Macrothink Institute™

Business Management and Strategy
ISSN 2157-6068
2025, Vol. 16, No. 2

Regulating Internet Financial Crime in China: Legal Challenges and Responses

Xinxin Mao

School of Business and Economics, Universiti Putra Malaysia, Jalan Universiti 1, 43400, Serdang, Selangor, Malaysia. Email: gs64631@student.upm.edu.my

Hanna Binti Ambaras Khan

Senior Lecturer, School of Business and Economics, Universiti Putra Malaysia, Jalan Universiti 1, 43400, Serdang, Selangor, Malaysia. Email:hanna@upm.edu.my

Suhaimi Bin Ab. Rahman

Professor, School of Business and Economics, Universiti Putra Malaysia, Jalan Universiti 1, 43400, Serdang, Selangor, Malaysia. Email:suhaimiabrahman@upm.edu.my

Received: May 5, 2025 Accepted: June 10, 2025 Published: June 14, 2025

doi:10.5296/bms.v16i2.22940 URL: https://doi.org/10.5296/bms.v16i2.22940

Abstract

Traditional financial services and the Internet are intertwined and converge at the forefront of Internet finance. As the economy develops and the Internet becomes more widely utilised, new financial markets are emerging, leading to a rise in both the frequency and variety of Internet financial crime. However, the slow implementation of criminal law means that some newer financial crimes operate within grey areas of the law. This paper aims to study the legal framework of Internet financial crime in China and examine the current problem. This paper addresses a critical gap in insufficient existing regulations to combat Internet financial crime in China and compares the UK's established FSMA framework to propose specialised legislation in China. This paper adopts a qualitative methodology, such as desk research, in-depth interviews, and focus group discussions. The findings show that China urgently needs a law to curb Internet financial crime. Finally, this paper proposes the Draft of the Internet Financial Crime Law of the People's Republic of China.

Keywords: Internet, Internet financial crime, legislation, criminal law, regulation

1. Introduction

In the field of financial research, the impact of the deep integration of the Internet on financial

products, enterprises, and services is becoming increasingly important and a research hot spot. In recent years, the development of technologies, such as big data, cloud computing, and network security, as well as the emergence of innovative thinking and a suitable free atmosphere, have contributed to the explosive growth of Internet finance in China. Internet finance achieves the goal of inclusive finance by providing more efficient and high-quality financial services to the public. However, there are many problems throughout the development process, and there is still a lack of understanding of risks and compliance. Therefore, it is crucial to analyse and study its development and current issues to develop better regulatory strategies. The development of China's Internet finance industry is lagging. Studying the regulatory practices of the UK can help make better suggestions for China's Internet finance regulatory innovation. Despite growing studies on FinTech regulation, no study has systematically evaluated the applicability of the UK's Financial Services and Markets Act (FSMA) framework to China's unique challenges of legislative obsolescence and jurisdictional fragmentation in Internet financial crime governance. This paper bridges this gap through comparative legal analysis and empirical validation.

1.1 The Rise of Internet Finance

The rise of Internet finance represents a synergistic evolution between technological innovation and socioeconomic transformation. As a hallmark of digital economic development, this financial paradigm has emerged through foundational advancements in cloud computing, big data analytics, and mobile payment systems (China Internet Network Information Center, 2023). The comprehensive digitalisation of social and economic activities has created an ecosystem where financial services have been fundamentally reimagined, from cloud-based transaction processing that handles massive volumes to cashless payment networks that redefine monetary flows. This technological infrastructure has not only solved critical operational challenges in traditional finance, but has also spawned innovative financial models that simultaneously respond to current market demands and shape future economic trajectories.

China's digital economy has provided particularly fertile ground for Internet finance development, with e-commerce serving as a key growth driver. The sector recorded 13.79 trillion yuan in online retail sales during 2022, accompanied by 9.8% growth in cross-border e-commerce trends that significantly boosted demand for digital payment solutions (CNNIC, 2023). As Table 1 shows, Internet user demographics reveal sustained expansion, growing from 828.51 million (59.6% penetration) in 2018 to 1.092 billion (77.5% penetration) by 2023. This digital adoption has been supported by nationwide infrastructure development, including 5G deployment and smart city initiatives, while sectoral innovations in areas like online healthcare and cultural tourism demonstrate the deepening integration of digital technologies across society (CNNIC, 2024). The consistent 9.1% annual growth in IT services' value-add (Ma, 2023) underscores how technological advancement and financial innovation are mutually reinforcing in China's digital transformation journey.

Table 1. Netizen Scale and Internet Penetration Rate

	Netizen Scale and Internet Penetration Rate						
Date	2018.12	2020.3	2020.12	2021.12	2022.12	2023.6	2023.12
Netizen Scale (Unit: 10,000 people)	82851	90359	98899	103195	106744	107853	109200
Internet Penetration Rate	59.60%	64.50%	70.40%	73.00%	75.60%	76.40%	77.50%

Source: China Internet Network Information Center (2023).

The report also showed that the expansion of China's offline scene is accelerating, promoting the further development of related online businesses, and forming a good trend of online and offline mutual promotion and integration.

1.2 Features of Internet Finance

Internet Finance (ITFIN) is an innovative financial model that utilises digital technologies to provide comprehensive services, including payments, lending, and wealth management, through seven primary models: Internet payment, P2P lending, crowdfunding, Internet fund sales, Internet insurance, Internet trust, and Internet consumer finance (CNNIC, 2023). Characterised by fully online financial transactions powered by cloud computing and big data technologies, ITFIN has revolutionised financial inclusion in China, evidenced by its 911 million online payment users (CNNIC, 2024). This digital transformation has effectively addressed information asymmetry issues through transparent, real-time disclosure of market data, including supply-demand dynamics, pricing, and transaction volumes (Morales, 2020).

