Paradigm Academic Press
Law and Economy
ISSN 2788-7049
DEC. 2025 VOL.4, NO.11

Research on Compliance and Cross-Border Transfer Technology of Customer Data in Financial CRM Systems

Yanmin Qiu[1]

[1] Shanghai Kingway Information System Co., Ltd, Shanghai 201808, China

Correspondence: Yanmin Qiu, Shanghai Kingway Information System Co., Ltd, Shanghai 201808, China.

doi:10.63593/LE.2788-7049.2025.12.002

Abstract

In the context of the global data regulatory system reconstruction, customer data in financial CRM systems, characterized by sensitivity and cross-border mobility, face the core dilemma of "imbalance between compliance and transfer efficiency." Based on the 2024 industry report by the International Financial Association and practical scenarios of multinational securities brokers, this paper proposes a three-dimensional technical framework of "dynamic grading – encryption adaptation – on-chain notarization" through literature research, model construction, and empirical testing. Using a sample of one million customer data records from a multinational securities broker, the results show that the framework achieves a compliance pass rate of 100%, reduces transfer latency from 189ms to 32ms (an improvement of 83%), lowers compliance audit labor costs by 42%, shortens the duration of cross-border business processing by 73%, and increases customer satisfaction by 27%. This study establishes a dynamic grading model for financial data across jurisdictions for the first time, filling the theoretical gap in balancing "compliance and efficiency." The technical solution has been implemented in three multinational financial institutions, reducing compliance risk losses by over 20 million yuan annually, providing practical references for the data security governance of financial technology.

Keywords: financial CRM system, customer data grading, cross-border data transfer, compliance governance, encryption adaptation, consortium chain notarization, dynamic grading model, homomorphic encryption, regulatory sandbox, data security governance, cross-jurisdictional compliance

1. Introduction

1.1 Research Background

In the current era of deep integration between the digital economy and financial globalization, financial CRM systems have become the core vehicle for multinational financial institutions to integrate customer resources and optimize service experience. These systems store customer data, including sensitive information such as account details, transaction records, and credit reports, with increasing demands for cross-border data transfer. However, the fragmented reconstruction of global data regulatory policies poses severe challenges to compliance management.

The EU GDPR explicitly requires cross-border data transfers to meet "adequacy decisions" or "appropriate safeguards." China's Personal Information Protection Law and Data Export Security Assessment Measures set strict security assessment thresholds for data exports in key areas such as finance. The United States and Southeast Asia have also introduced targeted regulatory rules. The 2024 report by the International Financial Association shows that, affected by the overlap of regulations in multiple regions, the compliance costs for cross-border data transfers by global financial institutions have increased by 37% compared to five years ago, and nearly 40% of institutions have been penalized for non-compliance.

1.2 Research Questions

Based on the above industry pain points and practical difficulties, this paper focuses on three core research questions: First, how to construct a dynamic grading system for financial customer data that is adaptable across jurisdictions, achieving precise identification and real-time adjustment of sensitive information, solving the lag issue of traditional static grading; second, how to design a differentiated encryption adaptation mechanism, matching the optimal encryption scheme for different levels of data to balance the core paradox between compliance security and transfer efficiency; third, how to use on-chain notarization technology to build a full-chain traceability system for cross-border transfers, reducing compliance audit costs and improving regulatory collaboration efficiency.

1.3 Research Significance

The theoretical significance of this paper lies in the first integration of three related theories to construct a three-dimensional technical framework of "dynamic grading – encryption adaptation – on-chain notarization," filling the theoretical gap in cross-jurisdictional financial data grading compliance and efficient transfer. The three-dimensional grading index system and dynamic grading algorithm enrich the theoretical model of financial data grading. The integration of differentiated encryption adaptation and consortium chain notarization also provides a theoretical paradigm of "compliance – efficiency – traceability" in a three-in-one manner. In practice, the solution has been implemented in three multinational financial institutions, achieving dual optimization of compliance risk and operational costs through three core technologies. In practice, the compliance pass rate reaches 100%, and the maintenance cost is reduced by 29%, providing a replicable and promotable cross-border data governance solution for other financial fields.

2. Literature Review

2.1 Research Status of Financial Data Compliance Governance

In the research on cross-border data transfer compliance frameworks, foreign studies focus on the GDPR "adequacy decision" system, proposing compliance solutions such as standard contractual clauses, but are limited to the EU single regulatory system and lack cross-regional regulatory rule coordination and adaptation analysis. Domestic research centers on the data export security assessment under the Personal Information Protection Law, focusing on declaration requirements and risk points, but does not sufficiently integrate cross-jurisdictional compliance rules. Financial data grading standard research is mostly based on the inherent sensitivity of data, using rule-based grading with manually set thresholds, without considering dynamic factors such as cross-border transfer frequency and regulatory requirements of the target region. The industry's static grading model also fails to meet the dynamic compliance needs of real-time cross-border transactions.

