DOI 10.15302/J-SSCAE-2020.06.013

Financial Retail Payment Risk Control: Current Status, Challenges, and Countermeasures

Zhou Hao [1, 2], Chai Hongfeng [1, 2, 3]

1. Institute of Cyberspace Security Science and Technology, Shanghai Jiao Tong University, Shanghai 200240, China
2. China UnionPay Co., Ltd., Shanghai 200135, China; 3. National Engineering Laboratory of Electronic Commerce and Electronic Payment, Shanghai 201201, China

Abstract: The development of financial openness, inclusive finance, and financial technologies in China is transforming and upgrading the country's financial retail payment industry from high-speed to high-quality growth; consequently, the current financial retail payment risks present a more complex and severe situation. The COVID-19 epidemic has changed people's consumption and payment habits, and has raised new topics on the risk control of financial retail payment. This study explores the necessity for risk control in China's financial retail payment industry by analyzing the new characteristics of financial retail payment and the deficiencies in risk control. It then summarizes the current status of risk control and the major challenges from seven perspectives: compliance performance, account management, transaction monitoring, credit evaluation, data security, identity verification, and technical risks. We conclude that the establishment and improvement of a comprehensive risk management system and an intelligent risk control system that match the complex and severe situation are key to risk control in the industry. Furthermore, we propose several countermeasures relative to five specific aspects: data sharing, intelligent model, system design, management system, and talent training.

Keywords: financial retail payment; payment risks; risk control; financial crime; financial intelligence

1 Introduction

As a basic arrangement of the financial system, the financial retail payment system pervades the entire process of financial activities. It has a special position and role in the financial system, and provides an infrastructure that supports economic operation and social development [1]. The People's Bank of China *Overall Operation of Payment System in 2019* reports a national payment system that is operating smoothly, with continual expansion of the scale of social fund transactions and a steady growth in the payment business volume. The financial retail payment business has wider coverage, and represents a large proportion of the transactions in the financial system. At the end of 2019, the per capita number of bank accounts in China reached 8.09, while the per capita number of bank cards held was 6.03. The payment system processed a total of $5.685×10^{11}$ payment transactions, while the interbank payment system and the online clearing platform that mainly deals with retail payments accounted for 93.7% of the a total number of transactions.

With the rapid development of financial technology, the financial retail payment industry has deepened its transformation, ushering in a new industrial pattern, development model, and technological realization [2]. In terms of the industrial structure, industry participants (parties that assume specific roles) are increasingly diversified; for

Received date: September 10, 2020; **Revised date:** October 28, 2020

Corresponding author: Zhou Hao, Phd student and senior engineer of Institute of Cyberspace Security Science and Technology of Shanghai Jiao Tong University. Major research fields include financial security and risk control technology. E-mail: zhouhao@unionpay.com

Funding program: CAE Advisory Project "Strategic Research on Cyberspace Security Assurance" (2017-XY-45)

Chinese version: Strategic Study of CAE 2020, 22 (6): 103–110

Cited item: Zhou Hao et al. Financial Retail Payment Risk Control: Current Status, Challenges, and Countermeasures. *Strategic Study of CAE*, https://doi.org/10.15302/J-SSCAE-2020.06.013

example, regarding mobile payment, new mobile device manufacturers, application program (APP) service providers, aggregate payment service providers, and payment technology service providers have been added. Regarding development models, commercial banks strengthen the development of mobile apps and open banking, deepen cooperation with Internet traffic application service providers, and expand the payment system in consumer finance and other retail businesses; non-bank payment institutions rely on payment channels to provide additional comprehensive services. Merchant service providers plan to gradually expand the overseas payment market. In terms of technical implementation, payment methods include magnetic stripe cards, chip cards, and QR codes, while payment terminals can be traditional point-of-sale (POS) terminals, wireless terminals, or mobile POS. Communication methods range from dedicated lines, through the Internet, to the Internet of Things. Methods for identity authentication include transaction passwords, SMS verification codes, fingerprints, faces, and other biological characteristics, while platform architecture may be centralized, distributed, or blockchain.