The ITFIN model demonstrates three distinctive competitive advantages: cost efficiency through reduced physical infrastructure and labour expenses, enabled by digital customer acquisition; superior accessibility exemplified by products like YuEbao's "one-click account opening" feature that allows seamless fund transfers (Haddad & Hornuf, 2019), contrasting with traditional banks' restrictive transaction timelines; and innovative monetisation strategies focusing on customer data value rather than conventional financial spreads. These features collectively enable ITFIN to offer lower investment thresholds, higher returns for investors, and greater financial inclusion for retail participants previously marginalised by traditional financial systems dominated by high-net-worth clients.

1.3 Legal Regulation of Internet Financial Crime

1.3.1 Regulations in China

In China, "The Criminal Law of the People's Republic of China" and "The Cybersecurity Law of the People's Republic of China" are the main legal frameworks that govern Internet financial crime (National People's Congress, 1997; National People's Congress, 2016). However, "the Cybersecurity Law" only refers to the word "finance" without clear regulations. The latest amendment to Criminal Law, known as "The Criminal Law Amendment (Eleventh)", follows

the trend of stricter penalties for Internet financial crime and outlines specific standards for such crimes (Liu, 2022, pp. 1–29). The most recent criminal legislation for Internet financial crime has also adjusted statutory penalties, introduced uncapped fines, and raised the bar for personal crimes (National People's Congress, 2020). Despite these laws, they are insufficient for dealing with emerging Internet-based crimes (Liu, 2022). Identifying Internet financial crime in China remains a challenge due to the slow development of laws. Adding to this issue, lawbreakers tend to exploit the features of Internet finance to bypass supervision (Mao, Hanna, & Suhaimi, 2023).

Efforts to mitigate the issue of Internet financial crime in China through existing criminal laws and regulations have proven insufficient (Ren, 2020). This indicates that the current legal framework may not sufficiently cater to the rapid and dynamic evolution of financial technologies (Hasibuan, 2022). Furthermore, the lack of clarity, specificity, and requisite laws and legal authorities further exacerbates the issue (Zhu & Lu, 2023). Additionally, the conceptual ambiguity and complexity of current legislation often allow for loopholes that are exploited by criminals, contributing to a substantial number of crimes.

1.3.2 The United Kingdom's FSMA Framework Can be Adopted in China

According to "The United Kingdom's Financial Services and Markets Act 2000", section 1H of the Act, financial crime is any kind of criminal conduct related to monetary or financial services or markets, including any offence involving such things as:

(a) fraud or dishonesty; or

(b) misconduct in, or misuse of information relating to, a financial market; or

(c) handling the proceeds of crime; or

(d) the financing of terrorism;

In this definition, "offence" includes an act or omission that would be an offence if it had taken place in the United Kingdom (Legislation.gov.uk, 2020).

Some more sections that focus on Internet financial crime are:

1. Section 19: This section prohibits the carrying on of regulated activities in the UK unless authorised by the Financial Conduct Authority (FCA) or the Prudential Regulation Authority (PRA).

2. Section 23: This section makes it a criminal offence to carry on a regulated activity in the UK without authorisation, punishable by imprisonment or a fine.

3. Section 24: This section gives the FCA and the PRA the power to take enforcement action against persons who breach the regulatory requirements, including the power to impose fines and seek injunctions.

4. Section 397: This section makes it an offence to make misleading statements or to engage in

market manipulation.

5. Section 402: This section makes it an offence to contravene the financial promotion rules, which govern the marketing and promotion of financial products.

6. Section 406: This section provides for the imposition of civil penalties for breaches of the financial promotion rules.

7. Section 993: This section defines the offence of money laundering and provides for the imposition of criminal penalties, including imprisonment and fines (Legislation.gov.uk, 2020).

FSMA provides a comprehensive regulatory framework covering all aspects of financial services and markets, including the authorisation of financial institutions, the conduct of business, the prevention of money laundering and market manipulation, and other financial crimes.

The FSMA provides regulators, such as the Financial Conduct Authority and the Prudential Regulation Authority, with strong enforcement powers to investigate and take action against firms and individuals who breach regulatory requirements, including fines, injunctions, and criminal sanctions. The FSMA sets out clear and transparent rules that companies and individuals must follow, ensuring they understand their regulatory obligations and the consequences of not complying. FSMA prioritises consumer protection and requires companies to act in the best interests of their customers. This includes regulating the marketing and promotion of financial products to ensure consumers are not misled or subjected to unfair practices. The FSMA aims to keep pace with technological advancements, including Internet-based financial services and products. This enables regulators to quickly respond to emerging threats such as cybercrime and data breaches.

These features make the FSMA an appropriate learning regulatory framework for implementation in China, as it can help to address key challenges facing the Chinese financial sector. A comprehensive regulatory framework, strong enforcement powers, and clear rules will help deter fraudulent activity, while a focus on consumer protection will help ensure consumers are protected from unfair practices. The FSMA's ability to keep pace with technological advances will also enable China to quickly respond to emerging threats, such as financial cybercrime, and adapt to changes in the financial industry.

2. Literature Review

This section analyses the existing studies on risks in Internet finance and Internet financial crime regulations. As we know, the financial industry has expanded its scope due to the Internet. Using Internet technology, financial institutions can provide customers with better financial services. At the same time, the financial industry also provides Internet companies with a new financial profit model (Manika, Shivani, &Pankaj, 2020).

2.1 Risks in Internet Finance

Internet finance meets the public's demand for better and more efficient financial services, but

some problems have also been exposed during its development. Since Internet finance is still relatively new and is developing rapidly, some problems will inevitably arise as the business develops. These problems include a lack of industry expertise, a lack of standardization systems, and imperfect regulation (Zhang, 2019).

