Studies in Law and Justice
ISSN 2958-0382
www.paradigmpress.org/slj
Volume 5 Number 3 September 2026

Legal Determination of Discriminatory Treatment in Opening Bank Data Interfaces

Wen Li[1]

[1] Quanzhou Huaguang Vocational College, Fujian, China
Correspondence: Wen Li, Quanzhou Huaguang Vocational College, Fujian, China.

doi:10.63593/SLJ.2026.09.06

Abstract

Whether open banking can promote competition depends on whether third parties can use data under the legal, secure and stable conditions. Capitation, update delay, repeated authentication can be used to control risks, but it may increase the operating cost of competitors. This paper takes in the combination of relevant research, and uses the transaction cost theory to explain how the access dependence forms, to improve the cost theory analysis of the technical limitation that affect the competition, and use the context integrity theory to discuss the legal limit of data use. On the basis of this, the analysis is conducted from the four aspects, dependency relationship, treatment difference, competition impact and security reason; When we compare the access treatment, the risk corresponding to the above disputed measure should be considered first, and then should be determined whether, when meeting the same security requirement, the access condition which does not exclude competition can be provided, and when reaching the similar security level, whether there are feasible solution with less restriction on competition. The bank cannot directly regard the operation difficulty caused by the restriction as reason for further restriction, and the emergency suspension should also be subject to the subsequent review; The evidence and remedy must follow the current law, the access dependence cannot replace the proof of the market dominance, and the individual authorization does not mean that the bank have the unlimited obligation to open up.

Keywords: open banking, access dependency, increase competitor costs, context integrity, financial security defense

1. Introduction

1.1 Research Background and Issues

Usually, open banking refers to the situation that with the client's permission, the bank transmits the information of account and transaction through the technical interface to the third party. Through this, the third party can use the client's existing data to provide the service, but the bank still controls the operating condition of the interfaces. Being able to access the interfaces does not mean being able to continuously provide the available service. For example, update speed, field integrity, call limit, and authentication requirement, all affect the actual operation of the third party. Even if the bank does not refuse to transmit, it may change the competitive situation of the third party through these conditions.

Transaction history needs long-term accumulation. For example, after the client

changes the accounts, the same records cannot be formed in the new account immediately. For the access of a bank by a third party, it may be necessary for it to spend in the development, the testing and the compliance of the resources. After that the quality of the service still depends on the arrangement of the interface of the bank. If the conditions change in any time, the extra cost and the customers' fail of the dissatisfaction may mainly be borne by the third party. Therefore, the law should distinguish the reasonable management of the interface from the behavior of the restriction of the competition by the conditions of the interface.

This distinction must consider the security responsibility. There are really some differences in the scope of authorization, the capacity of data processing, and the abnormal behaviors of the third party. The bank also has the responsibility to protect the information of the customer and the stability of the system. It is not reasonable to ask all the institutions to get exactly the same access condition; but to accept any restriction according to the "security need" is also without basis. The key is to say what kind of risk exists, why this restriction is needed, and thus give the corresponding evidence for the relevant departments to check.

The main object of this article is the reading of legal authorized personal account and transaction information. It does not involve information scraping that is not authorized, nor does it apply the same risk standard to the execution of payment instruction and information query. This research is based on the existing access relationship or the access obligation that can be demonstrated, not to derive from the name of open banking in China a unified mandatory open system. The internal credit scoring, the complete risk control model and all the derivative data should not be in the argument of this article.

1.2 Literature Review and Research Gaps

The review by Dezem et al. shows that the research of open banking is addressed by the system integration, the security and the models of implementation (DEZEM V, MARTINS R P, MACEDO M, et al., 2023). The review also points out that the research of open banking should not only think about how the interfaces are built, but also ask is the special access and operating conditions can really make data sharing work.

Sharmin et al. speak of personalized services, of modular cooperation, of security compliance and say that banks can cooperate with third parties or compete with them (SHARMIN S, PRABHA M, JOHORA F T, et al., 2024). Nothing in the validation of their workshop shows the scope of this, and this cannot be used to see if the incidence of interface exclusivity behavior is in it. The fact that there are cooperation and coexistence of the fact that there is competition is the point of departure to see the incentives in this article, not the argument that the banks have put in place some kind of discrimination.

Lazo studies third-party information security management from qualitative interviews with banks and financial service. The description of the narrative about false alarms in data leakage prevention systems shows that the security rules may be blocking the transmissions that are in fact needed by the business, and the management is still in reality to be corrected, with testing, exception and permission arrangements (LAZO G A., 2024). This study does not study the competitive violations neither, and it only can say that the security decisions may be wrong. Using the security tools does not show that each restriction is needed.

