INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 14, Issue 11, (2024) E-ISSN: 2222-6990

Dilemmas and Solutions for Chinese Lawyers in Defending Internet Financial Crime

[1]Mao Xinxin, [2]Hanna Binti Ambaras Khan, [3]Suhaimi Bin Ab Rahman

[1]School of Business and Economics, Universiti Putra Malaysia, Jalan Universiti 1, 43400, Serdang, Selangor, Malaysia, [2]Senior Lecturer, School of Business and Economics, Universiti Putra Malaysia, Jalan Universiti 1, 43400, Serdang, Selangor, Malaysia, [3]Professor, School of Business and Economics, Universiti Putra Malaysia, Jalan Universiti 1, 43400, Serdang, Selangor, Malaysia

Email: gs64631@student.upm.edu.my, hanna@upm.edu.my, suhaimiabrahman@upm.edu.my

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v14-i11/23495 DOI:10.6007/IJARBSS/v14-i11/23495

Published Date: 02 November 2024

Abstract

Conventional financial services and the Internet are increasingly intertwined, and Internet financial markets are emerging, resulting in an escalation in both the occurrence and diversity of Internet financial crime. Internet financial crime poses a significant challenge to lawyers in China. This paper aims to study the challenges faced by lawyers in dealing with Internet financial crime in China. Thereafter, this paper suggests making the specialised legislation to better address Internet financial crime. This paper adopts qualitative methodologies, such as desk research and in-depth interviews, in which the respondents are 5 lawyers. The findings indicate that lawyers in China face challenges with Internet financial crime, including the insufficiency of existing related legislation, challenges in prosecution, and the necessity to make the Internet Financial Crime Law of the People's Republic of China.

Keywords: Internet Financial Crime, Legislation, Challenge, Lawyer

Introduction

The surge of Internet financial crime in China has presented formidable hurdles for lawyers addressing these intricate cases. With the rapid progression of technology and the growing interconnectedness of global economic networks, cybercriminals have exploited digital platforms to execute a diverse range of fraudulent schemes, encompassing phishing scams, identity theft, online investment fraud, and money laundering. The pivotal role of lawyers in

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

combating Internet financial crime involves navigating the complex legal terrain to advocate for victims and ensure accountability for perpetrators. This study seeks to delve into the multifaceted challenges confronted by legal professionals in tackling Internet financial crime in China and to recommend potential enhancements to the existing legal framework.

The Connotation of Internet Financial Crime

Finance encompasses the movement and management of monetary resources (Liu, 2020). Economically, it encompasses currency circulation, credit activities, and related economic transactions, categorically falling under distribution within modern economic frameworks (Liu, 2020). The conceptual scope of finance typically includes currency issuance and withdrawal, deposit absorption and payment, loan issuance and recovery, as well as securities issuance, subscription, and transfer, among others (Liu, 2020). Since its inception, finance has been integral to driving societal economic development, serving as a nation's economic backbone and the essence of its social economy (Wu, 2018). Financial services such as savings, loans, payments, stocks, and insurance pervade various aspects of human existence, constituting a fundamental aspect of wealth distribution (Liu, 2022). Moreover, finance not only acts as a wealth distribution hub but also serves as a nexus for risks, encompassing credit, foreign exchange, cash, and payment-related risks, which have become systemic in nature (Liu, 2022).

The advent of the Internet era, characterized by connectivity, advanced technology, and globalization (Wang, 2018), has transformed cyberspace into a breeding ground for Internet financial crime, with the internet serving as a catalyst for its proliferation (Xie, 2022). Cyberspace has evolved into a crucial platform for societal activities, where online actions can transcend into tangible real-world consequences, exemplifying the “butterfly effect” between virtual and physical realms (Xie, 2022). Even seemingly minor keystrokes on a computer keyboard within cyberspace can precipitate significant outcomes in the real world, blurring the boundaries between virtual and tangible realms (Xie, 2022). Consequently, cyberspace has transitioned from being purely virtual to an indispensable component of real-world society, progressively diminishing its virtuality (Xie, 2022).

As the economy advances and the internet becomes increasingly pervasive, the incidence of Internet financial crimes is on the rise, fueled by the emergence of new Internet financial markets (Yu, 2023). We now reside in an era characterized by the convergence of the new economy and cutting-edge technology, marked by networking, advanced technology, and globalization (Liu, 2022). In this dynamic landscape, the financial sector witnesses a continuous stream of innovations, giving rise to novel markets, financial products, instruments, and transaction methods, each further segmented within the financial domain (Liu, 2022). Technological advancements drive financial innovation, injecting vigor into the financial market and catalyzing the evolution of financial crimes. Consequently, new methods and types of financial crimes continually emerge, ranging from fraudulent activities and illegal fundraising via online payment platforms, online lending platforms, and third-party payment platforms to manipulation crimes leveraging artificial intelligence technology in securities, futures, and emerging markets (Liu, 2022).

