

ICS 35.240.40
CCS A 11

JR

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

JR/T 0171-2020

**Personal financial information protection technical
specification
(English Translation)**

Issued on: February 13, 2020

Implemented on: February 13, 2020

Issued by: People's Bank of China

Table of Contents

Foreword	
Introduction	
1 Scope	
2 Normative references	
3 Terms and definitions	
4 Overview of personal financial information	
5 Basic Safety Principles	
6 Safety technical requirements	
7 Safety management requirements	
Appendix A (informative appendix) Information shielding	
References	

Foreword

This standard was drafted in accordance with the rules given in GB/T 1.1-2009.

This standard was proposed by the People's Bank of China.

This standard is under the jurisdiction of the National Financial Standardization Technical Committee (SAC/TC 180).

Drafting organizations of this standard. Department of Science and Technology of the People's Bank of China, Zhengzhou Central Branch of the People's Bank of China, Beijing UnionPay Gold Card Technology Co., Ltd Bank of China Co., Ltd., China UnionPay Co., Ltd., Net Union Clearing Co., Ltd., Zhejiang Ant Small and Micro Financial Services Group Co., Ltd., Lakala Payment Co., Ltd., China Financial Electronics Corporation, Wuhan Branch of the People's Bank of China, Industrial and Commercial Bank of China Co., Ltd., Agricultural Bank of China Co., Ltd., China Construction Bank Co., Ltd., Ping An Insurance (Group) of China Co., Ltd., Beijing CICC Guosheng Certification Co., Ltd., Beijing Software Product Quality Testing and Inspection Center, CICC Financial Certification Center Co., Ltd., Information Industry Information Security Evaluation Center, Huatai Securities Co., Ltd., People's Insurance Group of China Co., Ltd., Tenpay Payment Section Technology Co., Ltd., China Payment and Clearing Association, China Internet Finance Association, CCB Financial Technology Co., Ltd.

Introduction

Personal financial information refers to personal information in the financial field around account information, identification information, financial transaction information, personal identity information, financial the expansion and refinement of property information, lending information, etc. is an important foundation accumulated by financial institutions in the process of providing financial products and services Data is also an important part of personal privacy. Once personal financial information is leaked, it will not only directly infringe the legal rights of the subject of personal financial information Benefit, affect the normal operation of financial institutions, and may even bring systemic financial risks. In order to strengthen personal financial information security management, Guide all relevant institutions to regulate the handling of personal financial information, protect the legal rights and interests of personal financial information subjects to the greatest extent, and maintain the stability of the financial market.

Prepare this standard.

Technical specifications for personal financial information protection

1 Scope

This standard specifies the security protection of personal financial information in all aspects of the life cycle such as collection, transmission, storage, use, deletion, and destruction.

Requirements, from two aspects of security technology and security management, put forward normative requirements for the protection of personal financial information.

This standard applies to financial institutions that provide financial products and services, and provides security assessment agencies for security inspection and assessment work. reference.

2 Normative references

The following documents are indispensable for the application of this document. For dated reference documents, only the dated version applies to this document.

For undated references, the latest version (including all amendments) applies to this document.

GB/T 22239-2019 Information Security Technology Network Security Level Protection Basic Requirements GB/T 25069-2010 Information Security Technical Terms GB/T 31186.2-2014 Bank Customer Basic Information Description Specification Part 2: Name GB/T 31186.3-2014 Bank Customer Basic Information Description Specification Part 3: Identification Mark GB/T 35273-2017 Information Security Technology Personal Information

Security Specification JR/T 0068-2020 Internet Banking System Information Security
General Specification JR/T 0071 Implementation Guidelines for Information Security Level
Protection of Information Systems in the Financial Industry JR/T 0092-2019 Mobile
Financial Client Application Software Security Management Specification JR/T 0149-2016
China Financial Mobile Payment Tokenization Technical Specification JR/T 0167-2018
Cloud Computing Technology Financial Application Specification Security Technical
Requirements

3 Terms and definitions

The following terms and definitions defined in GB/T 25069-2010 and GB/T 35273-2017 apply to this document.

Financial industry institutions Financial institutions in this standard refer to licensed financial institutions supervised and managed by the national financial management department, and those involving personal financial information Relevant institutions for processing.

Personal financial information Personal information obtained, processed and stored by financial institutions through the provision of financial products and services or other channels.

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

Note 2: Rewrite GB/T 35273-2017, definition 3.1.

Payment sensitive information the payment information involves important information about the privacy and identification of the payment subject.

Note: Payment sensitive information includes but is not limited to bank card track data or chip equivalent information, card verification code, card validity period, bank card password, network payment Personal financial information used for payment authentication, such as payment transaction password.

Personal financial information subject the natural person identified by personal financial information.

Note: Rewrite GB/T 35273-2017, definition 3.3.

Personal financial information controller an organization that has the power to determine the purpose and method of processing personal financial information.

Note: Rewrite GB/T 35273-2017, definition 3.4.

Collect

The act of obtaining control over personal financial information.

Note 1: Collection behaviors include active provision by personal financial information subjects, through interaction with personal financial information subjects or recording of personal financial information subjects' behavior, etc.

Automatic collection, and indirect acquisition of personal financial information through sharing, transfer, and collection of public information.

Note 2: If a financial product or service provider provides tools for personal financial information subjects to use, and the provider does not access personal financial information, it is not Collected in this standard. For example, after the mobile banking client application software obtains the user's fingerprint feature information for local authentication, the fingerprint If the information is not returned to the provider, it does not belong to the collection of user fingerprint information.

Note 3: Rewrite GB/T 35273-2017, definition 3.5.

Public disclosure

The act of publishing information to society or unspecified groups.

[GB/T 35273-2017, definition 3.10] 3.8 Transfer of control the process of transferring control of personal financial information from one controller to another.

Note: Rewrite GB/T 35273-2017, definition 3.11.

Sharing

The personal financial information controller provides personal financial information to other controllers, and both parties have independent control over personal financial information the process of.

Note: Rewrite GB/T 35273-2017, definition 3.12.

3.10

Personal financial information security impact assessment in response to personal financial information processing activities, the degree of legal compliance is checked, and it is judged that it causes damage to the legal rights and interests of personal financial information subjects the various risks and the process of evaluating the effectiveness of various measures used to protect personal financial information subjects.

Note: Rewrite GB/T 35273-2017, definition 3.8.

3.11

Payment account

Bank accounts with financial transaction functions, payment accounts of non-bank payment institutions, and bank card numbers.

Note: Rewrite JR/T 0149-2016, definition 3.1.