Maksic et al. have studied service experience and satisfaction of the customers of the Serbian bank, which include the efficiency, the system availability and the privacy (MAKSIC K, GOLITSIS P, RADEV L, et al., 2024). According to their results, we can say that the service quality has an economic meaning, but we cannot use it directly to estimate how much competitive damage can be done in the Chinese interface market.

Borgogno and Colangelo noted that data sharing needs to be also standardization and some specific arrangements of implementation (BORGOGNO O & COLANGELO G., 2019). He, Huang and Zhou's model reveal that the welfare effects of sharing depend on the condition e.g. information structure (HE Z, HUANG J & ZHOU J., 2023). Awrey and Macey focus on the aggregation structure, he also notices that the open finance may form the market power in the new structure of links (AWREY D & MACEY J., 2023).

The circular relationship of risk classification and the comparison object is that in this article: the scale reduction, error increase, or service instability of having the access restriction is the cause, that may be used as the basis for the

aggravating restriction of. If the causal direction is not known, "different conditions" may not be able to be denied, so the comparison, defense and evidence rules need to be designed together.

1.3 Research Methods and Analysis Scope

This paper contains both the theoretical explanation and normative analysis: the mechanism of dependency and competitive harm are identified by the theory in this paper, the obligations and the liability thresholds are found by the present laws, and the above aspects are explained by the empirical research in this paper. This paper does not calculate the incidence of the behaviors in Chinese market, and this paper also does not interpret the experienced situations in the individual interviews as the general causal conclusion.

The argument is developed in four levels: first, why the interface relationships could bring difficult exit dependency; second, how the technological conditions change the operating costs and the service quality; third, which data flows have some legitimate purpose and some safety bound; finally, how to translate the above regulation in a comparison, defense and gathering of evidence rules.

2. Theoretical Framework

2.1 Transaction Costs and Access Dependency

In transaction cost theory of Williamson, uncertainty, transaction frequency and specific investment are emphasized (WILLIAMSON O E., 1979). The field mapping, authentication development, and the compliance testing which are completed by the third party for a certain bank, are usually not applicable to other banks. Such investment has relationship-specificity. After the service is operational, when one withdraws from the cooperation, it will lead to the customer function interruption and the depreciation of the initial investment. Thus, the bank can set down strong constraints to third parties on change of the access condition.

The dependency also comes from the data itself. Even if a customer holds multiple accounts, other accounts may not be able to replace the continuous records of the main account. The technical conversion cost is the expense that a third party needs to pay for system modification; the information reconstruction cost is the time and resources that one need to re-acquire the necessary transaction records. To see whether an alternative channel is effective, it is necessary to simultaneously consider the data coverage, update frequency, and legal acquisition conditions.

It is difficult for access contracts to pre-agree on all security issues. Because the vulnerabilities, the abnormal request, and system upgrade are changing all the time, the bank should keep the adjustment authority, and the third parties also need the relatively stable investment expectation. We should make a reasonable arrangement: the bank can make adjustments according to the risks, however, the reason of the adjustment, the scope of influence of the adjustment, the recovering condition of the adjustment and the error correction procedure of the adjustment should be clearly specified. The changes without reasons and the deadline will make third parties bear the operating risk which is difficult to estimate in advance.

The higher the specific investment and the more difficult it is to obtain alternative data, the more likely access downgrade will weaken the negotiation power of the third party. The negotiation advantage is not the same as the market dominance position under antitrust law. A bank may still be constrained by other accounts, financial services, or data channel. The dependency analysis explains why it is worth to review, whether it bears antitrust liability, but also needs to look at the competition in the market, actually.

2.2 Increasing Competitor Costs and Non-Price Constraints

The theory of increasing competitor costs proposed by Salop and Scheffman shows that it is not the case that the necessary manifestation of the exclusive behavior is the complete elimination of the competitors. Changing the conditions of costs of the competitors can also weaken the constraints of the competitors (Salop, S. C., & Scheffman, D. T., 1983). When this theory is applied to the dispute of the interface, still we have to show that the bank has the ability to maintain the restrictions, that the third parties do not have effective alternatives, and that the changes in the cost are enough to affect the downstream operation. The existence of the competitive relationship could not prove the validity of the exclusive strategy.

For example, the nominal access price is not changed, but for example, to complete the same service, more investment is needed. For example, data update delays will increase manual

verification, cache maintenance, and customer service expenses; repeated authentication will increase user operations and may cause customers to attribute the failure to the third party. Therefore, the impact of competition cannot be judged only by the charges, but also by how the interface conditions change costs and service quality.

The relationship between the bank and the third party may simultaneously contain cooperation and competition. The third party uses the bank's data to provide budget management or loan comparison service. The bank needs to supply data continuously. The third party may also compete with the bank's own products for the customers. Therefore, the bank may benefit, and the bank may restrict. This only indicates the relationship of interests. The measures and the security basis still need to be identified. The possible motives cannot be regarded as the proof of the actual behavior.