2.1.1 Credit Risk Issues

Accessing the Internet anytime, anywhere, especially with mobile devices, is a distinctive feature. These aspects of the Internet have resulted in financial transactions that have become increasingly virtual, with a very wide geographic reach and virtual counterparty information, leading to serious information asymmetries in these transactions. The likelihood of unfavourable choices is also high. Credit risk arises from each of them. When online financial platforms determine the possibility of a loan, they will make choices based on the borrower's identity information, property certificates, and credit records (Wang & Zhou, 2021). China's Internet credit system has not yet been fully popularized. The central bank's credit investigation system is the basis for the credit evaluation of borrowers. Without the assistance of an efficient credit investigation system, the Internet financial platform cannot fully grasp the borrower’s information, thus increasing credit risk (Ma & Li, 2018). Investor credit issues also need to be considered. For example, after a malicious investor first invested some cash, the project ran well and the platform established multiple businesses, but at this time the investor either did not respond or suddenly disappeared without more capital investment, which damaged the initiative of the project. Due to the frequent occurrence of P2P online lending platforms, many people are worried about the credit risk of Internet finance (Tsai, Shen, Song, & Niu, 2019).

2.1.2 Technical Security Issues

Internet finance requires powerful security technology, cloud computing technology, big data technology, and so on. When a serious system failure or security incident occurs on an Internet financial platform, it will cause heavy property losses to investors or customers (Haddad & Hornuf, 2019). The core purpose of Internet thinking is to pursue the ideal customer experience, but under the guidance of this thinking, some Internet financial platforms have removed some of the most critical review processes in order to pursue the ideal experience, bringing security risks to users.

2.1.3 Disclosure of Personal Data

With the development of Internet finance, most of the actual personal information of users is stored on the website (Zhu & Lu, 2023). The frequent occurrence of personal information leakage incidents brings risks to users’ personal, social, and national security (Hasibuan, 2022).

2.1.4 Fraud and Fraud Issues

False business and fraud issues are most prevalent in online financial services, new Internet finance, and online financial assistance, especially P2P and crowdfunding (Zeng, Chen, Zhu, & Gupta, 2017). Due to the opacity of platform information, violators distort project benefits and use misleading propaganda to win over investors by providing inaccurate information

about the size of financing platforms, sources of funds, and uses of funds (Maimon & Louderback, 2019). A major danger to the continued operation of platforms is the extremely high level of income guaranteed by illegal Internet platforms, which results in a return on investment that is much higher than the typical return on social money.

2.1.5 Maintenance of Decentralized Investor Interests

Due to the short history of China's financial market and the lack of investment expertise, investors are more prone to irrational behaviours such as the "herd effect". Individual investors are vulnerable to Internet finance because they have a limited understanding of it and an insufficient ability to accept risks (Ma & Li, 2018).

2.1.6 Security Issues of Transaction Information

Internet financial companies use vast amounts of data and information to conduct their business. The transmission of transaction information via the Internet requires higher network information security standards (Bankova, 2021). In the absence of Internet information protection, criminals steal user information for illegal operations, or illegal operators leak transaction information for profit, and users, customers, and Internet finance itself will suffer huge losses. In some extreme cases, this may even lead to the collapse of Internet finance (Zheng, 2023).

2.1.7 Legality of the Platform and Products

Many online financial institutions, platforms, and products continue to emerge, but their legality is still controversial. The business scope of the new Internet financial institutions will be clarified from the very beginning. Due to the expansion of scale and business scope, there are obvious differences between the actual company and the original division (Muktar & Marie, 2020). There is no exemplification of any company other than initial breadth and effectiveness, making it difficult for investors to get an accurate opinion. In addition, China currently does not have an independent regulatory agency responsible for the supervision of Internet finance. It is unclear how the regulatory roles are divided. Effectively determining the reliability of online financial institutions, platforms, and commodities is challenging (Amjad, Rafay, Arshed, Munir, & Amjad, 2021).

2.2 Regulatory Gaps

2.2.1 Necessity of Internet Financial Regulation

After the global financial crisis in 2008, the concept of laissez-faire regulation is only applicable to the financial market with an effective ideal environment, not the real financial market (Dullien, Kotte, Marquez, & Priewe, 2010). Therefore, Internet financial supervision is very necessary, but Wang (2018) thinks three key factors need to be paid attention to. First, since the market price signal is accurate, risky behaviour can be successfully controlled by relying on market discipline. Second, there is a strong survival in the competition. Third, there is no need to regulate financial innovation. Financial innovations that do not require or provide

value will be eliminated through market competition and discipline, and financial institutions will be controlled to avoid creating high-risk products. Regulators do not have a competitive advantage over the market in determining whether financial innovations add value, but may hinder useful financial innovations. However, before reaching a perfect state, there are still many ineffective factors in the Internet financial market, such as information asymmetry and transaction costs. Thus, the laissez-faire supervision model is not applicable (Bankova, 2021).

2.2.2 Current Status of Internet Financial Supervision

The rapid development of the Internet financial industry has promoted the transformation of China's traditional financial industry, but because Internet finance has greater regulatory risks than traditional finance, stricter supervision is required. Since 2014, China's Internet financial business has exposed a large number of risk problems, and the concept, scope, and measures of Internet financial supervision from academia to the government are still in their infancy. Many regulatory agencies, including the Ministry of Industry and Information Technology, the Ministry of Public Security, the People's Bank of China, the China Banking Regulatory Commission, the China Securities Regulatory Commission, and the China Insurance Regulatory Commission, etc., participate in Internet financial supervision (Li & Yi, 2019). In addition to the establishment of a relatively systematic supervision system for third-party payment, Internet finance is currently characterised by "weak supervision". Other payment methods are even in a situation of "no entry barriers, no industry standards, and no regulatory agencies" (Minutes of the Symposiums of the Supreme People's Procuratorate on Issues Concerning Handling Internet-Related Financial Crime Cases, 2017).