Against the background of the rapidly growing financial retail payment business, profound changes in business formats, and severe risk situations, there is an urgent to explore ideas and measures to ensure a sound development of the country's financial retail payment business. This study analyzes the risk control needs of the financial retail payment system, including the system's characteristics and the difficulties it faces; the study establishes the status of development of risk control in the financial retail payment system, focusing on compliance performance, account management, transaction monitoring, credit evaluation, data security, identity verification, and technical risks. Finally, safeguard measures are proposed.

2 Financial retail payment risk control needs

Financial retail payment risks have always been accompanied by innovation and development; the two are intertwined, and currently face five new developments: (1) new participants. In addition to traditional commercial banks, there now exist payment clearing organizations, non-bank payment institutions, mobile phone terminal manufacturers, Internet giants, financial technology start-up companies, etc. These new participants may introduce new risks; (2) new business forms. Payment business scenarios gradually evolve from in-store payment to payment at any time, while payment is no longer a single activity, constantly penetrating, and being integrated into, other financial scenarios, such as credit, wealth management, insurance, and leasing. Additionally, risks have spread, and continue to spread, from a single business link to entire chains; (3) new cybercriminals [3,4]. While artificial intelligence (AI) technology is widely used in technological innovation, it is also used by cybercriminals. Criminal methods tend to evolve in groups, specialization, intelligence, and internationalization; (4) new crimes are driven by interests, cross-border gambling, telecommunications network fraud, the use of the dark web and bitcoin money laundering, and other illegal activities that have repeatedly been prohibited. The shift from offline to online activities continues to attract high-level attention at the national level, while a multi-sectoral joint crackdown on cross-border gambling has been implemented to punish the platform institutions that provide funds for payment and settlement in contravention of the law; (5) the new focus of contradiction. The issuance of the *Network Security Law of the People's Republic of China* and the public consultation on the *Personal Information Protection Law of the People's Republic of China (Draft)* make the balance between personal information protection and data intelligent use a new focus of contradiction, which is conducive to promoting the research and application of user privacy protection technology.

Given the profound changes and severe situation in the financial retail payment industry, there remain four shortcomings in payment risk control: (1) The perceptions of risk have not kept up with the trend in the rapid evolution of risk. Credit risks continue to rise, fraud risks continue to be renovated, compliance risks are becoming more severe, while liquidity risks are beginning to emerge. Payment service entities (i.e., payment and clearing organizations, commercial banks, and non-profit organizations) hold inconsistent perceptions of the aforementioned risk hazards, while the ability of their control systems to deal with the risks vary considerably. (2) The application of data has not yet adequately addressed the shortcomings of the risk control system. Relevant cases [5] show that criminals target the flaws in both the mechanism and the model of the risk control system for their fraudulent or criminal activities. However, the linked data are not fully authorized, effectively collected, processed, and cleaned, while they not cross-analyzed, which makes it difficult to detect early warning signals before or during an illegal event, or to respond effectively and timeously to such an event following its occurrence. (3) AI has not yet been fully adapted to the interpretability requirements of intelligent risk control. The application of intelligent algorithms, such as neural networks in medical [6], transportation [7], agriculture, and other fields, is gradually being commercialized; however, the development of an AI-based risk control model system still requires improvement and verification,

DOI 10.15302/J-SSCAE-2020.06.013

especially the challenges relating to the interpretability of algorithms, personal privacy protection, fair modeling, etc. (4) The management mechanism does not fully satisfy the requirements of the governance system, while the establishment of a comprehensive risk management system is necessary to modernize financial corporate governance. The important link of the company itself will inevitably require strengthening the risk awareness of all employees within the enterprise and establishing risk professional sections; the organizational structure of the internal risk management function in different institutions needs to be strengthened, and the risk control concept changed.

Presently, risk control in the financial retail payment field is becoming increasingly critical, and has become a strategy to ensure the development of a high-quality payment industry. Such development must begin, urgently, with such aspects as data sharing and coordination, intelligent model upgrade [8,9], system intensification and unification, comprehensive risk management, and cross-personnel training; thus, the process of building a comprehensive ability to effectively and timeously respond to the changing risk situation can be fast-tracked.

