

Analysis Of Problems and Countermeasures in The Development of Financial Technology in China

Zhuoran Hao *

UCD College of Business, University College Dublin, Singapore

* Corresponding Author Email: CT0378125@kaplan.edu.sg

Abstract. In recent years, Financial Technology (fintech) has developed rapidly in China, gradually changing the operation mode of traditional finance and also bringing some new risks and challenges. This article will focus on three typical problems that have emerged in the development process of fintech: information and privacy leakage, and the upgrading of financial fraud methods and the structural unemployment problem caused by the change in the job structure of the financial industry. On this basis, targeted countermeasures such as strengthening data supervision, upgrading risk control and identification technologies, and guiding the unemployed to re-employment are proposed, including strengthening data access permission management, enhancing technical identification capabilities, and providing institutional support for employment transformation of the unemployed. This study aims to draw attention of the public to the potential risks in the development of fintech while analyzing the problem and provide some practical reference directions for relevant policies and industry adjustments.

Keywords: Fintech; data leakage; AI face-swapping; structural unemployment.

1. Introduction

Finance plays an indispensable role in modern society and helps people make key decisions such as financing, investment and risk management [1]. A healthy financial system not only helps improve the efficiency of capital allocation but also enhances the stability and risk-resistance capacity of the economy [2]. Moreover, as technology integrates into financial industry, new services and products such as "buy now, pay later" and crypto assets keep emerging, significantly enhancing financial efficiency and consumption convenience. However, this technological progress has also brought about problems such as impulse consumption and excessive borrowing, increasing the complexity of risks. Especially in China, a country with a large population and a vast market, while fintech has rapidly integrated into the consumption and living scenarios of the Chinese people and driven economic growth, it has also exposed many potential risks, including the leakage of user information, the escalation of fraud methods, and the adjustment of the employment structure in the financial industry, which are social issues that cannot be ignored. While technology empowers finance, its operating mechanism also contains new risk incentives. Therefore, this article will analyze three typical problems that have emerged in the development of fintech in China, deeply delve into their underlying causes and manifestations, and attempt to propose feasible countermeasures and suggestions from the perspectives of data supervision, upgrading risk control and identification technologies, and guiding the unemployed to re-enter the job market, providing necessary references for a more stable development path of fintech in China in the future.

2. Problem

2.1. Data Leakage

Although fintech has enhanced business efficiency, due to its large volume of data involved, long processing chain and numerous participants, once problems arise, the impact will be even wider. The core of the data leakage problem lies in the fact that it is often not a one-off event but can occur at every small stage of the entire system operation process and gradually accumulate into serious consequences [3]. For instance, during the process where users register an application account and

fill in the information for authorization, many people are not clear about exactly which fields they have authorized and where these data will flow. Even if the platform marks the scope of use, users still find it difficult to perceive whether their data is being shared multiple times. The data sharing and system connection between platforms may also further expand the scope of data leakage [4].

Take the "Baitiao Pay" on the JD shopping platform as an example. Its essence is to allow users to use it first and pay later, and it is made possible by a complete system chain composed of financial technology. When a user clicks on "Baitiao", the back-end system will simultaneously initiate multiple steps such as identity authentication, risk control review, credit limit generation, and payment authorization. These steps may seem short, but each one requires the invocation of a large amount of user personal information. Throughout the entire process, the data of users is not only submitted to the platform itself, but may also be transferred to third-party institutions, such as risk control platforms, cloud storage services or credit partners and so on. This multi-party collaboration mechanism itself enhances efficiency, but at the same time amplifies risks [5]. Once there is an oversight in any step of the management or the internal authority control is unclear, it is possible that the information will be exported, leaked or even resold.

As different steps may be contracted by different fintech companies or external service providers, once a security issue occurs in a certain step, the data may be copied or transferred to other channels, increasing the complexity of tracking the leakage path. For instance, if the consumption behavior data of users is stored after being processed by the cloud, and the platform does not strictly restrict access rights, managers or external interfaces might read these data, thereby posing a risk of leakage.

2.2. Escalation of Fraud

The development of fintech has enhanced the efficiency of loans and payments, but it has also led some fraudsters to start using technological means to carry out more covert frauds. In the past, methods of fraudsters might have been limited to pretend as customer service representatives and sending phishing text messages. But now, they are beginning to utilize AI technologies, such as face-swapping, voice synthesis, and simulated videos, to create more realistic identity forgery methods [6-7]. For instance, some fraudsters would forge identity information of users and bypass the identity verification system of platform through AI-synthesized facial video or voice to apply for loans or defraud the credit limit of the platform. This kind of approach no longer merely targets ordinary users but turns to deceiving the platforms themselves. By pretending as real users, they bypass risk control reviews, defraud large loans and then directly cash them out.