Also, multiple minor restrictions may accumulate to produce effects. For example, a lower limit, a repeated authentication and a lack of updated documentation, taken alone, may not be enough to disrupt business, but taken together they may force the third party to repeatedly remedy. The review should therefore be on the effect of a normal service over a reasonable period, excluding the error of the third party and of widespread failures of the system, and not too much to pass.

The third party's own inefficiency: or, making requests that are not only allowed by the legitimate service needs of that third party, their losses are, not necessarily considered as competitive damages. The legal guarantee is the effective competition, and not the expected profit of a certain operator. The we should compare with the benchmark shall be a legal, secure and cost-effective access arrangement, and not set as the free, unimitated calls and no authentication required interface.

2.3 Context Integrity and Data Usage Boundaries

According to the theory of context integrity of Nissenbaum, the flow of information should be judged in the context of the specific scenario for decide if it is in accordance with the appropriate norms (NISSENBAUM H., 2004). The same transaction record, which is used for the customer authorization for income and expenditure reconciliation, and for the marketing profiling for nothing related, cannot be judged with the same. To decide the legal flow the data content, the data provider, the data recipient, the purpose of the service, and the method of transmission need to be seen together.

Even if the two institutions obtain the customer consent, the two do not have the same risks. One of the institutions reads only the fields necessary and deletes it very quickly, the other one has the complete records and gives to every other entity. The two should be subject to different reviews. When we compare the treatment of access, the way the data is really used should be explained, not only classified in function of the size of the institution or of the nature of the cooperation. The customer authorization still has to be restrained in term of purpose, of necessity of the scope and of security obligations.

Security is not only encryption and authentication. The review of Waweru et al. is also on such as the factor of social engineering, the personnel training and the internal process (WAWERU E, KARUME S M & KIBET A., 2025). The materials of Waweru et al. cannot be used to determine the actual risk of a certain third-party in China, but it recommends that using permission, how to handle exception and how to report the event are as important as what he speaking above. Through one authentication, it is not mean that all business and all period are not risk; the small scale does not mean that the specific process is certainly not safe.

The data flow that is appropriate cannot be defined by the bank itself. For example, if the self-operated business and the external business are classified into different categories only because they are different identities, the bank has to explain why the actual risk is different. The bank has the right to do the security management of itself, but it does not have the right using its commercial interests to be the base of security classification indiscriminately. The judgment should be restrained by law, legal business purpose, and verify facts.

2.4 Risk Adjustment and Counterfactual Analysis

These three theories explain different things. Transaction costs explain why third parties are hard to withdraw; increasing the cost of the competitors explains how the restriction affects the competitive conditions; contextual integrity explains which flows can be legitimate objects for comparison. The integrated causal sequence is: dependence makes the access conditions binding, if the conditions are different, they change costs

or quality, changes may weaken the competition, and risk differences and their handling requirements may give a legitimate explanation for these conditions. Only by putting this causal sequence together, the argument cannot be concluded with the "open advantage" or "financial sensitivity" directly.

In this paper, two counterfactual tests are proposed, that is to say, comparing with the actual measures with other possible arrangements. First, under the condition that corresponding security requirement is met and the cost is feasible, can the banks give the access conditions which do not exclude the competition? Second, is there a way that can have the similar level of security and put less restrictions on the competition? The former is for not using the unbound access as the benchmark, the latter is for requiring the bank to explain the necessity of the present measures, neither of which is for the court to make the best system selection on the behalf of bank.

The comparison also has to separate the sources of risk. Bank throttling can lead to an increase of the error rate of third parties and a decrease of customers. If one uses this result to prove that the risk is high, we have a circle. The review should make the separate look of the existing risks before the restrictions, the change of risks that happens alone and the abnormality that is caused by the restrictions.

3. Legal Determination of Differential Treatment in Interfaces

3.1 Legal Basis for Access Obligations

In any case, for differential treatment to be considered, there must be a legal basis for access. In particular, Art. 45 of the Personal Information Protection Law states that when the following conditions are fulfilled, a means for the transfer of personal information should be given, however, it cannot be directly inferred that any third party has the right to make, in real time, free and unlimited requests for access (Standing Committee of the National People's Congress, 2021). The obligations deriving from the contract should be clarified with respect to the data and service levels stipulated; the ones deriving from a regulatory rule should be also looked in respect of the subjects and scopes of applicability. The customer consent has to respect the legitimate purposes, the necessary scope, the business conditions of the recipient.