3 The development status of risk control in the financial retail payment industry

With the continuous promotion of user demand and the support of financial technology, the financial retail payment industry chain has continued to expand and develop innovatively. Regulators, service entities, and relevant participants in the chain (Fig. 1) pay increasing attention to the value and significance of risk control: regulatory authorities have implemented multiple measures to prevent high risks in the payment field, while payment and clearing organizations have steadily promoted risk clearance and focused on improving the level of risk control services. Meanwhile, commercial banks have explored the application of big data and AI technology in entity-wide risk monitoring. Non-bank payment institutions, in accordance with regulatory requirements, centrally deposit and manage customer reserve funds, while financial technology companies provide intelligent risk control services and products, including intelligent perception, intelligent analysis, intelligent decision-making, and intelligent disposal. In addition, payment service entities focus increasing attention on the protection of personal information, while the payment tokenization technical specifications issued by the International Chip Card Standardization Organization [10] have achieved good application effects in China.

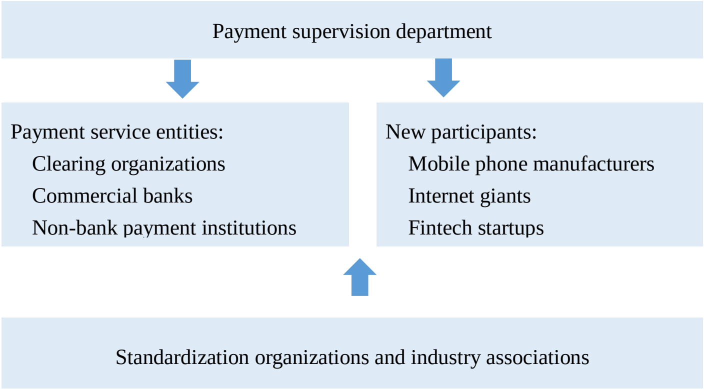
Payment supervision department
Payment service entities:
Clearing organizations
Commercial banks
Non-bank payment institutions
New participants:
Mobile phone manufacturers
Internet giants
Fintech startups
Standardization organizations and industry associations

Fig. 1. Main participants in the financial retail payment industry.

3.1 Regulatory authorities continue to strengthen the regulations for payment risk control

In the past five years, the People's Bank of China and the China Banking and Insurance Regulatory Commission have increased the regulations (and related penalties) pertaining to the prevention and resolution of financial risks; these regulations are targeted at illegal commercial banks, non-bank payment institutions, and related practitioners to ensure compliance with the law, curb the high risks in the industry, and maintain financial market order.

From 2015 to 2019, the People's Bank of China proposed the core principles of grasping supervision and innovation, balancing safety and efficiency, matching openness and supervision, strict supervision and normalization, and strict control of various cross-risks at the China Payment and Settlement Forum; during this time, the bank pointed out that non-bank payment institutions were different from general industrial and commercial enterprises; therefore, the bank proposed, these non-bank payment institutions must strengthen risk control and risk awareness. Meanwhile, an effective risk management mechanism should be established to promote the development of industry risk information management systems; established measures should be adopted to digest existing risks and the monitoring of incremental risks should be strengthened, to take precautions in advance, handle the risks between the different entities, and focus on systemic risk prevention. In the areas of telecommunications network fraud, cross-border gambling, the black and gray network industry, and account risk monitoring, a blacklist system must be established to continue to improve the level of risk monitoring.

3.2 The payment and settlement organizations steadily promoted risk clearance and improved risk control service levels

As the hub for the processing of bank card clearing business, China UnionPay Co., Ltd., together with all the industry parties, actively carried out the prevention of Categories II and III account risks, the monitoring of reserve fund risks, the fight against telecommunications network fraud and cross-border gambling, payment risk security inspections, account information security management, and other risk rectification work. The company cooperated with the People's Bank of China and the public security department to research and solve the problems of "one person with multiple cards" and self-service teller (ATM) biometrics [2].