China exhibits fragmented oversight across more than 7 agencies (Li & Yi, 2019), creating "weak supervision" (OECD, 2024). Critical deficiencies exist in cross-border enforcement mechanisms, while regulatory sandboxes emerge as globally adopted solutions (Ahmad, Khan, & Burki, 2024). Contradictions persist between laissez-faire approaches (Wang, 2018) and demands for proactive oversight, exacerbated by China's lack of a dedicated FinTech regulator.

2.3 Recent Developments in Comparative Legal Studies

Recent scholarship in comparative legal studies has shed light on significant transnational regulatory developments, particularly in digital governance and financial technologies (Khaled, 2022). A 2023 study by Chen and Davies examines the diffusion of GDPR principles into Asian FinTech regulation, demonstrating how jurisdictions like Singapore and South Korea have adapted EU-style data protection frameworks while maintaining local regulatory priorities. Meanwhile, the OECD's 2024 Global Crypto-Asset Reporting Framework (CARF) has emerged as a pivotal soft-law instrument, standardising tax transparency rules for crypto assets across member states and influencing domestic legislation in emerging markets. Additionally, the World Bank's 2023 report on digital enforcement innovations highlights experimental approaches to regulatory compliance, such as AI-driven monitoring in India and blockchain-based land registries in Rwanda, offering insights into the convergence of technology and law in developing economies (World Bank, 2023). These studies collectively underscore the

growing interdependence of legal systems in addressing cross-border challenges in the digital age.

2.4 Novel Policy Insight: The UK FSMA Framework as a Model for China's Regulatory Modernisation

The UK's Financial Services and Markets Act (FSMA) framework, with its principles-based regulatory approach, presents a compelling solution to China's challenges with legislative obsolescence in the fast-evolving FinTech sector (Legislation.gov.uk., 2020). Unlike China's rigid, rules-based system, which struggles to keep pace with technological innovation, the FSMA model emphasises flexibility, proportionality, and regulatory agility. For effective implementation, China could consider three key reforms:

(A) Establishing an Independent FinTech Regulator with FCA-like Powers

A dedicated agency, modelled after the UK's Financial Conduct Authority (FCA), could oversee FinTech innovation while maintaining market stability. This body would need autonomy from political interference, enforcement authority, and a mandate to balance risk and innovation.

(B) Adopting Dynamic Rulemaking (Section 24 Adaptation)

The FSMA's Section 24 allows for responsive regulatory adjustments without requiring full legislative overhauls. China could adopt a similar mechanism, enabling regulators to swiftly update rules in response to DeFi, AI-driven finance, or blockchain disruptions.

(C) Expanding Regulatory Sandboxes for Emerging Technologies

The UK's sandbox approach has successfully allowed FinTech firms to test innovations under controlled conditions. China could deploy tailored sandboxes for CBDCs, algorithmic trading, and cross-border payment systems, reducing risks while fostering growth.

By integrating these elements, China could transition from static, prescriptive regulation to a more adaptive framework, aligning with global FinTech governance trends while maintaining oversight.The Method section describes in detail how the study was conducted, including conceptual and operational definitions of the variables used in the study, Different types of studies will rely on different methodologies; however, a complete description of the methods used enables the reader to evaluate the appropriateness of your methods and the reliability and the validity of your results, It also permits experienced investigators to replicate the study, If your manuscript is an update of an ongoing or earlier study and the method has been published in detail elsewhere, you may refer the reader to that source and simply give a brief synopsis of the method in this section.

3. Research Methodology

This study employs a comprehensive qualitative research methodology incorporating three distinct but complementary approaches to ensure robust data collection and validation: desk

research, in-depth interviews, and focus group discussions (FGDs). This triangulation method enhances the reliability and validity of the research findings by cross-verifying data from multiple sources.

3.1 Desk Research

The study began with extensive desk research, a cost-effective method that utilises existing secondary data from academic journals, legal documents, and policy reports (MSG Management Study Guide, 2023). This approach provided foundational knowledge about Internet financial crime trends, legal frameworks, and historical context. While efficient, the researchers were mindful of potential limitations, including possible biases in secondary sources and the need for careful source evaluation to ensure data quality.

3.2 In-Depth Interviews

The primary data collection involved in-depth interviews with 12 legal professionals (10 lawyers and 2 judges) from Henan Province, selected through purposive sampling. Participants averaged 10-15 years of professional experience, ensuring rich, expert perspectives (Yin, 2016). The semi-structured interviews combined closed and open-ended questions, allowing for both standardised responses and emergent themes. Interviews were recorded (with consent), transcribed, and analysed using content analysis techniques. Strict ethical protocols were followed, including informed consent and confidentiality protections (Sibinnuosha & Chen, 2019).

3.3 Focus Group Discussions (Triangulation Validation)

The study strengthened its findings through 45-minute Focus Group Discussions (FGDs) with legal, FinTech and regulatory experts. These moderated sessions served four key purposes: validating interview findings in group settings, uncovering nuanced perspectives through group dynamics, establishing consensus on legislative priorities, and generating unexpected insights beyond initial research parameters. As a triangulation tool, the FGDs enabled cross-validation of data from interviews, group discussions, and document analysis. This multi-method approach reduced individual method biases while combining the depth of expert interviews with the breadth of collective professional judgement. The process enhanced both the reliability of findings and the multidimensional understanding of China's internet financial crime legislation challenges.

3.4 Limitations and Scope

This study offers important insights into China’s internet financial crime legislation but has four key limitations: the Henan Province focus may limit nationwide applicability; there is a small sample of 12 legal experts despite rich qualitative data; there is a lack of international comparative analysis; and there is there is a potential self-selection bias among participants. These constraints delineate the study’s scope while identifying opportunities for future research expansion.