What is more complicated is that some fraud gangs take advantage of system loopholes to carry out "account nurturing" operations. In the early stage, it is manifested as normal repayment, timely consumption, and accumulation of good credit. After the platform relaxes its vigilance, they suddenly apply for large loans and then go missing [8]. This kind of "account nurturing and loan fraud" is no longer a single-user behavior, but rather an organized process with clear division of labor, with the aim of gaining the trust of the platform system. In addition to deceiving platforms, some technical frauds have also begun to target the relatives of users. In addition to deceiving platforms, some technical frauds have also begun to target the relatives of users. For instance, if social media accounts of some people are stolen by fraudsters, then these accounts will be utilized by fraudsters for AI face-swapping or fake videos and to trick family members of these people into transferring money. Some offenders may even complete the entire fraud process in a short period of time, and it is often difficult for people to distinguish the true from the false in such a short time. The key to the success of these measures lies in the high degree of automation of platform review. Although facial recognition and voice recognition have improved efficiency, if there is a lack of corresponding anti-fraud mechanisms, once the system is bypassed, it is easy to cause system-level risks. The increasing reliance of fintech on automated models, along with the reduction of manual reviews, has provided opportunities for some technological fraud methods.

Combining these inferences into a general view, the upgrading of financial fraud methods is closely related to the digital characteristics of financial technology. When all the processes of the

system rely on technology, once the technology is abused or bypassed, the risks will also be magnified accordingly. Therefore, the change in fraud methods cannot be simply regarded as the alteration of the fraud means themselves, but rather as the operation mode of the entire financial technology providing fraudsters with new space.

2.3. Structural Unemployment

The development of fintech has brought about a whole new set of financial operation methods, gradually reducing many job positions in traditional financial institutions [9]. In the past, in banks or credit platforms, after customers submitted their applications, they had to go through multi-level review, communication and follow-up by employees. But now, the vast majority of these processes can be completed through the system. For instance, nowadays, as long as users upload information online, the system of platform can automatically recognize and judge it, without the need for too many people to get involved. As a result, those tasks that relied on manual labor are gradually being replaced. This change has directly led to the gradual disappearance of the originally numerous employment positions, with some employees being laid off or their job contents being compressed, making them increasingly marginalized. This process reflects the structural unemployment caused by social development and economic changes, where the existing skills of workers do not match the skills required for their current jobs [10].

Meanwhile, some platforms in China have also undergone changes in recruiting talents. Nowadays, there is a common phenomenon on recruiting talents who are proficient in modeling, data, and products, rather than traditional customer service representatives, account managers and so on [11]. And these new positions have relatively high requirements for ability and major. People who are originally engaged in traditional positions will also have great difficulty adapting to the new ones. Although many employees also want to learn new skills, have no foundation and the transformation process is rather difficult. It turns out that there are a wide variety of job types in the financial industry, and many people can find suitable positions within it. But now, after these traditional positions have been replaced by the system process, the opportunities left for people have become fewer, and the barriers to entry for new positions is very high. Some people are unable to change positions or industries easily, and thus stuck in a dilemma. When these changes combined, have made the employment structure of the entire financial industry no longer as stable as before. Although fintech has brought about efficiency improvements, it has also made many employees face difficulties in transformation and even the risk of unemployment. Such a trend may continue in the short term and also sows the seeds of hidden risks for future social conflicts.

3. Countermeasure

3.1. Reduce Information Leakage

The key of the information leakage problem lies in the fact that data operation needs to go through multiple links, and if there are any problems in any link, there will trigger risks throughout the entire chain. The platform can take action from both the technical and management aspects and gradually establish a set of multiple protection mechanisms. For instance, establish access classification for sensitive data, strictly control employee permissions, and prohibit unauthorized extraction of information. Meanwhile, the platform should record each data invocation behavior to ensure that any issues can be traced back promptly once they arise.

In addition, for third-party cooperative platforms, clear boundaries of responsibility and data usage norms should also be established to prevent data from being transferred or shared without authorization. In terms of management, the principle of "whoever accesses it, takes responsibility" should be adopted, and every link in the data access chain should be supervised. These additional measures can minimize the risk of information leakage as much as possible while reducing the impact on efficiency.