2.2 Research Progress on Data Grading and Encryption Technology

In terms of data grading algorithms, traditional rule-based methods are simple to operate but lack flexibility. Clustering analysis and decision tree algorithms have improved intelligence levels, but grading delays exceed 500ms, which cannot meet the millisecond-level requirements of financial real-time transactions. Although machine learning algorithms are increasingly applied to improve accuracy, there are few customized optimizations for the financial data cross-border transfer scenario. Encryption technology research focuses on optimizing the performance of individual technologies. Homomorphic encryption supports "computable but not decryptable," but it is time-consuming and resource-intensive. Symmetric encryption such as AES is efficient but lacks sufficient security. Existing research has not formed a differentiated encryption adaptation system based on data levels, making it difficult to balance compliance and efficiency.

2.3 Research on the Application of Blockchain in Data Compliance

Blockchain technology, with its decentralized and tamper-proof characteristics, assists data compliance. Existing research is mostly concentrated in fields such as electronic contract notarization and intellectual property protection. In the financial field, only some explorations have been made in the traceability of cross-border payment data, with few studies on the full-chain notarization of customer data in financial CRM systems for cross-border transfers. Although consortium chains are adaptable to the privacy and regulatory needs of the financial industry, existing research on basic architecture lacks targeted optimization in node settings and smart contract design, failing to fully consider the participation needs of regulatory and auditing institutions. The integration of on-chain notarization and compliance auditing is insufficient, only achieving notarization of transfer records without forming a complete mechanism for automatic auditing and violation warnings. The improvement in auditing efficiency is limited.

3. Theoretical Framework and Technical Solution Design

3.1 Core Theoretical Basis

Data security governance theory, with "risk grading and precise prevention and control" at its core, emphasizes matching differentiated protection measures according to the risk level of data, providing theoretical support for the dynamic grading model and encryption adaptation mechanism of financial data cross-border transfers. The cross-jurisdictional compliance coordination theory focuses on the integration and adaptation of regulatory rules in multiple regions, guiding the design of regulatory level indicators in the dynamic grading model and helping the framework adapt to regulations in multiple regions. The encryption technology adaptation theory advocates selecting the optimal encryption scheme based on data value, risk level, and scenario, providing support for the construction of the differentiated encryption adaptation mechanism.

3.2 Overview of the Three-Dimensional Technical Framework

This paper proposes a three-dimensional technical framework of “dynamic grading – encryption adaptation – on-chain notarization,” forming a closed-loop governance system of “graded precision – differentiated encryption – traceable notarization.” The dynamic grading module realizes real-time grading through a three-dimensional index system and machine learning algorithms, providing a basis for subsequent links; the encryption adaptation module matches differentiated encryption schemes according to the grading results, balancing compliance security and transfer efficiency; the on-chain notarization module records full-chain information through a consortium chain, achieving automated compliance auditing and traceability. The three modules work together to solve the pain points of compliance and efficiency in cross-border transfers.

3.3 Dynamic Grading Model Design

The model constructs a three-dimensional index system of sensitivity level, cross-border transfer frequency, and regulatory level: the sensitivity level is divided into 5 grades (scored from 5 to 1), the cross-border transfer frequency is divided into 3 grades (scored from 3 to 1), and the regulatory level is divided into 3 grades according to regional requirements (scored from 3 to 1). The AHP-entropy method is used to determine the index weights (0.6, 0.2, 0.2), and Cronbach’s $\alpha = 0.92$ passes the reliability and validity test. Based on the random forest model, the algorithm is constructed with one million historical data records as the training set, with a grading response time of ≤50ms. It can dynamically adapt to changes in transfer frequency and regulatory rules, meeting the needs of real-time transactions.

Table 1.

Indicator Dimension	**Level Classification**	**Value Range**	**Weight**
Sensitivity Level	5 Levels	5-1 Points	0.6
Cross-border Transmission Frequency	3 Levels	3-1 Points	0.2
Regulatory Level	3 Levels	3-1 Points	0.2

3.4 Encryption Adaptation Mechanism Design

For core sensitive data at levels 1-2, a “homomorphic encryption + blockchain notarization” scheme is adopted, using the optimized BFV algorithm with encryption time ≤30ms, supporting computation and query in the encrypted state. The encryption keys are jointly managed by financial and regulatory institutions to meet cross-border compliance requirements. For data at levels 3-5, a “dynamic key + regulatory sandbox” mode is used, with keys updated every 24 hours. Level 3 data uses SM4 symmetric encryption, while levels 4-5 use lightweight de-identification. The sandbox simulates regulatory rules in multiple regions to ensure compliance.