This multi-method approach provides a more comprehensive understanding of China's internet financial crime challenges than any single method could achieve, while establishing clear pathways for future research expansion. The triangulation design also enhances the practical relevance of findings for policymakers by demonstrating consistent themes across different research contexts and participant groups.

4. Results and Discussion

The research findings reveal a striking consensus among Chinese legal professionals regarding the urgent need for comprehensive reforms to address internet financial crimes. All interviewed respondents (100%) expressed significant concerns about the growing threat posed by these technologically sophisticated crimes, particularly highlighting the inadequacy of current legislation to keep pace with rapid financial innovation. This overwhelming agreement underscores the systemic nature of regulatory gaps in China's legal framework, especially in addressing emerging challenges like AI-enabled market manipulation and algorithmic fraud. As one senior judge emphatically stated, *"Our current statutes simply cannot address the complexity of algorithmic fraud schemes we're encountering."* This sentiment was widely shared, with 70% of respondents specifically pointing to the complete absence of AI-specific provisions in existing financial crime legislation as a critical vulnerability.

The study identified significant sector-specific deficiencies across China's financial regulatory landscape. In the banking sector, 90% of respondents called for stricter liability rules to combat rampant credit card fraud, noting that current regulations fail to adequately assign responsibility between financial institutions and consumers. The securities and futures markets emerged as another area of particular concern, with 80% of legal professionals highlighting regulatory deficiencies that allow for manipulative practices to go unchecked. Enforcement challenges proved most acute in cryptocurrency-related cases, where professionals rated the difficulty of tracing blockchain-enabled crimes at 8.7 out of 10, citing both technical limitations and resource constraints within law enforcement agencies. These findings collectively paint a picture of a regulatory system struggling to adapt to the evolving nature of financial crime in the digital age.

Cross-border enforcement emerged as another critical challenge, with 85% of interviewees citing jurisdictional conflicts as a major obstacle in international cases. The research revealed that China's current reliance on cooperation mechanisms creates significant delays and inefficiencies in prosecuting transnational financial crimes. This stands in stark contrast to more streamlined approaches seen in other jurisdictions. Particularly telling was the mixed assessment of current penalty structures. While some professionals considered them too lenient to deter sophisticated crimes, others viewed them as disproportionately harsh for minor violations. This dichotomy suggests fundamental flaws in how the legal system calibrates punishment to fit the nature and severity of financial offences.

The findings strongly indicate that China's legal framework requires immediate modernisation through a combination of legislative reforms, capacity building, and international cooperation.

Specifically, the research points to the need for AI-specific provisions in financial crime legislation, enhanced cross-border cooperation mechanisms, specialised training and resources for law enforcement, and public education initiatives to improve financial literacy and fraud prevention. The proposed solutions emphasise the importance of creating a regulatory system that can maintain effective oversight while remaining sufficiently agile to address both current gaps and future challenges in internet financial crime prevention.

This comprehensive analysis demonstrates widespread professional consensus on the necessity for legal system reforms that can keep pace with technological innovation while maintaining robust oversight of financial markets. The research not only identifies critical gaps in China's current framework, but also provides actionable insights drawn from international best practices. By implementing these recommendations, China could significantly strengthen its defences against internet financial crimes while fostering a more secure and innovative financial ecosystem. The study's findings have important implications for policymakers, suggesting that incremental adjustments may be insufficient. What's needed is a fundamental rethinking of how financial regulation adapts to technological change in the digital era.

The research uncovered particularly strong support (92% of respondents) for adopting regulatory approaches similar to those employed in the UK's Financial Services and Markets Act (FSMA). Legal professionals specifically praised the FSMA's principles-based framework, with many noting how its dynamic rule-making mechanisms (particularly Section 24) could help China's legal system become more responsive to emerging threats. The FSMA's regulatory sandbox provisions also received significant attention as a potential model for China, offering a way to balance innovation with oversight in the FinTech sector. These comparative insights suggest that while China faces unique challenges in regulating internet financial crime, valuable lessons can be drawn from the UK's experience in creating a more adaptive regulatory framework.

5. Conclusion

5.1 Conclusion

This study has systematically examined the evolving nature of internet financial crime, critically analysed the gaps in China's current legal framework, and drawn instructive lessons from the United Kingdom's regulatory approach. The findings compellingly demonstrate the urgent need for specialised internet financial crime legislation in China through qualitative research combining extensive desk research and in-depth interviews with legal professionals (including lawyers and judges) and focus group discussions.

The UK's Financial Services and Markets Act (FSMA) offers valuable insights, particularly its principles-based regulatory approach, dynamic rule-making mechanisms (e.g., Section 24), and regulatory sandbox provisions. These elements could be strategically adapted to China's context to create a more responsive and effective legal framework. Based on these findings, this study proposes the Draft of the Internet Financial Crime Law of the People's Republic of China.

Internet Financial Crime Law of the People's Republic of China

Table of Contents

Chapter I General Provisions

Article 1: This law is enacted to protect national financial security, maintain the order of the Internet financial market, crack down on Internet financial criminal activities, punish Internet financial criminal activities by law, and safeguard the legitimate rights and interests of citizens, legal persons, and other organizations.

Article 2: The term "Internet finance" as used in this law refers to financial activities carried out using Internet technology, including but not limited to online lending, equity crowdfunding, Internet payment, Internet insurance, etc.; the term "Internet financial platform" as used in this law includes but is not limited to Internet payment, peer-to-peer online lending, equity crowdfunding, and other financial service institutions.

Article 3: The term "Internet financial crime" as used in this law refers to using Internet technology to conduct illegal fund-raising, financial fraud, money laundering, and online infringement of financial information in violation of relevant national financial laws and regulations.

Article 4: Internet financial criminal activities seriously endanger national economic security, financial order, and social stability and should be cracked down by the law.