Faced with the high risks of the industry, China UnionPay Co., Ltd. promptly carried out institutional interviews, high-risk merchant responsibility transfers, and other restraint disposal work, and worked with all the parties in the industry to appropriately deal with electronic e-toll collection (ETC) fraud, overseas centralized fraud, and cross-border fraud. Through real-time monitoring, cargo interception, and delayed fund settlement mechanisms for risk events such as border movement, a total of approximately CNY 830 million in losses was avoided (or recovered) for institutions and cardholders in 2019. China UnionPay Co., Ltd. relies on the China UnionPay Risk Management Committee, Bank Card Security Cooperation Committee, Internet Payment Security Alliance, and other basic platforms and mechanisms to strengthen communication, deepen industrial cooperation, strengthen joint prevention and control, and protect the legitimate rights and interests of cardholders. The company continuously upgrades its intelligent risk control capabilities and builds an integrated intelligent risk control system architecture, machine learning modeling platform, and a legal and compliant data sharing mechanism across units, fields, and lines in the payment industry. It promotes a three-level risk control product system covering basic risk control, a standard risk control application program interface output, and customized solutions. As of the third quarter of 2020, it has provided more than 130 financial and non-bank payment institutions with related services.

As a payment and clearing organization that processes online payment services between non-bank payment institutions and banks, NetsUnion Clearing Co., Ltd. continues to provide timely and accurate information for the regulatory authorities. The information is used to monitor risks through measures such as institutional and capital change monitoring, to realize timely investigation and disposal of potential risks. In response to risk scenarios such as illegal misappropriation of funds and high-risk personal-to-person (P2P) transactions, a mechanism for monitoring and analyzing market entities' capital changes and information linkage synchronization has been established. Furthermore, based on intelligent learning technology, a monitoring model for suspected gambling transactions and other violations has been established [11].

Other overseas payment organizations, e.g., Visa and MasterCard, are also establishing and improving risk control mechanisms based on big data. Visa, for example, provides risk control services for banks and other financial institutions to improve transaction security and processing efficiency by identifying transaction subjects and the risk of transaction fraud. Specifically, it provides services such as bank card transaction authorization management, fraud detection, user identity verification solutions based on biometrics, and personal credit evaluation predicting overdue risks, based on card issuing banks' authorized transaction data.

3.3 Commercial banks improve the level of the refined management of payment risks

Different types of commercial banks have increased their risk control investment in technology and business according to their own business development needs, especially in the retail and inclusive business sectors, and have prioritized payment risk control.

State-owned banks have established a bank-wide risk control system. For example, the Industrial and Commercial Bank of China (ICBC) has built a "risk + intelligence" smart risk control system, deployed more than 200 real-time calculation and quasi-real-time calculation models, and has cumulatively warned and blocked more than 2×10^7 million credit cards , debit cards, and electronic banking fraudulent transactions, effectively curbing various fraudulent behaviors [12]. Joint-stock banks have established a full-process risk management system; for instance, China Merchants Bank has built an intelligent big data anti-fraud platform, comprehensively using mobile device fingerprints, optical character recognition, face comparison, electronic contract comparison, and other technical

DOI 10.15302/J-SSCAE-2020.06.013

means to significantly improve the risk management level and operational efficiency [13]. Urban commercial banks, rural commercial banks, rural cooperative banks, rural banks, rural credit cooperatives, and foreign banks in various regions have established corresponding risk control systems and measures in their anti-fraud system for high-risk areas [14].

3.4 Frequent exposure of non-bank payment institution risks

With the rapid development of the Internet economy, many new business models have been built for non-bank payment, which have brought about not only opportunities, but also risk problems related to external regulations, reserve management, human operation, cybercrime, finance, and liquidity [15].

The *Measures for the Deposit of Reserve Funds for Customers of Non-bank Payment Institutions (Draft for Comment)* clearly impose penalties on misappropriation of reserves in accordance with the *People's Bank of China Law of the People's Republic of China*. In June 2020, the parent company of a non-bank payment institution issued an announcement that a company that had a business relationship with the non-bank payment institution had misappropriated its reserve account funds equaling CNY 1.495 billion; its payment license may be revoked. In July 2020, the Shanghai Municipal People's Procuratorate disclosed a theft case in which hacker technology was used to intrude into the computer system of a non-bank payment institution. From April to June 2018, criminals took advantage of the loopholes in the recharge system between a Shanghai wealth management platform and a P2P company; they used fabricated methods to inflate the small actual recharge into an enormous amount, and then transferred a large amount—hundreds of millions of dollars—from the reserve account to the P2P account, which they then illegally controlled. In April 2020, a document digital certificate of a non-bank payment institution was attacked by hackers. After inspection, the hacker used the stolen document certificate to forge payment instructions, and paid hundreds of millions of dollars to multiple accounts controlled by criminals in a short period of time.