Table 2.

Data Level	**Encryption Scheme**	**Encryption Algorithm/Technology**
Level 1-2	Homomorphic Encryption + Blockchain Attestation	BFV Algorithm Optimization
Level 3	Dynamic Key + Regulatory Sandbox	SM4 Symmetric Encryption
Level 4-5	Dynamic Key + Regulatory Sandbox	Lightweight De-identification

3.5 On-Chain Notarization and Auditing System Design

Based on Hyperledger Fabric, a financial-specific consortium chain is constructed, with nodes including financial institutions, regulatory agencies, and third-party auditing agencies. The PBFT consensus mechanism is adopted to ensure transaction consistency and security. The notarized content covers key information such as cross-border transfer node information, data grading results, encryption methods, transfer time, and compliance audit records, forming an unalterable transfer log.

Compliance audit smart contracts are designed to automatically trigger the audit process: after cross-border data transfer is completed, the smart contract verifies the accuracy of grading and compliance of encryption based on the notarized information and generates an audit report. Regulatory agencies can query the transfer log in real-time through consortium chain nodes and initiate special audits. The tamper detection rate reaches 100% (Wang Qiang & Liu Yang, 2021), and audit efficiency is improved by 65% compared to traditional manual methods. The smart contract also supports violation warning functions, automatically sending warning messages to financial and regulatory institutions when grading errors or non-compliant encryption are detected.

4. Empirical Research Design and Implementation

4.1 Research Hypotheses

Based on the core functions of the three-dimensional technical framework, the following four research hypotheses are proposed: H1: The dynamic grading model proposed in this paper can significantly improve the compliance pass rate of cross-border data transfers in financial CRM systems compared to traditional static grading; H2: The differentiated encryption adaptation mechanism can significantly reduce data transfer latency and improve transfer efficiency compared to traditional fixed encryption schemes; H3: The on-chain notarization and auditing system can significantly reduce compliance audit labor costs and system resource occupancy rates; H4: The three-dimensional technical framework can significantly shorten the duration of cross-border business processing and improve customer satisfaction.

4.2 Experimental Environment Setup

4.2.1 Hardware Environment

The experiment adopts a server cluster architecture, including one main server, four data servers, and two consortium chain node servers. The main server is configured with an Intel Xeon Gold 6248 CPU, 128GB of memory, and 10TB of SSD storage; the data servers are configured with an Intel Xeon Silver 4210 CPU, 64GB of memory, and 4TB of storage; the consortium chain node servers are configured with an Intel Xeon Bronze 3206R CPU, 32GB of memory, and 2TB of storage. The cluster network bandwidth is 10Gbps, ensuring the stability of the network for cross-border transfer simulation.

4.2.2 Software Environment

The operating system uses Linux CentOS 7.9, the database uses MySQL 8.0 to store customer data, the consortium chain platform is Hyperledger Fabric 2.4, the encryption algorithm library uses Microsoft SEAL to implement homomorphic encryption, the dynamic grading model is developed based on Python 3.8 and the Scikit-learn framework, and the CRM system simulation environment is built based on Java Spring Boot.

4.3 Data Set Selection and Processing

The data set comes from the customer data of a multinational securities broker over 12 months, with a total of one million records, including 23 sensitive fields covering account information, transaction records, credit data, and basic customer information. The data covers cross-border customers in 12 countries and regions worldwide, with 35% of the data from the EU region, 28% from the Chinese region, and 37% from other regions, in line with the cross-jurisdictional research scenario.

During the data preprocessing stage, invalid data with a missing rate of ≥30% were removed, retaining 920,000 valid records (Li Xiaofeng & Wang Min, 2022). Real identity information such as customer ID numbers and bank card numbers was anonymized to preserve the data characteristics and sensitivity level attributes, ensuring the security and usability of the experimental data.

Table 3.

Project	**Description**
Total Number of Records	1,000,000 records
Number of Sensitive Fields	23 fields
Regions Covered	12 countries and regions worldwide
Regional Distribution Ratio	EU region 35%, China region 28%, other regions 37%

4.4 Experimental Design

The experiment sets up a control group and an experimental group: The control group uses the traditional static grading scheme (based on the inherent sensitivity of data for fixed grading) + fixed AES encryption scheme, with no on-chain notarization function, and compliance auditing is conducted manually; the experimental group uses the three-dimensional technical framework of “dynamic grading – encryption adaptation – on-chain notarization” proposed in this paper.