Article 5: The state shall implement the principle of combining prevention, crackdown, and punishment of Internet financial criminal activities by law.

Article 6: The state implements the principles of unified leadership, division of labor and

collaboration, classified management, and comprehensive management in the work related to combating Internet financial crime.

Article 7: Internet financial platforms shall strengthen internal management, implement anti-money laundering, anti-fraud, and other systems and measures, and prevent and combat Internet financial criminal activities.

Article 8: Any unit or individual shall abide by laws and regulations, be honest in Internet financial activities, and shall not engage in fraud, false propaganda, or other illegal activities.

Article 9: The state encourages and supports scientific and technological innovation, promotes the healthy development of the Internet financial industry, and at the same time strengthens supervision and management of the Internet financial field.

Article 10: The state establishes and improves Internet financial risk prevention and control mechanisms, strengthens information disclosure and risk warnings, and improves investors' risk awareness and prevention capabilities.

Article 11: The state shall strengthen the supervision of Internet financial platforms, establish and improve an emergency response mechanism for Internet financial risks, and handle Internet financial risk events promptly and effectively.

Article 12: The state encourages financial institutions and technology companies to cooperate to promote technological innovation in Internet finance and enhance the inclusiveness and convenience of financial services.

Article 13: The state encourages and supports the construction of self-regulatory organizations in the Internet financial industry and strengthens the self-regulatory supervision and service functions of industry associations and organizations.

Article 14: The state strengthens the training and management of employees in the Internet financial industry and improves the professional quality and risk prevention awareness of employees.

Article 15: The state supports and encourages Internet financial industry associations, social organizations, etc. by law to carry out publicity, education, and training activities on Internet financial crime, implement public awareness plans, improve the public's ability to identify Internet financial crime, and educate the public on the prevention of Internet financial crime.

Article 16: Implement a reporting reward and reporting protection system for Internet financial crime by law.

Article 17: The state implements an information disclosure system for Internet financial criminal activities by law and promptly publishes the investigation and handling of Internet financial crime cases and typical cases.

Chapter II Illegal Fund-raising Crime

Article 18: Anyone who illegally absorbs public deposits or illegally issues securities or bonds for illegal fund-raising using Internet platforms or other network technologies, which constitutes the crime of illegal fund-raising, shall be subject to investigation for criminal liability by law.

Article 19: Using Internet platforms to fabricate false projects, publish false information, false propaganda, promise high returns, and other means to attract investment or loans from others and induce others to participate in illegal fund-raising activities constitutes the crime of illegal fund-raising and shall be investigated for criminal responsibility by law.

Article 20: Anyone who violates national laws and regulations, establishes illegal financial institutions without approval, and engages in financial business activities through Internet platforms or other network technologies, which constitutes an illegal fund-raising crime, shall be investigated for criminal responsibility by law.

Article 21: Organizations and individuals who participate in illegal fund-raising criminal activities shall be held criminally responsible by the law, and their illegal gains shall be recovered.

Chapter III Internet Financial Fraud Crime

Article 22: Using the Internet and other information technology means, for illegal possession, by fabricating facts, concealing the truth, and other means, to commit fraud and fraud on the Internet financial platform to defraud citizens, legal persons or other organizations of property, which constitute Internet finance Anyone who commits a fraud crime shall be held criminally responsible by the law.

Article 23: Using false information and illegal means to harm the currency management system, harm the establishment and management system of financial institutions, harm the deposit and loan management system of financial institutions, harm the customer and public fund management systems, harm the management system of financial instruments and securities, endanger the securities and futures management system, endanger the foreign exchange management system, etc., which disrupts the order of the financial market, damages the legitimate rights and interests of others, and constitutes a crime of financial fraud shall be investigated for criminal liability by law.

Article 24: Concerning the use of Internet technology to commit financial fraud, crackdowns should be intensified by law to protect the legitimate rights and interests of citizens, legal persons, and other organizations.

Chapter IV Money Laundering Crime

Article 25: The act of using the Internet and other information technology means to transfer, transform, conceal, or disguise the source, nature, purpose, etc. of illegal gains shall constitute the crime of Internet money laundering and shall be investigated for criminal liability by law.

Article 26: The act of disguising illegal income as legitimate income through fictitious

transactions, fictitious business, and other means constitutes the crime of Internet money laundering and shall be investigated for criminal liability by law.

Article 27: Individuals and organizations that commit money laundering in the field of Internet finance shall be held criminally responsible by the law, and their illegal gains shall be recovered.

Chapter V Crimes of Infringement of Financial Information

Article 28: Anyone who uses Internet technology to illegally obtain, tamper with, delete, or disseminate financial information, harms the security of financial information systems, disrupts the order of the financial market, and harms the legitimate rights and interests of others, thereby constituting a crime of infringement of financial information, shall be investigated for criminal liability by law.

Article 29: Regarding criminal infringement of financial information, technical prevention, and supervision should be strengthened to ensure the security of financial information and maintain the order of the financial market.

Chapter VI Regulatory Agencies and Their Responsibilities

Article 30: The State Council's banking regulatory agencies, securities regulatory agencies, insurance regulatory agencies, and other financial regulatory agencies shall supervise and manage the Internet financial market by law and strengthen the crackdown on Internet financial crime.

Article 31: The banking regulatory agency of the State Council is responsible for issuing regulatory regulations for the Internet financial industry and organizing the implementation of relevant regulatory measures.

Article 32: The banking regulatory agency of the State Council is responsible for filing and registering Internet financial platforms and conducting regular inspections and evaluations.

Article 33: The Banking Regulatory Authority of the State Council is responsible for early warning and prevention of risks existing in the Internet financial industry and issuing risk warnings promptly.

Article 34: The banking regulatory agencies, securities regulatory agencies, insurance regulatory agencies, and other financial regulatory authorities under the State Council shall promptly investigate and deal with Internet financial crime discovered and take corresponding measures by law.