The inadequate supervision of financial innovation results in certain new financial criminal activities operating within legal ambiguities, forming a gray area that challenges financial

management and security, thereby impacting the application of criminal laws (Liu, 2022). Internet financial crime has garnered increasing attention in China, posing a significant threat as evidenced by the escalating number of reported cases (Chen & He, 2021). The prevalence of Internet financial crime creates challenges and risks for businesses operating in the financial sector within China's business environment (Chen & He, 2021). This trend is anticipated to persist in 2023, with criminals continually adopting new technologies and strategies to defraud unsuspecting victims (Wang & Zhou, 2021). The repercussions of Internet financial crime on the Chinese economy are substantial, eroding consumer confidence in the financial system and leading to diminished investments and slower economic growth (Wang & Zhou, 2021). To mitigate these risks, many companies are proactively investing in cybersecurity measures and collaborating closely with regulatory bodies to ensure compliance with the latest legal requirements (Guo & Zhang, 2020).

The Rise of Internet Financial Crime in China

From August 15 to 16, 2023, the Ministry of Public Security of the People's Republic of China, in collaboration with the Thai Police General Administration, the Myanmar Police Headquarters, and the Ministry of Public Security of Laos, convened a joint launching meeting for a specialized cooperation crackdown in Chiang Mai, Thailand (Yang, 2023). A mutual decision was made to establish a comprehensive coordination center for special operations in Chiang Mai, Thailand, with designated joint action points in areas plagued by rampant cybercrimes. This initiative aims to foster closer cooperation, launch more proactive offensives, and execute more professional actions to effectively combat Internet financial crime and associated offenses (Yang, 2023). Subsequently, on August 22, the Chinese Ambassador to Myanmar, Chen Hai, convened a tripartite meeting with the Thai Ambassador to Myanmar and the Laotian Ambassador to Myanmar to facilitate communication and coordination in combating cybercrimes within the region (Hu, 2023). The three parties underscored the significance of the joint meeting held by the police forces of China, Thailand, Myanmar, and Laos in Chiang Mai, Thailand, reaching a consensus on initiating specialized cooperative crackdowns on telecommunications and network fraud, cybercrimes, and their associated crimes such as human trafficking, kidnapping, and illegal detention (Hu, 2023). Strengthening coordination among the embassies of the three nations in Myanmar, they pledged support to Myanmar and jointly implemented the agreed consensus, conducting rigorous crackdowns to decisively mitigate the prevalence of related crimes (Hu, 2023).

In 2022, China's procuratorial organs took proactive measures to address Internet financial risks, resulting in the prosecution of 29,000 suspects for financial fraud and disrupting the order of financial management (Peng, 2023). The Supreme People's Procuratorate of the People's Republic of China, in collaboration with the People's Bank of China and other relevant departments, initiated a three-year campaign to combat money laundering crimes, significantly intensifying penalties. As a result, 2,585 individuals were prosecuted for money-laundering offenses, marking a twofold increase compared to the preceding year (Peng, 2023).

In 2023, the procuratorial authorities remained steadfast in safeguarding financial security by formulating 23 procuratorial opinions aimed at promoting and safeguarding high-quality financial development. They intensified efforts to combat financial crimes and prevent and mitigate financial risks. Notably, 27,000 individuals were prosecuted for financial fraud and

crimes against financial management orders, including 18,000 individuals for fund-raising fraud and illegally absorbing public deposits. This concerted effort maintained a rigorous stance against crowd-related financial crimes, prioritizing the recovery of stolen assets and minimizing losses.

Collaborating closely with the State Administration of Foreign Exchange (SAFE), significant progress was made in addressing securities-related crimes, particularly in the prosecution of 10,000 cases involving the illegal absorption of public deposits. Additionally, stringent measures were undertaken to combat foreign exchange-related crimes, with typical cases being issued and crackdowns conducted in tandem with the State Administration of Foreign Exchange. Furthermore, bolstered collaboration with supervisory commissions and public security organs at all levels enhanced anti-money laundering efforts, resulting in the prosecution of 2,971 individuals for money-laundering offenses, reflecting a notable year-on-year increase of 14.9 percent (Jia, 2024).

The Current Legal Regulation of Internet Financial Crime in China

In China, legislation governing Internet financial crime primarily revolves around two key laws: “The Criminal Law of the People's Republic of China” (National People's Congress, 2020) and “The Cybersecurity Law of the People's Republic of China” (National People's Congress, 2024). However, while the Cybersecurity Law acknowledges the realm of finance, it lacks specific legal provisions targeting cyber-financial crimes. Despite efforts to address these gaps, the legislative landscape still struggles to keep pace with the rapidly evolving nature of Internet-based crime.

The “Criminal Law Amendment (Eleventh)” reflects a trend towards stricter penalties for Internet financial crime and provides clearer standards for prosecution (Liu, 2022). Notably, recent criminal legislation adjustments have modified statutory penalties, introduced unlimited fines, and raised the threshold for personal culpability (National People's Congress, 2020). Yet, despite these updates, the laws remain insufficient in effectively combating emerging forms of Internet-based crime.