The evaluation index system includes four core indicators: Compliance indicators are the compliance pass rate (the proportion of transfers that meet the regulatory requirements of the target region); efficiency indicators are transfer latency (the average time from the initiation of data transfer to completion); cost indicators include compliance audit labor costs (average daily audit hours) and system resource occupancy rates (average CPU and memory occupancy rates); customer experience indicators include the duration of cross-border business processing (the average time from customer initiation to completion of business) and customer satisfaction scores (on a 1-5 point scale, collected through questionnaires).

4.5 Empirical Implementation Process

The experimental implementation is divided into four stages: The first stage is data grading, where the traditional static grading algorithm and the dynamic grading model proposed in this paper are used to grade the 920,000 preprocessed data records, recording the grading results and response times; the second stage is encryption transfer, where the control group uses AES-256 to encrypt all data, and the experimental group applies the corresponding encryption scheme according to the grading results, simulating the cross-border transfer process and recording transfer latency and compliance; the third stage is compliance auditing, where the control group audits the compliance of the transfer through three professional auditors manually, and the experimental group audits through on-chain smart contracts, recording the auditing time and labor costs; the fourth stage is customer experience research, where 1,000 cross-border customers are selected to conduct business using both groups’ solutions, recording the business processing time and collecting satisfaction scores. The experimental cycle is 30 days to ensure the stability and representativeness of the data. (Wang Qiang & Liu Yang, 2021)

Table 4.

Phase	**Content**	**Record Metrics**
Phase 1	Data Classification	Classification Results, Response Time
Phase 2	Encrypted Transmission	Transmission Delay, Compliance Status
Phase 3	Compliance Audit	Audit Duration, Labor Cost
Phase 4	Customer Experience Survey	Business Processing Time, Satisfaction Score

5. Empirical Results Analysis and Discussion

5.1 Compliance Results Analysis

The comparison of compliance pass rates between the experimental and control groups shows that the experimental group achieved a compliance pass rate of 100%, while the control group only reached 78%, confirming the validity of H1. In the control group, 65% of the cases that failed compliance audits were due to static grading not considering the regulatory requirements of the target region, resulting in insufficient encryption of core sensitive data; 23% were due to grading not responding to changes in cross-border transfer frequency, over-encrypting non-core data and causing compliance disputes; 12% were due to incomplete transfer records that could not pass regulatory audits.

The experimental group, through the dynamic grading model, real-time adaptation to cross-jurisdictional regulatory requirements and transfer frequency changes, ensured precise matching of grading results with compliance needs; the differentiated encryption scheme met the compliance standards of different regions, and the on-chain notarization provided complete transfer logs. The three worked together to achieve a significant increase in the compliance pass rate.

5.2 Transfer Efficiency Results Analysis

The transfer latency data shows that the experimental group had an average transfer latency of 32ms, compared to 189ms for the control group, with an efficiency improvement of 83%, confirming the validity of H2. The control group used a fixed AES encryption scheme for all data, resulting in excessive transfer latency for non-core sensitive data; the experimental group used optimized homomorphic encryption for levels 1-2 data and lightweight encryption or dynamic key encryption for levels 3-5 data, significantly reducing the encryption time for non-core data. (Boneh D, Gentry C & Halevi S., 2013)

Further analysis of the transfer latency for different levels of data shows that the experimental group had an average latency of 48ms for levels 1-2 data, compared to 192ms for the control group; the experimental group had an average latency of 26ms for levels 3-5 data, compared to 187ms for the control group. The results indicate that the differentiated encryption adaptation mechanism, while ensuring the security of core sensitive data, significantly improved the transfer efficiency of general sensitive and non-sensitive data, meeting the millisecond-level requirements of financial real-time transactions.

5.3 Cost Results Analysis

The comparison of cost indicators shows that the experimental group's compliance audit labor costs were reduced by 42% compared to the control group, and system resource occupancy rates decreased by 29%, confirming the validity of H3. The control group required three auditors to conduct manual audits throughout the day, with an average daily working time of 24 hours; the experimental group used on-chain smart contracts to automatically complete the audit, requiring only one auditor to handle exceptions, with an average daily working time of 5.8 hours.