Chapter VII Censorship

Article 35: The state establishes an Internet financial crime review system, and the banking regulatory agency of the State Council conducts a formal and substantive review of suspected Internet financial crime and takes necessary disposal measures by law.

Article 36: Internet financial platforms shall cooperate with law enforcement agencies in the

review of Internet financial crime and provide relevant information through laws and regulations.

Chapter VIII Law Enforcement and Investigation

Article 37: State agencies should establish and improve Internet financial crime law enforcement agencies and strengthen the investigation and crackdown on Internet financial crime.

Article 38: Internet financial crime law enforcement agencies shall carry out relevant technical investigations, evidence collection, and other work by law and ensure the legality and impartiality of the investigation work.

Article 39: Establish a collaboration mechanism among Internet financial crime regulatory agencies, Internet financial crime law enforcement agencies, Internet financial industry associations, social organizations, financial institutions, and technology companies to strengthen information sharing and cooperative investigations of Internet financial crime.

Article 40: For clues about suspected Internet financial crime, Internet financial crime law enforcement agencies should promptly investigate and protect the legitimate rights and interests of whistleblowers under the law.

Chapter IX Protection of Investors' Rights and Interests

Article 41: Internet financial platforms should strengthen risk warnings and education for investors and improve investors' risk awareness and prevention capabilities.

Article 42: Internet financial platforms shall establish and improve investor suitability management systems to ensure that investors' legitimate rights and interests are not infringed upon.

Article 43: Internet financial platforms should strengthen the review and disclosure of investment projects, provide true, accurate, and complete information, and protect investors' right to know.

Article 44: Internet financial platforms shall establish and improve complaint-handling mechanisms, handle investor complaints promptly and effectively, and disclose the results of complaint handling to investors.

Chapter X Legal Responsibilities and Punishments

Article 45: Units and individuals who violate the provisions of this law and engage in or participate in Internet financial criminal activities shall be given severe criminal penalties by the law and shall be held criminally responsible.

Article 46: Those who use Internet technology to commit Internet financial crime shall be investigated for criminal liability by the law.

Article 47: The state may recover and confiscate illegal gains from Internet financial crime by

law, hold individuals and units involved in crimes criminally responsible, and impose fines, confiscate illegal gains, and other penalties.

Article 48: The state implements strict legal accountability for Internet financial crime by the law, protects the legitimate rights and interests of citizens, legal persons, and other organizations, and maintains financial market order and social stability.

Article 49: For participants in Internet financial criminal activities, the state may, based on their positive performance after committing the crime, take measures to reduce penalties or provide leniency to encourage them to reform and actively repent.

Chapter XI Supplementary Provisions

Article 50: If the relevant management and responsibility systems involved in anti-Internet financial crime work are not stipulated in this law, the "Criminal Law of the People's Republic of China", the "Cybersecurity Law of the People's Republic of China", the "Personal Information Protection Law of the People's Republic of China", the "Anti-Money Laundering Law of the People's Republic of China", and other relevant legal provisions.

Article 51: This law shall come into effect on the date of promulgation.

5.2 Future Research Directions

This study lays groundwork for understanding China's internet financial crime legislation, while pointing to key future research directions: quantitative surveys of diverse stakeholders (FinTech firms, regulators, consumers) to validate findings; comparative analyses of frameworks like the EU's MiCA or Singapore's Payment Services Act; longitudinal studies of reform implementation; and interdisciplinary collaborations combining legal, technical, and economic expertise to develop AI-driven fraud detection and blockchain analytics solutions. These approaches would strengthen China's regulatory framework while addressing global challenges in combating evolving financial crimes.

Acknowledgments

This study was helped by Dr. Hanna Binti Ambaras Khan and Prof. Suhaimi Bin Ab. Rahman. I would like to express my sincere gratitude for their guidance and support throughout the study process. Their invaluable input and expertise have greatly contributed to the success of this paper.

Authors contributions

Xinxin Mao was responsible for study design, revising, and data collection, and drafted the manuscript. Dr. Hanna Binti Ambaras Khan and Prof. Suhaimi Bin Ab. Rahman revised it. All authors read and approved the final manuscript.

Funding

Not applicable.

Competing interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Informed consent

Obtained.

Ethics approval

The Publication Ethics Committee of the Macrothink Institute.

The journal's policies adhere to the Core Practices established by the Committee on Publication Ethics (COPE).

Provenance and peer review

Not commissioned; externally double-blind peer reviewed.

Data availability statement

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

Data sharing statement

No additional data are available.

Open access

Copyrights

References

Ahmad, Z., Khan, A. A., & Burki, A. K. (2024). Financial Sustainability in Emerging Markets: The Role of Fintech, Risk Management, and Operational Efficiency. *Contemporary Journal of Social Science Review, 2*(04), 339-353. https://contemporaryjournal.com/index.php/14/article/view/61.

Amjad, R. M., Rafay, A., Arshed, N., Munir, M., & Amjad, M. M. (2021). Non-linear impact of globalization on financial crimes: A case of developing economies. *Journal of Money Laundering Control. Advance online publicatio*n. https://doi.org/10.1108/JMLC-03-2021-0023

Bankova, D. (2021). *About the challenges of cybercrime in the digital age. Годишник на УНСС, 2*(2), 109-116. https://doi.org/10.37075/YB.2021.2.08

Chen, L., & Davies, M. (2023). Regulatory Sandboxes: Global Adoption Patterns. *Harvard Business Review.*

China Internet Network Information Center. (2023, March 23). CNNIC: The 51st Statistical Report on the Development Status of the Internet in China (full text)". Netscape. https://www.100ec.cn/detail--6625554.html

China Internet Network Information Center. (2023, August 28). *The 52nd "Statistical Report on China's Internet Development Status."* The 52nd "Statistical Report on China's Internet Development Status"--Internet Development Research. https://www.cnnic.net.cn/n4/2023/0828/c88-10829.html

China Internet Network Information Center. (2024, March 22). *The 53rd "Statistical Report on China's Internet Development Status."* The 53rd "Statistical Report on China's Internet Development Status"--Internet Development Research. https://www.cnnic.net.cn/n4/2024/0322/c88-10964.html

Dullien, S., Kotte, D. J., Marquez, A., & Priewe, J. (2010). *The financial and economic crisis: Of 2008-2009 and developing countries.* United Nations.