3.5 Payment risk control service providers offer professional risk control capabilities

Under the dual influence of increasing supervision and accelerating changes in payment formats, the ability to resist risks can support enterprises to improve quality, increase efficiency, and reduce costs, which has become the direction recognized and committed to by all participants in the industry. Commercial banks and non-bank payment institutions realize that their own risk data and risk models are insufficient, while payment risk control service providers have emerged and developed accordingly.

While overseas payment organizations, such as Visa and MasterCard, perform payment and clearing duties, they also provide payment security services to member institutions by analyzing suspicious transactions and abnormal information in the transaction network under the framework of the risk and responsibility sharing system. Large-scale Internet companies use one billion users' data as the cornerstone to output the AI models and technical capabilities of the profile analysis that they have developed and nurtured. Intelligent analysis and decision-making vendors rely on innovative technology capabilities and financial service experience to help customers deploy localized risk control systems and models. China UnionPay Co., Ltd. refers to Visa's and MasterCard's payment security service models, and combines the needs of the country's payment risk control service market to provide differentiated levels and categories of risk services to customer groups.

4 Challenges facing financial retail payment risk control

4.1 Compliance performance

The People's Bank of China and the China Banking and Insurance Regulatory Commission focus on comprehensive risk management, and continue to increase their joint efforts with public security departments to combat criminal activities. They use modern technology to strengthen the compliance risk monitoring of the payment market, carry out law enforcement inspections, and increase penalties. Consequent on the abovementioned strict requirements, some payment service entities experience problems, such as imperfect institutional systems, unsound risk control systems, and inadequate risk operations. One example relates to the credit card pre-loan approval system: after the Shanghai Banking and Insurance Regulatory Bureau proposed the requirement for rigid deduction in 2014, some commercial banks simply pursued business development goals without approval, as required, and excessively granted credit to customers whose income did not meet the requirements: they suffered administrative punishment in July 2019. The *Interim Measures for the Administration of Internet Loans of Commercial Banks*, issued in July

2020, also requires that the Internet loan business be included in a comprehensive risk management system to ensure that the development of the business is compatible with its own risk appetite and risk management capabilities.

4.2 Account management

In the processes of cross-border gambling, telecommunications network fraud, and malicious arbitrage of marketing funds, criminals take advantage of the management flaws and technical loopholes in individual bank accounts to apply for these accounts in a centralized manner, or to purchase and use them for fund transfer. With respect to the criminal account and capital chains, criminals also use individual banks' technical flaws in the remote opening verification of Types II and III bank accounts and corporate bank accounts to conduct verification and account opening in batches to carry out criminal activities remotely.

4.3 Transaction monitoring

Criminal gangs use stolen payment account information and SMS verification codes to maliciously steal and scan in high-risk countries and merchants overseas. With the development of mobile payment, the criminal gangs attempt to make false applications (that is, combine payment accounts in mobile APPs) after stealing information, and then maliciously steal from such accounts. Moreover, criminal methods change constantly, and tend to be concealed, posing challenges to traditional rules-based methods of interception or early warning. In addition to using risk big data to analyze user behavior [16] and establish risk monitoring methods that cover the entire process of mobile payment transactions [17], there is also an urgent need to improve the monitoring capabilities of risk situation awareness and real-time quantitative decision-making, and to extend them from the prevention of criminal individuals to include that of criminal gangs.