Article 22 of the Anti-Monopoly Law prohibits the operator with the market dominance to operate the specific abusive behaviors without reasonable reasons, such as the behavior including using of data, using of algorithm, using of the technology, using of the platform rule (Standing Committee of the National People's Congress, 2022). The arrangement of interface cannot be exempted from the review just because it is the technical management; the bank cannot just because have the financial data, has the obligation to open up in the case of anti-monopoly. The safety defense referred in this article is the claim of the bank that the specific risk is the reason why the act is the legitimacy.

3.2 Comparability of Access Conditions

The phrase identical conditions should not be interpreted as the complete consistency of the transaction counterpart in all conditions. Any two institutions will have differences in size, in history, in technical architecture. If you ask for the absolute uniform, the review of differential treatment will lose in practical application space. On the contrary, if you just consider similarity in providing similar products, you will ignore the real differences in the ability to handle the sensitive information. The risk adjustment comparison proposed in the present article should check that the differences have a substantive impact in the disputing condition of the access and to prove this impact in the context of the business task which is in the question.

The first dimension is purpose and authority. For example, reading account balances, downloading of historical transactions and continuously monitor the changes of accounts may need different scopes of information and the speed of updating. The calling quotas of two institutions are capable to be compared directly only when the purpose and the boundary of the authorization are like the same. If one side requires the more record, the unit authorized customers, the unit data volume and the task frequency should be compared instead of just compare the total calling volume. This can avoid to confuse the difference of business scale with the differential restriction.

The second dimension is access security capabilities. The key is not in the overall reputation of this institution, but in the authentication management, permission isolation, vulnerability repair and event response capabilities related to this access. The low visibility cannot independently as evidence of

high risk, and the large institution does not necessarily have more reliable specific system. The third dimension is resource consumption. We should identify request load, concurrency, query complexity, and abnormal retry. The fourth dimension is legal and performance conditions, which includes the business qualifications, the restriction on the data using, and the actual performance records.

In the comparison, the causal direction in the theoretical framework mentioned above, is manifested as the issue of indicator sources. Suppose Bank A provides similar data access to two institutions, Bank B and Bank C. If Bank A first restricts Bank C's interface and as a result, the customer of Bank C grows slower, and Bank A then explains the lower quota on the ground of Bank C is smaller. It will take the consequence of the measures as the original cause. Similarly, the error rate caused by the lack of updated documentation cannot directly be used as the evidence of the access party's low ability. The review should distinguish the pre-existing risk, the changes caused by the outside event, and the indicators of the restrictions formed by the dispute. Only the relative independent risk differences are suitable as the explanation for the access difference.

3.3 Judgment of Substantive Unfair Treatment

Interface treatment is not a single numerical value. The response time description indicates how long it takes to receive feedback, whether the availability description can be connected, the data freshness description shows how far the record is from the latest state, the completeness description indicates whether the required fields are complete, and the authentication burden description indicates how much additional operation the user needs to pay for maintaining the service. If the bank only proves that the interface is online, it cannot fully address the issues of data obsolescence and authentication friction; the access party only proves that individual requests are slow, but it cannot explain that the overall service has been significantly weakened.

The explanation of service functions also needs for the substantive unfair treatment. A delay has not affected the promised function it can only show the difference of technical. It cannot directly be explained as the competitive barrier. If the call failure makes the legal task cannot continue to be completed, then it has to be reviewed more. The judgment benchmark should be come from the legitimate business pass need, the contract or the apply standard, it cannot be set by the access party as the "ideal performance" arbitrarily. The open of data does not mean that the account provider should bear all the expansion cost for all the future products.

When, the request types, time period, data volume, retry rules should be as controlled as possible when comparing, and the duration and abnormal distribution of the differences should be observed. When there is no outside comparison object, changes of treatment in time with same institutions can be clues, but the reasons, e.g. accident, load, upgrade, etc. should not be taken as it is. The comparison of tech feasible and comparison of legal entity should be treated separately.

3.4 Market Dominance and Competitive Harm

Bank control of specific customer data does not mean that the bank has a dominant position in the relevant market. It is not sufficient to narrow the market to "the data market of a certain customer of Bank A", because the specific records cannot be directly copied by others. Otherwise, every data holder could be a monopolist. It should be examined based on the service purpose the other data sources, the degree of customer substitution, and the time and cost required to obtain other data or to reconstruct the records.

It is better to think about differentiating the data access service and the downstream financial service and check the transmission relationship to them, but it is not necessary to think that they should be divided into two market. How the access can be traded independently and whether the customer can easily transfer to other account will affect the judge of the market. The market share of the bank in the deposit and loan business cannot be used to prove the market power of the bank in the disputed access business without the reason.

