

**INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

JR/T 0199-2020

**General Specification for Fintech Innovation and Security
(English Translation)**

Issued on: October 21, 2020

Implemented on: October 21, 2020

Issued by: People's Bank of China

Table of Contents

- 1 Scope
- 2 Normative references
- 3 Terms and definitions
- 4 Abbreviations
- 5 Transaction security
 - 5.1 Transaction verification
 - 5.2 Transaction confirmation
 - 5.3 Transaction monitoring

1 Scope

This document specifies the basic security requirements for financial technology innovation, including transaction security, service quality, business continuity, algorithm security, Architecture security, data security, network security, internal control management, etc.

This document applies to licensed financial institutions engaged in financial service innovation, as well as related business systems, computing power storage, and algorithm models.

Technology companies and safety assessment agencies that develop scientific and technological products.

2 Normative references

The contents of the following documents constitute the indispensable clauses of this document through normative references in the text. Among them, dated reference documents, Only the version corresponding to that date is applicable to this document; for undated references, the latest version (including all amendments) is applicable to this document file.

GB/T 20988 Information Security Technology Information System Disaster Recovery Specification GB/T 22240 Information Security Technology Network Security Grade Protection Classification Guide JR/T 0044 Banking Industry Information System Disaster Recovery Management Specification JR/T 0071 Implementation Guidelines for Information Security Level Protection of Information Systems in the Financial Industry JR/T 0118-2015 Financial Electronics Certification Specification JR/T 0166 Cloud Computing Technology Financial Application Specification Technical Architecture JR/T 0167 Cloud Computing Technology Financial Application Specification Security Technical Requirements JR/T 0168

Cloud Computing Technology Financial Application Specification Disaster Recovery JR/T
0171-2020 Personal Financial Information Protection Technical Specification JR/T
0193-2020 Blockchain Technology Finance Application Evaluation Rules

3 Terms and definitions

The following terms and definitions apply to this document.

Fintech innovation

Under the premise of complying with the requirements of current laws and regulations, departmental rules, and regulatory documents, in areas that do not yet have management rules, use new Technical design, products or services for financial users.

Fintech innovation institution Licensed financial institutions engaged in financial service innovation and science and technology products research and development such as related business systems, computing power storage, algorithm models, etc.

Technology company.

Personal financial information Personal information acquired, processed, and stored by financial technology innovation institutions through the provision of financial services or technological products.

Note 1: Personal financial information in this document includes account information, identification information, financial transaction information, personal identification information, property information, loan information, and Other information that reflects certain circumstances of specific individuals.

Note 2: Rewrite JR/T 0171-2020, definition 3.2.

Business continuity

After an interruption event occurs, the organization's ability to continuously deliver products or provide services at a predetermined acceptable level.

4 Abbreviations

The following abbreviations apply to this document.

API. Application Programming Interface (Application Programming Interface) APP. Client Application Software (Application Software) DDoS. Distributed Denial of Service (Distributed Denial of Service) IP. Internet Protocol (Internet Protocol) LQA. Lowest Quality Acceptable QoS. Quality of Service (Quality of Service) RPO. Recovery Point Objective RTO. Recovery Time Objective SDK. Software Development Kit (Software Development Kit) UPS. Uninterruptible Power System Web. World Wide Web

5.1 Transaction verification

a) Transaction verification can combine the following 3 types of elements.

- Elements that are only known to the customer;
- Elements that are only held by the customer and unique, and cannot be copied or reused;
- The biological characteristics of the customer.

b) The use of transaction verification elements shall meet the following requirements.

--Should ensure that the elements used are independent of each other, that is, damage or leakage of some elements should not cause damage or leakage of other elements dew;

--Strictly restrict the use of initial transaction passwords and prompt customers to modify them in time, establish a transaction password complexity verification mechanism, and avoid the transaction-free password is too simple (such as "111111", "123456", etc.) or is related to personal financial information (such as date of birth, ID number, mobile phone number, etc.) are too similar;

--Where digital certificates and electronic signatures are used as authentication elements, the digital certificates and the process of generating electronic signatures shall comply with the relevant Laws and regulations, JR/T 0118-2015 and other relevant regulations to ensure the uniqueness, integrity and resistance of transactions Dependent - If a one-time password is used as a verification element, the one-time password acquisition end and the transaction instruction initiation end should be prevented from being the same the risks caused by the same physical equipment, and the one-time password validity period is strictly limited to the shortest necessary time;

- If the customer's biometrics is used as the verification element, it shall comply with national and financial industry standards and relevant information security management Management requirements to prevent illegal storage, copying or replay;

--Technical measures that match the transaction verification strength and the transaction amount should be taken to improve the security of the transaction;

--Should go through customer confirmation and transaction verification. Transaction verification should use two of the above three types of elements at the same time.

The corresponding risk compensation measures shall be taken for those in the second category.

5.2 Transaction confirmation

Transaction confirmation should meet the following requirements.

a) Effective measures should be taken to ensure that customers can confirm transaction

information such as transaction content and transaction amount before executing transaction instructions, and after the transaction instruction is completed, the transaction information will be displayed or the customer will be notified of the result in time.

b) The authenticity, completeness, traceability and consistency of the transaction information shall be ensured, and shall not be tampered with or hidden Hidden transaction information.

c) Reliable technical means such as static passwords, dynamic passwords, digital certificates, etc. should be used to realize the self-confirmation to ensure the user's knowledge Rights, property security rights and other legal rights.

5.3.1 Establishment of transaction monitoring system

Fintech innovation institutions should establish an effective transaction monitoring system to meet the following requirements.

a) A transaction monitoring system should be established to identify and warn transactions with potential risks, and generate risk monitoring reports.

b) A risk transaction model should be established according to the risk characteristics of the transaction, suspicious transactions should be effectively monitored, and reports, review, and review of suspicious transactions should be established.

Check mechanism.

c) Big data analysis, customer behavior modeling and other means should be used to establish transaction risk monitoring models and systems, and conduct monitoring of abnormal transactions.

Early warning, and take measures such as investigation and verification, risk warning, and delayed settlement.

d) The risk assessment model should be continuously optimized through transaction behavior analysis, machine learning, etc., to increase the success rate of fraudulent transaction interception, and reduce errors.

Judgment rate, and effectively improve transaction security protection capabilities.

5.3.2 Transaction risk identification

Fintech innovation institutions should support the knowledge of fraud risks and compliance risks...