4.4 Credit assessment

Due to the cross-effects of the macroeconomic downturn and the global novel coronavirus pneumonia epidemic, the amount and ratio of non-performing loans in bank retail credit and credit card businesses have continued to rise, while the credit risk problems in some small- and medium-sized financial institutions have become more severe. With the rectification and clean-up of Internet financial loan platforms, the low repayment ability of low-income, high-shared debt customer groups has become an input risk point for banks' credit business. Therefore, banks urgently need to strengthen the identification, differentiation, and management of common debt groups. Some banks have launched remote Internet loans; however, they have not yet established a matching risk management system, especially with regard to effective management in terms of risk models and manual reviews.

4.5 Data Security

Data security involves the challenges brought about by the disclosure of payment information, as well as those brought about by the protection of user privacy in smart models. The method of payment information leakage has changed from the original installation of a measuring and recording device at an ATM to obtain a small amount of single-point information, through hackers attacking merchants or non-bank payment institutions with system vulnerabilities to obtain bulk multi-point information, to attacking mobile apps to obtain a full set of information, which is sold on the Internet and dark web, making monitoring and analysis more difficult; there is an urgent need to improve the coverage and accuracy of analysis through intelligent computing technologies, such as Internet- and dark web-based risk intelligence analysis and deep learning models [18,19], to change passive response to active warning. In the digital age, data have become an important asset and strategic resource for companies to drive business decisions and improve operational efficiency; however, as required by laws and regulations on privacy and personal financial information protection, breaking "data islands" and balancing privacy protection and data applications have become critical issues.

4.6 Authentication

As one of the trust foundations in the digital economy era, trusted digital identities are gradually being used by financial institutions in a number of business processes, such as identity recognition, scene integration, risk control, and privacy protection. Based on the core technology of the Internet Plus trusted identity authentication platform, the Ministry of Public Security has established an authoritative, safe, credible, and convenient network identity authentication system. It has launched a resident ID card online function voucher, and actively promotes the

DOI 10.15302/J-SSCAE-2020.06.013

international exchange of online electronic identities [20].

Biometric identification has become an important element of user identity verification. Once leaked and illegally used, it will seriously damage the user's own interests; this poses challenges to the biometric AI algorithm model, such as distinguishing the authenticity of a user's will not from actual identity but from actual internal willingness.

4.7 Technology risk

The improper application of scientific and technological achievements in the field of payment risk control may lead to the double superposition of business security and technical risks, which, in turn, will have a greater impact on the payment market, transactions, and products [21]. AI has been piloted and applied in the field of payment risk control. Recently, some scholars have conducted research on AI security issues and security threats, and believe that technical defects and poor interpretability may cause irreversible security threats. Algorithms and data are the core of AI, and both have potential security risks that may lead to the risk of AI application decision-making [22]. In addition, AI systems have security risks in actual operation. Once they are improperly designed, they can easily be used by attackers to carry out illegal activities.

5 Suggestions

5.1 Build a multi-level big data sharing, analysis, and feedback platform

Starting from the three levels of country, industry, and enterprise, a multi-level platform for big data sharing, analysis, and feedback should be built to provide critical support for financial retail payment service entities as a public basic service.

Under the premise of complying with the relevant national laws and regulations, it is recommended that the national regulatory authority should establish a multi-ministerial joint data sharing mechanism, and refer to the joint working mechanism of the ministries and commissions to combat cross-border gambling and telecommunications network fraud, to further enrich and improve the national-level blacklist basic database. In the field of big data credit investigation, the establishment of an authoritative information database should be speeded up, covering the rural population and Internet lending information. Approved by relevant state departments, and with the support of local governments, local regulatory authorities should take the lead in establishing a regional data sharing platform, promoting the storage of credit information from local government departments and public institutions, and creating a credit information service platform with local characteristics to serve local financial institutions.

Payment industry associations and payment clearing organizations should build an industry-level big data analysis system based on voluntary market rules from the perspective of preventing payment risks and promoting the sound development of the payment industry. For example, China UnionPay Co., Ltd. uses its own network of inter-agency transaction data and risk case handling capabilities, based on blockchain and cloud computing technology, to perform risk control data and intelligence sharing analysis services and to establish a joint prevention and control mechanism.