Competitive harm should describe the complete causal relationship: first step is to clearly identify who implemented the restriction; the second step is to explain that it have increased the cost or reduced the functionality required for reasonable operation; the third step is to prove that this impact is sufficient to change entry, operation, or customer switching, and not only a reduction in the income for a single institution that is temporary.

3.5 Types of Behaviors and Their Applicable

Boundaries

From the evaluation path of differential treatment and refusal of transactions provided by the Anti-Monopoly Law Article 22 and the related judicial interpretation, article 41 of the 2024 judicial interpretation is the substance of transaction conditions and competitive impact (Standing Committee of the National People's Congress, 2022; Supreme People's Court, 2024). If the corresponding third party is only subjected to bad conditions, we can talk about the problem of differential treatment; if the condition is so bad that the deal cannot be concluded, we can talk about the problem of refusal of transactions; if it is also set with some irrelevant requirements, it is also the problem of unreasonable transaction conditions. We should choose which path to be according to the fact and the litigation request.

Some interfaces not meeting the expectations of the third party does not mean that the bank should open all internal systems. Not because no comparable institutions can be found, one can simply call it "substantive refusal" to bypass proof. The bank uniform restriction of all external institutions is not because it is legal or illegal; it still needs to be looked at regarding the access foundation the extent of restriction the technical possibility and the effects to competition.

Article 38 of 2024 judicial interpretation is in view of the factors of technical feasibility, substitutability, dependence, and competitive consequences in the issues of refusal of transactions regarding interface compatibility and open sharing (Supreme People's Court, 2024). We can link with the analysis of access dependence, but the respective of the conditions that cannot be omitted. the idea of necessary facilities can hint the importance of substitutability and reconstruction cost, but it is not appropriate to say 'data cannot be replicated' is equal to 'must be open'. The transaction record is also the customer right, the information of other transaction participants and the investment in the bank maintenance system. Whether there is an executable, secure and proportion method to access that meet the business need is the premise for us to discuss the open measure.

4. Review Criteria for the Financial Security Defense

4.1 Risk Basis and Professional Judgment

The security defense should clearly declare what risks the measures are meant to avoid. For example, unauthorized reading, token fail, storage vulnerability, and abnormal concurrency, all the of above can affect security, but the measures are different. To prevent unauthorized reading, is not necessary to drop of the update frequency of all normal requests. To mitigate the system overload is not necessary to increase the frequency of each authentication. Only when one knows clearly what risk, what object the risk affects, and how the risk is connected to the disputed access, one can say whether the measures are right.

Banks do not need to wait until the losses occur before he/she takes the action. Banks can handle the issues based on the vulnerability, the abnormal signal, or the trusted threat intelligence in advance. "Theoretically possible leakage" is not enough to explain, that only the certain institution has been long-term throttled by. The preventive measures should have the fact, what should trigger the measures and the measures after the incident should explain, what was the scope of the incident and how is connected the accessing party. The weaker is the risk basis, the more comprehensively and long-time the restrictions and the more the bank should give the full explanation.

The professional judgment should be respected, but the respect should be based on the judgment methods and the materials. Reviewers do not need to design firewalls or to select parameters for the bank, but they can check if the judgment is based in some relevant data, if counterarguments and revised outdated conclusions have been taken into account. It is ok to have errors in reasonable predictions, but decisions that have not the documentation and the shifting of reasons cannot not be used as excuse of the technical complex to avoid the review.

4.2 Relevance and Necessity of Measures

The bank should also explain the measures that can be taken to reduce risks. The review should identify which risk aspect the measures are targeting. Reducing the number of read operations may alleviate system load but may not fix storage risks. Frequent authentication may prevent token abuse but may also increase errors, because of complex jumps. The bank should not assume that the measures are effective just because the measure name contains "security". The connection can be illustrated with security testing, incident retrospection, trusted technology assessment.

Orucho et. al reviewed the ways and advantages/disadvantages of different encryption schemes in the transmission of data in mobile banking (ORUCHO D O, AWUOR F M, MAKIYA R, et al., 2023). From this, we know that the choice of the technology needs to have specific analysis and cannot be regarded as a general security authentication in view of the technical suggestions in the review. The necessity analysis is to ask: Under the premise of achieving a reasonable level of security, is there a less competitive and feasible approach? For example, only suspending the permissions that cause abnormality may be more precise than deactivating all the interfaces; restricting the abnormal requests while retaining normal requests may be more appropriate than uniformly lowering the amount; requiring the repair of specific vulnerability s and the retest may be more targeted than indefinitely excluding the access. These are possible solutions that need to be tested in the specific scene and cannot be uniformly required of the banks without considering the cost.

Alternative solutions must have similar risk control capabilities. For example, it is impossible to refute the current measures by just saying use more advanced technology, without to say how much mature, how long it would take, and how much the cost is. Banks cannot just reject the alternative solution if it just increases the cost. The review should compare the incremental cost, the difficulty of implementation, the risk effect and competitive impact, and also make the difference between the normal maintenance investment and the more required than that of the access scope.