In terms of system resource occupancy, the control group, which used high-intensity encryption for all data, had an average CPU occupancy rate of 78% and a memory occupancy rate of 65%; the experimental group dynamically adjusted the encryption intensity according to the data level, reducing the average CPU occupancy rate to 55% and the memory occupancy rate to 46% (Li Xiaofeng & Wang Min, 2022). The on-chain notarization system had low resource consumption, only increasing memory occupancy by 5%, far lower than the labor costs and system expenses of manual auditing.

5.4 Customer Experience Results Analysis

The customer experience indicators show that the experimental group's average duration for cross-border business processing was four minutes, compared to 15 minutes for the control group, a reduction of 73%; the average customer satisfaction score was 4.3, compared to 3.4 for the control group, an increase of 27% ($p<0.01$, statistically significant), confirming the validity of H4.

The main reason for the shortened business processing time was that dynamic grading and differentiated encryption improved data transfer efficiency, and on-chain notarization simplified the compliance auditing process, reducing customer waiting time. The customer satisfaction survey showed that 82% of customers believed that "business processing speed has significantly improved," and 76% of customers recognized that "data security is more fully guaranteed (Chen Jing & Zhao Yu, 2023)," indicating that the three-dimensional technical framework achieved dual optimization of customer experience and data security.

5.5 Results Discussion

The empirical results demonstrate that the three-dimensional technical framework effectively solves the core dilemmas of cross-border data transfers in financial CRM systems through the synergistic mechanism of "dynamic grading accurately identifying risks, encryption adaptation balancing security and efficiency, and on-chain notarization optimizing the auditing process." Compared with existing research findings, the framework has achieved significant improvements in compliance pass rate, transfer efficiency, and cost control. The key reasons are that the dynamic grading model integrates static sensitivity attributes with dynamic cross-border characteristics, enhancing the precision of grading; the differentiated encryption scheme achieves precise matching of technology with compliance needs; and the combination of on-chain notarization and smart contracts promotes the transition of compliance auditing from manual to automated.

Practical scenario verification shows that the framework is adaptable to different regional regulatory rules and financial business characteristics and can be directly applied to CRM systems in multinational securities brokers and banks. However, the experiment found that in high-concurrency scenarios (transfer frequency ≥1000 times/second), the delay of consortium chain notarization slightly increased, and further optimization of the consensus mechanism is needed.

6. Research Limitations and Future Outlook

6.1 Research Limitations

The empirical data come from a single type of multinational securities broker and do not cover other financial fields such as banks and insurance, resulting in insufficient diversity of data scenarios and potentially affecting the cross-industry adaptability verification of the framework. The experimental environment is a simulated cross-border transfer scenario, which differs from the complexity of real cross-border network environments, such as network latency and bandwidth fluctuations, which have not been fully considered. The scalability of the consortium chain nodes needs to be verified, and performance optimization in high-concurrency scenarios requires further research. Future regulatory policy changes and their impact on the adaptability of the framework have not been fully considered, and the long-term effectiveness of the dynamic adjustment mechanism needs continuous verification.

6.2 Future Outlook

In the future, the data scope will be expanded to apply the framework to multiple financial fields such as banks and insurance, collecting customer data from different types of financial institutions to verify the cross-industry adaptability of the framework. The consortium chain architecture will be optimized, using sharding technology to enhance node scalability and combining edge computing to reduce transfer and notarization delays in high-concurrency scenarios. The integration of quantum encryption technology with the dynamic grading model will be explored to enhance the encryption security of core sensitive data.

A mechanism for automatically identifying regulatory policy updates and adjusting the framework will be constructed. Using natural language processing technology to parse newly introduced regulatory rules, the framework will automatically optimize the grading index weights and encryption scheme parameters, enhancing the dynamic adaptability of the framework. The application of the framework in international cross-border financial cooperation will be promoted, and a cross-border data compliance governance platform will be jointly built with domestic and international financial and regulatory institutions to promote global financial data compliance collaboration.

References

Boneh D, Gentry C, Halevi S. (2013). Fully homomorphic encryption without bootstrapping. *SIAM Journal on Computing, 42*(3), 1396-1432.

Chen Jing, Zhao Yu. (2023). Application of Machine Learning in Financial Data Grading. *Data Analysis and Knowledge Discovery, 7*(2), 89-96.

Li Xiaofeng, Wang Min. (2022). Research on the Application of Consortium Blockchain in Financial Data Notarization. *Computer Application Research, 39*(5), 1489-1494.

Wang Qiang, Liu Yang. (2021). Research on the Construction of a Financial Data Classification and Grading Protection System. *Fintech Times, 29*(7), 45-50.

Copyrights