The main body of a payment service is the user of the big data risk control application. It is recommended that, in accordance with the requirements of the People's Bank of China on establishing a big data risk control system, the data in various business lines within an enterprise should be opened up, that data authorization from users in business products should be obtained, and that an integrated big data management and application platform should be built. Those who access and use national and industry big data platforms should report data in a timely manner as required, and feed back the application and decision results after querying the data, to dynamically close the data application .

5.2 Promote an in-depth application of AI technology in the field of risk control

The application of AI technology in the field of payment risk control remains in its infancy; only some large Internet companies, national banks, and payment clearing organizations have carried out exploration and pilot projects, while many financial institutions still rely on experience-based and rule-based methods to carry out risk control, or only apply machine learning algorithms in individual business areas. To meet the high concurrency, real-time, and low tolerance business requirements of payment and related financial scenarios, it is recommended that the problems of model maturity, data availability, and computing power reliability be resolved expeditiously to promote AI applications.

In terms of model maturity, the regulatory authorities have proposed the full lifecycle management process and requirements for risk models. The application of AI technology in risk models should supplement relevant technical specifications and testing guidelines. Payment service entities need to develop mature AI models related to application scenarios. With a high-level index system, scientific research institutes and universities can cooperate to conduct basic and technical research on high-cognition models in the real-time financial risk control scenario.

Regarding data availability, the data required for risk control must be massive data, including enterprise internal and external data. In an era when personal information protection regulations and supervision are tightening, there is an urgent need to accelerate the application of privacy protection technologies, such as data joint modeling based on blockchain, secure multi-party computing, and federal learning frameworks. The two parties do not share the data, while they can still leverage the value of the data fusion.

Regarding computing power reliability, AI model operation and big data analysis require strong hardware resources; payment service entities should plan and formulate a technical roadmap for AI computing power and supporting platforms, and solidly promote infrastructure development.

5.3 Improve the comprehensiveness and robustness of the risk control system

The risk control and business systems are both coupled and separate. It is recommended that payment service entities establish a centralized intelligent risk control system for business systems.

Regarding comprehensiveness, it is recommended that all aspects of data, models, strategies, and operations be opened up. The data link is responsible for raw materials, categorizing and processing data from different business lines, covering real-time streaming computing, quasi-real-time distribution, and batch label pre-generation. The model link is processing with incoming materials, and multi-dimensional data is imported into the algorithm rule system for rapid calculation to produce quantitative results. The strategy aspect is classification and grading, while intelligent decision-making is carried out based on business expectations. Operational aspects refer to reaching customers, i.e., automating all matters of the workflow, improving customer experience, and forming a closed loop.

Regarding robustness, as complex system engineering, real-time risk control systems usually involve multiple modules, such as current data, historical tags, black and gray lists, external data, model rules, monitoring strategies, and operating procedures; the architecture design should fully evaluate the business key technology design solutions such as growth, external interface, system security, backup mechanism, fuse mechanism, and system performance, to ensure low latency, high concurrency, and flexibility.

5.4 Promote a culture and awareness of comprehensive risk management

Establishing a complete comprehensive risk management system is an important part of the modernization of financial enterprise governance. It is recommended that the risk awareness of all employees within an enterprise should be strengthened, and that risk professional sections or departments be established; there should be a change from managing and controlling risks to operating risks, and to promoting risk services to embedded, one-stop service upgrades to achieve full coverage of all business lines, all types of risks, and personnel in different positions.

The payment industry is currently facing a severe risk situation. It is recommended that commercial banks and other payment service entities establish a comprehensive risk management mechanism to build a risk middle platform; it is further recommended that risk management objectives at different stages be determined, risk management evaluation and full-process control be conducted, and that different business terms and risk responsibilities be defined for online business departments to prevent and resolve systemic risks.

5.5 Increasing payment risk control compound talent training

Traditional risk control experts are experts in the business field. Their professional backgrounds are usually economics and finance majors, and a few are statistics and data analysis related majors. With the popularization of big data, AI, cloud computing, and other scientific and technological achievements in the field of risk control, the demand for compound talents has become particularly urgent.