The necessity of measures may also change in time. For example, in the beginning of the event there is not enough information so that in the beginning it was reasonable to suspend completely; after that one finds out that the problem is about few permissions so that to continue to block all the interfaces one should give an explanation. The decision in the beginning is reasonable but there is no reason to always say that the restriction in the later should be reasonable. So, why take the measures and why continue the restrictions should be separately reviewed and the continuous measures should be checked.

4.3 Risk Classification and Uniform Application

It does not mean that institutions with different risks should enjoy the same treatment with uniform application. It requires that similar risks should receive similar treatment. Banks can make classification rules, but they need to have reason to explain how the classification basis determine the measures. If a competitor is classified as high risk, but a partner with in the same risk is not restricted, the bank should explain what other facts there are that can support that there is a difference in handling.

For example, if a bank restricts a certain institution on the grounds of its small size, while a partner of the same size is not restricted, the bank should explain whether there are indeed different conditions for the separation of authority and so on. If the initial reason was a scale issue, but later it involved changes in qualifications or load, and there were no relevant records during the same period, it will weaken the credibility of the explanation. If a bank publishes unified rules, it does not mean that the actual application is always uniform. It still needs to choose appropriate measures based on specific circumstances.

Banks can update safety standards, but they should explain the basis of the risk and notify the access party and give a reasonable migration time. If only competitors have difficulty meeting the requirements, even if the new rules formally apply to all institutions, it should still be examined whether it is related to the safety goals. On the surface, neutral standards may also have adverse effects that need to be explained, but this effect itself cannot exempt the burden of proof for the elements of the illegal act.

4.4 Emergency Measures and Continuous Review

In the case in which there is a credible basis for an urgent risk, the bank can do some temporary, to not expand losses measures to try to wait for a complete hearing. It is better to keep on the event the necessary records, and when there is the possibility to do it, explain how much is the scope of impact and the conditions to recover and the channels to review. The explanation of the event done after the event has not to disclose any detail which can be used by the attacker, but it would let to the accessing party to know what have to be corrected in that case.

The recovery conditions should correspond to the specific risk. For example, if the risk is the certificate expiration, in principle, the judgment should be based on certificate repair, and the irrelevant exclusivist cooperation requires

should not be added as an opportunity of recovery. The bank can check the effect of rectification, but testing cannot be a reason of endless waiting. If the risk still exists, the basis of continuing restrictions should be explained regularly, and the requirement for the accessing party to prove an "absolute security" that is impossible to achieve should not be made.

5. Evidence Rules and Remedy Mechanisms

5.1 Allocation of Burden of Proof

According to Article 28 of the 2024 Judicial Interpretation on Anti-Monopoly Civil Litigation, the plaintiff shall prove the existence of market dominance and its abuse, and the defendant shall bear the burden of proof for the defense of the legitimacy of the behavior (Supreme People's Court, 2024). This article does not describe "the bank proving the safety reasons" as a newly created and universal inversion of the burden of proof. What needs to be improved is the existing allocation of proof content in the interface scenario. The plaintiff can not only claim that the safety reasons are not credible and thereby do not give its own proof, and the defendant cannot avoid present the legitimacy materials by citing that the plaintiff cannot obtain the internal logs.

The access party should submit the basis for access, the disputed interface and the period, the request response, communication records, comparable objects and business impact. If it is a single failure, first the configuration and maintenance reasons of the party should be excluded, and for the continuous difference, the different processing of similar requests should be explained.

The legitimacy materials should enable the reviewer to restore the decision and test whether a less restrictive solution is feasible. General security systems can only explain how to manage in general, but cannot explain why a request from a certain institution is abnormal or why it has been long-term deactivated. The bank should provide the risk discovery corresponding to the disputed measures, the decision basis, the applicable scope, the review and recovery records.

Three types of obligations should be distinguished. The obligation of explanation is the obligation the parties should specifically explain the claim; the obligation of presenting evidence is the obligation the holder of specific materials should provide the materials under the applicable procedure; the ultimate burden of proof is the adverse consequences when the facts cannot be ascertained. The three can support each other, but they cannot be confused. This article does not suggest that the bank by having access to the information should bear the whole burden of proof for the illegal elements, but rather the availability of controlled evidence should be strengthened.

5.2 Acquisition and Verification of Technical Evidence

Third parties can observe their own transactions but have no knowledge of whether the bank has configured different rules for other of institutions; the bank has knowledge of the gateway settings, rule versions, and risk handling records. The review has to cross the information from both sides. Request times, identifiers, and error codes can be matching clues. However, clock errors, retries, missing logs, can lead to misjudgment, which have to be explained by the personnel with the proper capabilities.