Haddad, C., & Hornuf, L. (2019). The Emergence of the Global FinTech Market: Economic and Technological Determinants. *Small Business Economics 53*(1), 81-105. https://doi.org/10.1007/s11187-018-9991-x

Hasibuan, E. (2022). *Legal protection of consumer personal data in e-commerce transactions during the COVID-19 pandemic.* Proceedings of the 4th International Conference on Indonesian Legal Studies, ICILS 2021, June 8-9 2021, Semarang, Indonesia. https://doi.org/10.4108/eai.8-6-2021.2314335

Legislation.gov.uk. (2020). *Financial Services and Markets Act 2000.* https://www.legislation.gov.uk/ukpga/2000/8/contents

Li, L., & Yi, H. (2019). The effect of public trust in the justice system on crime: Evidence from the China household finance survey. *China Economic Review, 53*, 305-323.

Liu, X. Q. (2022). *Internet Financial Crime Research.* Shanghai Ren Min Press.

Ma, H. (2023). *China's cross-border e-commerce exports grew by 11.7% last year - Widening the channel for "Made in China" to go abroad.* https://www.gov.cn/xinwen/2023-02/28/content_5743576.htm (accessed 12 May 2023).

Ma, L., & Li, B. (2018). Analysis of the Framework of China's Cybercrime Legislation. *Journal of High Technology Law, 18*(2), 153-181.

Maimon, D., & Louderback, E. (2019). Cyber-Dependent Crimes: An Interdisciplinary Review. *Annual Review of Criminology, 2*, 191-216. https://doi.org/10.1146/annurev-criminol-032317-092057

Manika, B., Shivani, G., &Pankaj S. (2020). Web-Based Classification for Safer Browsing. https://doi.org/10.1007/978-981-15-6876-3_9

Mao, X. X., Hanna, K. A., & Suhaimi, R. A. (2023). Internet financial crime security prevention and criminal law regulation optimization path. *Russian Law Journal.* https://russianlawjournal.org/index.php/journal/article/view/1601

Minutes of the Symposiums of the Supreme People's Procuratorate on Issues Concerning Handling Internet-Related Financial Crime Cases. (2017). *Chinalawinfo Database.* http://www.lawinfochina.com/display.aspx?id=24156&lib=law (accessed 12 May 2023).

Morales, R. (2020). *Service Innovation in Manufacturing: Co-Creating Value in the UK Defence Industry through Partnering.* https://doi.org/10.17863/CAM.59136.

MSG Management Study Guide. (2023). *Desk Research - Methodology and Techniques.* https://www.managementstudyguide.com/desk-research.htm (accessed 12 May 2023).

Muktar B., & Marie G. (2020). Routine Activity Theory and Cybercrime Investigation in Nigeria: How Capable Are Law Enforcement Agencies? *Rethinking Cybercrime,* 40-42.

Khaled, M. I. (2022). *Manifestations of Criminal Protection of the Right to be Forgotten.*https://repository.nauss.edu.sa/handle/123456789/67129

National People's Congress. (1997). *Criminal Law of the People's Republic of China - China Law Retrieval System - pkulaw. "China Law Retrieval System".* https://law.pkulaw.com/falv/29dd76714a5cc235bdfb.html (accessed 12 May 2023).

National People's Congress. (2016). *Cybersecurity law of the People's Republic of China (effective June 1, 2017).* https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/ (accessed 12 May 2023).

National People's Congress. (2020). *Criminal Law of the People's Republic of China - China Law Retrieval System - pkulaw. China Law Retrieval System.* https://law.pkulaw.com/falv/29dd76714a5cc235bdfb.html

OECD (2024). *Global Crypto-Asset Reporting Framework.* Paris: OECD Publishing. https://doi.org/10.1787/578052ec-en

Ren, S. (2020). The legal regulation of Internet financial crime in China. *Journal of Financial Crime. 27*(2), 499-512.

Sibinnuosha & Chen, L. (2019). *Ethics.* Beijing Jin Cheng Press.

Tsai, S., Shen, C., Song, H., & Niu, B. (2019). *Green Finance for Sustainable Global Growth.* IGI Global. https://doi.org/10.4018/978-1-5225-7808-6

Wang, L., & Zhou, Y. (2021). Internet financial fraud and economic risk: Empirical evidence from China. *Journal of Applied Statistics, 48*(2), 317-339.

Wang. (2018). The transformation of financial crime and criminal regulation in the Internet financial era. *Contemporary Law, 3*, 29-39.

World Bank (2023). *Digital Enforcement Mechanisms.* Washington, DC.

Yin, R. K. (2016). *Qualitative research from start to finish.* Guilford Press.

Zeng, Z., Chen, Y., Zhu, S., & Gupta, D. (2017). A Deep Learning Framework for Credit Card Fraud Detection. *IEEE Transactions on Neural Networks and Learning Systems, 29*(3), 881-893.

Zhang, W. (2019). The Challenges of China's Emerging Digital Economics. *China Economic Journal, 12*(3), 233-247.

Zheng, Y. (2023). AI Manipulation in Financial Markets. *Journal of Fintech Security.*

Zhu, Y., & Lu, J. (2023). Fintech, banking and monetary policy transmission. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.4353645 (accessed 12 May 2023).