It is recommended that the cultivation of a compound talent team be prioritized and accelerated; in addition to traditional risk control experts, talents should be supplemented with professional backgrounds, such as mathematics, computer, and cyberspace security. The business of data analysis, AI, architecture design, and other capabilities and payment risk control should be promoted, combining the requirements to create an intelligent risk control expert team with a solid theoretical foundation, rich practical experience, and complete management capabilities.

DOI 10.15302/J-SSCAE-2020.06.013

References

[1] Wen X X. On the establishment of a modern payment system in the new era—Based on modernizing China's system of governance and governance capacity [J]. Frontiers, 2019 (24): 66–71. Chinese.

[2] Shao F J, Shi W C. Report on the development of China's bankcard industry [M]. Shanghai: Shanghai Culture Press, 2020. Chinese.

[3] Chen Y F, Mao X F, Li Y H, et al. AI security—Research and application on adversarial example [J]. Journal of Information Security Research, 2019, 5(11): 1000–1007. Chinese.

[4] Zhu L F. Research on artificial intelligence security problems and control measures [J]. Telecom Engineering Technics and Standardization, 2019, 32(12): 33–37. Chinese.

[5] Zhao B, Chai H F. A collection of excellent cases against bank card crimes (2014—2016) [M]. Beijing: Law Press · China, 2017. Chinese.

[6] Chen X H, Jiang J W, Zhou H, et al. Rapid layout and development strategy of hospital artificial intelligence during the COVID-19 pandemic [J]. Strategic Study of CAE, 2020, 22(2): 130–137. Chinese.

[7] Zhao S J, Xu K, Xue X Q, et al. Implementation countermeasures for information security management of intelligent connected vehicles [J]. Strategic Study of CAE, 2019, 21(3): 108–113. Chinese.

[8] Zheng X L, Zhu M Y, Li Q B, et al. FinBrain: When finance meets AI 2.0 [J]. Frontiers of Information Technology & Electronic Engineering, 2019, 20(7): 914–924.

[9] Pan Y H. Heading toward Artificial Intelligence 2.0 [J]. Engineering, 2016, 2(4): 409–413.

[10] EMVCo. Payment tokenisation specification technical framework V2.1 [EB/OL]. (2019-06-14) [2020-08-20]. https://www.emvco. com/emv-technologies/payment-tokenisation/.

[11] Dong J F. Efficient payment guarantees financial security [J]. China Finance, 2019 (21): 40–42. Chinese.

[12] Zhang Y. Consolidate the foundation of safety protection and build a safety system with both offensive and defensive functions [J]. Financial Computer of China, 2019 (8): 10–13. Chinese.

[13] Zheng Y. How technology supports "digital transformation" [J]. E-Finance, 2018 (4): 24–28. Chinese.

[14] Xu J, Qiao H. Association graph, a new tool for fraud risk prevention [J]. E-Finance, 2020 (6): 94–95. Chinese.

[15] Zhng L. Research on risk analysis and prevention of third party payment in China [J]. Think Tank Era, 2020, 228(8): 38–40. Chinese.

[16] Chai H F. Research on bankcard industry risk prevention and control in the era of Internet [J]. China Credit Card, 2016 (6): 38–41. Chinese.

[17] Zhou Y K, Chai H F. Research and practice on system engineering management of a mobile payment project [J]. Front of Engineering Management, 2017, 4(2): 127–137.

[18] Yang S L, Zhou B, Jia Y, et al. On the monitoring, analysis, and management of network public opinion: Current status and challenges [J]. Strategic Study of CAE, 2016, 18(6): 17–22. Chinese.

[19] Li J H. Overview of the technologies of threat intelligence sensing, sharing and analysis in cyber space [J]. Chinese Journal of Network and Information Security, 2016, 2(2): 16–29. Chinese.

[20] Fang B X, Du A N, Zhang X, et al. Research on the international strategy for national cyberspace security [J]. Strategic Study of CAE, 2016, 18(6): 13–16. Chinese.

[21] Chen H, Guo L. The causes, negative effects and the construction of prevention system of financial science and technology risks [J]. Reform, 2020, 313(3): 63–73. Chinese.

[22] Li J H. AI and cyberspace security [J]. China Information Security, 2019 (7): 32–34. Chinese.