The materials submitted for the application should specify the target, period, related facts, and reasons for not being able to obtain them on one's own. The dispute is the reduction of the credit limit, so one should obtain the evidence related with the credit limit change and the load records, not to release all the source codes of risk control. One can look the rule summaries and the sample materials firstly, and only open the scope when there are still questions. It can reduce the exposure of the irrelevant information and the review cost.

For materials involving comparable institutions, for anonymous numbering, summaries of risk attributes and for restricted access, we can also use for them, to avoid to disclose the lists of customers and the details of the transactions. For the de-sensitization, it should not delete the names, but leave on the other side sufficiently detailed to re identify the customer. The access party should ask itself on what basis are the differences? it is not necessary it know all the data of the competitions; if the anonymization affects the verification, the limitations should be explained and other materials should be filled.

The legal evaluation is made by the court or regulatory authorities, experts can explain performance differences, risk paths and the feasibility of alternative solutions. The interests, methods, data sources, and uncertainties of the experts should be subject of review. The industry certification is not sufficient to prove security for

the entire period. A single test is not sufficient to support the research and exclusion for the fact that a single test failure is not sufficient to.

The legal consequences resulting from the refusing to provide evidence must be determined according to the procedures applicable. The confidentiality only involves the access ways and condition of protection, but it does not mean that there is no way to check the evidence in the normal way. If the scope is clear and there is reasonable protection, there should not be a good reason to refuse to provide the materials, and the consequence should be judged according to the procedures applicable. When the retention period is expired or the original records do not have the fields, the judgment should be based on the fact and not infer the adverse situation uniformly.

5.3 Operational Supervision and Comparative Method Reference

The UK Open Banking regulations separate the regulation obligations, the instructions for operational implementation and the reference of performance benchmark. They also consider the evaluation of the availability and the performance linkage between the dedicated interfaces and the direct channel of the customer connection (Open Banking Limited, 2026). The statistical data of the open interfaces also give the way for the monitoring of their real operational state (Open Banking Limited, n.d.). These materials show that the access quality can become an object that is recorded is continually. The value of this reference is that the debate goes from the general response of "an interface has been provided" to the verification of the particular performance and service arrangements.

Aggregate indicators are suitable for daily supervision, but not for replace institutional level comparison. For example, a high overall availability rate may hide the degradation in some local, while a low availability rate may only mean that there are wide failures somewhere. Thus, for the aggregated result which is publicly disclosed, dispute handling should check the records of some specific institutions for which is necessary, and also controls the exposure of customer information.

5.4 Scope of Relief and Implementation Conditions

For the ordinary performance dispute, they can be settled in the way of the restoration by contract, cost recovery or compensation. For the issue which is not in the industry standard, it can be solved for the corresponding regulation procedure. For the anti-monopoly relief, it is based on the establishing of competitive violation. It is good to distinguish these paths for the diligence of the technical dispute and also will not include all the interface failure in the competition lawsuit.

The relief should be aimed at the above-mentioned restrictive methods. If there is no reasonable basis for the amount difference, it should be adjusted and the standards should be clarified; if the certification burden is too heavy, the corresponding processes should be improved; if the update is delayed, the update arrangements should be implemented. The order should not simply require opening of all data, or just state "stop discrimination", but should specify the applicable objects, the data scope, the verification indicators, the time limit and the security exception.

Differences should also be corrected so that the quality is not flattened downward. The argument of uniform treatment also cannot be used by the banks in order to correct the originally better comparable interfaces to that is unusable. But this does not mean that also all the institutions should get the highest-level services. First, the legal functions required, cost feasibility and the compliance with the legal obligations should be determined and then the service classification with objective basis should be kept.

It is not possible to count all the money not earned as a loss, nor should only the technical repair costs be compensated. Extra customer service expenditures are easier to record. Compensation should distinguish between access restrictions, own errors and the impact of market changes. Customer churn and future revenues should be compared with the situations that would have been the case without the disputed restrictions. Comprehensive estimation can be made by comparing the data before and after the restrictions, the businesses that are not affected by the restrictions, and the situations of the similar institutions.

6. Conclusion

The open interface has not removed the control of the banks for the conditions for the data usage. The fact that the third-party investment is specific, the fact that the bank has achieved the accumulation of the large part of the history of the transactions of the customers and the fact that

he has to work in continuous, could make that there is access restrictions that could have an effect on the downstream competition. The law should think of the degree of the reliance, the changes of the cost and quality, as well as the scope of the legal use of the data, to not just declare an effective opening because of the existence of the open interface.

