financial cooperation regulation can be promoted from static rules to dynamic rules, from single-entity obligations to multi-entity responsibility, post-event penalties, pre-event assessment, in-event monitoring, and post-game auditing. Boundaries should be defined through classification and grading, consumer control enhanced by substantive consent, third-party responsibility reinforced through contracts and audits, and rights protected from automated decision-making violations via algorithmic interpretation and human inspection. In the future, the institutional development of financial data sharing should integrate technological governance. Tools such as privacy computing, federated learning, blockchain notarization, access control and data anonymisation can enhance the security and traceability of sharing, but technology cannot replace legal responsibility. Only by combining legal rules, regulation, technical standards, and internal institutional compliance systems can the value of the data elements be released while ensuring financial data

security while simultaneously enabling the development of digital finance.

References

AlBenJasim, S., Dargahi, T., Takruri, H., & Al-Zaidi, R. (2024). FinTech cybersecurity challenges and regulations: Bahrain case study. *Journal of Computer Information Systems*, *64*(6), 835-851. https://doi.org/10.1080/08874417.2023.2251455

Alibeigi, A., Munir, A. B., & Asemi, A. (2021). Compliance with Malaysian Personal Data Protection Act 2010 by banking and financial institutions, a legal survey on privacy policies. *International Review of Law, Computers & Technology*, *35*(3), 365-394. https://doi.org/10.1080/13600869.2021.1970936

Alrawhani, E. M., Romli, A., & Al-Sharafi, M. A. (2025). Evaluating the role of protection motivation theory in information security policy compliance: Insights from the banking sector using PLS-SEM approach. *Journal of Open Innovation: Technology, Market, and Complexity*, *11*(1), Article 100463. https://doi.org/10.1016/j.joitmc.2024.100463

Casolaro, A. M. B., Rauber, G. N., & de Lima, U. S. M. (2025). Open banking: A systematic literature review. *Journal of Banking Regulation*, *26*(3), 340-355. https://doi.org/10.1057/s41261-024-00262-x

Chan, R., Troshani, I., Rao Hill, S., & Hoffmann, A. (2022). Towards an understanding of consumers' FinTech adoption: The case of Open Banking. *International Journal of Bank Marketing*, *40*(4), 886-917. https://doi.org/10.1108/IJBM-08-2021-0397

Ciocanel, A., Wallace, A., Beer, D. G., Cussens, J., & Burrows, R. J. (2024). Open banking and data reassurance: The case of tenant referencing in the UK. *Information, Communication & Society*, *27*(9), 1810-1825. https://doi.org/10.1080/1369118X.2024.2310481

Kaur, G., Lashkari, Z. H., & Lashkari, A. H. (2024). Privacy implications of central bank digital currencies (CBDCs): A systematic review of literature. *EDPACS*, *69*(3), 1-37. https://doi.org/10.1080/07366981.2024.2376794

Koul, S., Verma, R., & Ajaygopal, K. V. (2025). Stakeholders' understanding of data privacy: Implications for digital credit consumer. *Cogent Business & Management*, *12*(1), Article 2568200. https://doi.org/10.1080/23311975.2025.2568200

Kulkarni, A. V., Mondal, T., & Modi, D. (2025). Enhancing privacy in banking systems: A blockchain-based access management and KYC solution. *Cogent Business & Management*, *12*(1), Article 2570063. https://doi.org/10.1080/23311975.2025.2570063

Preziuso, M., Koefer, F., & Ehrenhard, M. (2023). Open banking and inclusive finance in the European Union: Perspectives from the Dutch stakeholder ecosystem. *Financial Innovation*, *9*(1), Article 111. https://doi.org/10.1186/s40854-023-00522-1

Rahman, S. M. M., Yii, K.-J., Masli, E. K., & Voon, M. L. (2024). The blockchain in the banking industry: A systematic review and bibliometric analysis. *Cogent Business & Management*, *11*(1), Article 2407681. https://doi.org/10.1080/23311975.2024.2407681

Xie, C., & Hu, S. (2024). Open banking: An early review. *Journal of Internet and Digital Economics*, *4*(2), 73-82. https://doi.org/10.1108/JIDE-03-2024-0009