3.2. Upgrade the Anti-fraud Mechanism

In the face of increasingly complex fraud methods, the platform should first enhance its technical identification capabilities. For example, a system that recognizes AI-synthesized images and audio can be added to detect whether there are any traces of forgery when users verify their identities. For abnormal behaviors and application processes, model-based detection and early warning can enhance the defense capabilities of system.

At the same time, anti-fraud alerts should also be strengthened on the user end. For instance, risk warnings should be popped up during sensitive operations, security authentication should be required, and even simple anti-fraud tests can be designed to enhance their awareness of prevention. In addition, the platform should also establish a coordination mechanism with public security organs or anti-fraud institutions, share risk account information and new fraud models in real time, and form a more effective prevention and control network.

3.3. Guide Industry Transformation

In the face of the structural unemployment phenomenon emerging in the financial industry, short-term measures can be taken by the platform to provide certain buffer measures, such as offering transitional subsidies and psychological counseling to laid-off workers. Long-term measures should open up channels for employees to transition to technical positions through training, certification and other means. Furthermore, the government can collaborate with enterprises to establish specialized courses for transitional groups, with a focus on helping the unemployed master basic technical tools. Meanwhile, to ensure that the transformation is of practical significance, it is suggested to establish valuable professional qualification certificates, certify those who have completed the training, and encourage enterprises to refer to the results of these certificates in recruitment. Moreover, the platform can also provide suitable positions for people of different ability levels. Doing the above measures can not only alleviate the direct impact brought by layoffs, but also reduce social anxiety to a certain extent.

4. Conclusion

In recent years, with the accelerated popularization of fintech in China, the operational logic of the traditional financial industry is undergoing a significant transformation. Although the wide application of technology has brought about the optimization of processes and the improvement of efficiency, it is also accompanied by a series of new problems gradually emerging. This article explores three prominent practical predicaments in the development of fintech, namely the expanding risk of user data leakage, the increasing intelligence of fraud methods, and the employment pressure brought about by the reorganization of industry job structures. Centering on the above issues, this paper attempts to propose specific countermeasures, including strengthening the data processing norms of the platform, improving the risk identification mechanism and security verification process, and promoting support measures for career transformation from the institutional level at the same time. It is hoped that through these analyses, all sectors of society can be guided to have a more comprehensive understanding of the potential risk factors in the development process of fintech, and provide feasible reference basis for future policy-making and industry reform.

However, in the entire analysis and countermeasures, there is also a loophole that cannot be ignored. For instance, regarding the issue of user privacy leakage, although many regulatory measures have been proposed in the article, in reality, once data is leaked, it is no longer within the controllable range. This information is very likely to have long been rapidly copied, stored and disseminated on the Internet, rather than being completely erased like deleting a file. This also means that no matter how strict the regulation becomes in the future, it cannot completely erase the past losses. Therefore, the countermeasures in this part are more suitable for preventing a new round of data risks. As for the leaked data, the impact can only be minimized as much as possible through measures such as tracing responsibility, restricting usage and enhancing anti-fraud awareness.

References

- [1] Beck T, Levine R. Stock markets, banks, and growth: Panel evidence. *Journal of Banking & Finance*, 2004, 28(3): 423–442.
- [2] Levine, Ross. Finance and growth: theory and evidence. *Handbook of economic growth*, 2005, 1: 865-934.
- [3] Telefónica Tech. Systemic Cyber Risk: Threatening organizations and society. *Telefónica Tech Blog*, 2023.
- [4] Zhang Y, Wang X, Li M. Corporate Data Sharing, Leakage, and Supervision Mechanism Based on Game Theory. *Sustainability*, 2021, 13(2): 931.
- [5] Safetica. Data Loss Prevention in Fintech. *Safetica Blog*, 2023.
- [6] Wang X. Ways to combat telecom fraud. *China Daily*, 2023.
- [7] The Straits Times. China scammer uses AI to impersonate victim’s friend, steal millions. 2024. Available at: <https://www.straitstimes.com/asia/east-asia/china-scammer-uses-ai-to-impersonate-his-victim-s-friend-steal-820000>
- [8] Zhang Y, Wang X, Li M. Financial literacy and fraud detection—Evidence from China. *Journal of Economic Behavior & Organization*, 2021, 190: 1–15.
- [9] Fintech’s Double-Edged Sword: Innovation vs. Job Displacement in the Financial Industry. *B2B Technology Zone*, 2023.
- [10] IMF. Unemployment: The Curse of Joblessness. IMF, 2023
- [11] Zhang L, Liu M. The impact of financial technology on employment: Protection or displacement. *Journal of Economic Behavior & Organization*, 2024, 190: 1–15.