The treatment comparison should identify the risk differences related to the disputed conditions. The security review should explain why the measures were taken, why they continue, and whether there are feasible alternatives with the same security level but smaller restrictions. The treatment comparison should not identify the errors and the operational difficulties that are caused by the restrictions as being due to the initial restrictions. Emergency suspension can be done first, but the maintenance afterwards still needs the corresponding basis.

This framework does not make an unlimited right of open access independent of the current law. The personal authorization, the contracts, the regulative obligation and the anti-monopoly responsibility have each their area of scope, and the analysis of the reliance cannot in general be replaced to the proof of the dominance of the market. The evidence should follow the existing distribution and he check the facts with the bilateral logs, the classification criteria and the review records, and use the necessary confidentiality measures. The relief should attack the restrictions identified, keep the effective access of the use that is needed for the legal service, and also keep the space of the risk management with the factual based.

References

AWREY D, MACEY J. (2023). The Promise & Perils of Open Finance. *Yale Journal on Regulation, 40*, 1. https://chicagounbound.uchicago.edu/journal_articles/10420/.

BORGOGNO O, COLANGELO G. (2019). Data sharing and interoperability: Fostering innovation and competition through APIs. *Computer Law & Security Review, 35*(5), 105314. DOI: 10.1016/j.clsr.2019.03.008.

DEZEM V, MARTINS R P, MACEDO M, et al. (2023). Integrative Review of International Publications about Open Banking. *Modern Economy, 14*, 551-568. DOI: 10.4236/me.2023.145030.

HE Z, HUANG J, ZHOU J. (2023). Open banking: Credit market competition when borrowers own the data. *Journal of Financial Economics, 147*(2), 449-474. DOI: 10.1016/j.jfineco.2022.12.003.

LAZO G A. (2024). Third-Party Information Security: Generic Qualitative Inquiry in Banking and Financial Services. *Journal of Financial Risk Management, 13*, 576-603. DOI: 10.4236/jfrm.2024.133027.

MAKSIC K, GOLITSIS P, RADEV L, et al. (2024). Impact of Digitalization on Serbian Banking: Social Factors and Customer Satisfaction. *Theoretical Economics Letters, 14*, 2000-2035. DOI: 10.4236/tel.2024.145100.

NISSENBAUM H. (2004). Privacy as Contextual Integrity. *Washington Law Review, 79*, 119-158. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/.

Open Banking Limited. (2026, March 18). Key indicators for availability & performance. https://standards.openbanking.org.uk/operational-guidelines/availability-and-performance/key-indicators-for-availability-and-performance/latest/ (Retrieved October 11, 2026).

Open Banking Limited. (n.d.). API performance stats. https://www.openbanking.org.uk/api-performance/ (Retrieved October 11, 2026).

ORUCHO D O, AWUOR F M, MAKIYA R, et al. (2023). Review of Algorithms for Securing Data Transmission in Mobile Banking. *Modern Economy, 14*, 1192-1217. DOI: 10.4236/me.2023.149062.

Salop, S. C., & Scheffman, D. T. (1983). Raising rivals' costs (Bureau of Economics Working Paper No. 81). Federal Trade Commission. https://www.ftc.gov/system/files/documents/reports/raising-rivals-costs/wp081.pdf (Retrieved October 11, 2026).

SHARMIN S, PRABHA M, JOHORA F T, et al. (2024). Open Banking and Information Service: A Strategic Relationship in the FinTech World. *Open Journal of Business and Management, 12*, 3743-3758. DOI: 10.4236/ojbm.2024.125186.

Standing Committee of the National People's Congress. (2021). Personal information protection law of the People's Republic of China. https://www.cac.gov.cn/2021-08/20/c_1631050028355286.htm (Retrieved

October 11, 2026).

Standing Committee of the National People's Congress. (2022). Anti-monopoly law of the People's Republic of China (Revised in 2022). https://www.samr.gov.cn/zw/zfxxgk/fdzdgknr/fgs/art/2023/art_f0fae9eb3a684fc39e84d89eabfc2caa.html (Retrieved October 11, 2026).

Supreme People's Court. (2024). Interpretation on several issues concerning the application of law in civil dispute cases involving monopoly (Legal Interpretation No. 6 of 2024). https://ipc.court.gov.cn/zh-cn/news/view-3112.html (Retrieved October 11, 2026).

WAWERU E, KARUME S M, KIBET A. (2025). A Review of Human Vulnerabilities in Cyber Security: Challenges and Solutions for Microfinance Institutions. *Journal of Information Security, 16*(1), 114-130. DOI: 10.4236/jis.2025.161006.

WILLIAMSON O E. (1979). Transaction-Cost Economics: The Governance of Contractual Relations. *Journal of Law and Economics, 22*(2), 233-261. DOI: 10.1086/466942.