Academic evaluations underscore the inadequacies of current regulations in addressing the complexities of cyber-financial crimes in China. These deficiencies can be attributed to several factors. Firstly, the absence of specific legal provisions within existing laws creates ambiguity and hampers the prosecution of cyber-financial criminals. For instance, while the Cybersecurity Law acknowledges finance in cyberspace, it lacks detailed regulations pertaining to cyber-financial crimes. Secondly, legislative updates often lag behind technological advancements and evolving cybercrime tactics, leaving existing laws ill-equipped to address novel forms of Internet financial crime. Delays in legislative updates may fail to cover schemes like cryptocurrency fraud or sophisticated phishing scams, making it challenging to identify, prosecute, and penalize perpetrators effectively. Furthermore, even when laws do address Internet financial crime, prescribed penalties may not sufficiently deter offenders or reflect the severity of the offense. Additionally, enforcement mechanisms may be inadequate due to resource constraints, technical limitations, or jurisdictional complexities. Moreover, the intricate nature of Internet financial crime, often involving complex schemes leveraging online system vulnerabilities, presents additional challenges for detection and prosecution. Perpetrators may exploit encryption technologies, anonymity

services, or international networks to evade detection, complicating law enforcement efforts. Lastly, the transnational nature of many Internet financial crime cases exacerbates challenges, as perpetrators, victims, and infrastructure span multiple jurisdictions. The lack of a unified international legal framework and cooperation mechanisms further hinders effective enforcement efforts, impeding timely information exchange and coordination among law enforcement agencies.

Review of Literature

This section examines the current body of research concerning Internet finance and Internet financial crime. With the proliferation of the Internet, the financial sector has undergone significant expansion, leveraging Internet technology to enhance customer services offered by financial institutions. Simultaneously, the financial industry has introduced novel financial profit models to Internet companies (Manika, Shivani, & Pankaj, 2020).

Internet Finance

This section examines the progression of the Internet finance industry and the challenges it faces. In the nascent stages of any industry, rapid growth often outpaces regulatory frameworks, resulting in the accumulation of risks that strain legal systems. The advent of Internet technology has facilitated the integration of finance and the Internet, giving rise to Internet finance, which encompasses various financial activities conducted through online platforms (Liu, 2022). The convergence of finance and the Internet has been propelled by Internet thinking, which emphasizes leveraging Internet technology for data collection, analysis, and real-world application. This mode of thinking is essential in the contemporary era, where the Internet has become indispensable for societal functioning (Zhou, 2021).

The economic foundation for the development of Internet finance stems from the rapid expansion of China's e-commerce sector. With significant growth in online retail sales, cross-border e-commerce, and the digital economy, there has been a surge in demand for efficient online payment solutions, paving the way for the rise of Internet finance (China Internet Network Information Center, 2023). Various financial models, such as third-party payment platforms, peer-to-peer lending (P2P), and crowdfunding, have catalyzed the growth of the Internet finance industry. These innovations have accelerated the integration of traditional financial institutions with Internet businesses, ushering in the era of Internet finance (Ma, 2023). Internet finance offers unparalleled convenience and accessibility, eliminating geographical and temporal constraints. Leveraging Internet technology, Internet finance optimizes financial services through personalized offerings based on extensive data analysis, challenging traditional financial paradigms (Mustafa, 2019).

However, the rapid expansion of Internet finance has brought about a host of challenges. Credit risk is a prominent issue, exacerbated by the virtual nature of online transactions and inadequate credit evaluation systems. Technical security concerns, such as system failures and data breaches, pose significant threats to investors and customers (Wang & Zhou, 2021). Furthermore, the storage of personal data on Internet finance platforms raises privacy concerns, with frequent instances of data breaches compromising users' personal information (Hasibuan, 2022). Fraudulent activities, particularly in P2P lending and crowdfunding, undermine investor trust and financial stability. The lack of investor expertise and the “herd effect” contribute to irrational investment behaviors, perpetuating the cycle of

risk (Ma & Li, 2018). Moreover, the legality of online financial institutions and products remains ambiguous, with inadequate regulatory oversight complicating the determination of their reliability..

Addressing these challenges requires comprehensive regulatory frameworks, robust security measures, and enhanced consumer education to safeguard the integrity of Internet finance and protect investor interests (Bakker & Fiebrandt, 2016).

Internet Financial Crime

Internet financial crime emerges as a byproduct of the ascent of Internet finance, manifesting within the sphere of online financial activities. Perpetrators, leveraging modern communication technologies like online banking, third-party payment platforms, and virtual currency exchanges, exploit regulatory loopholes to disrupt financial stability, thereby necessitating legal intervention (Zhang, 2023).

The rise of Internet financial innovation introduces substantial risks to ongoing financial market reforms and poses a formidable challenge to regulatory oversight. Criminal endeavors within Internet finance, capitalizing on the innovative features of online platforms and financial mechanisms, jeopardize investor asset security and undermine established legal frameworks governing capital markets (Liu, 2022). The proliferation of Internet financial crime closely aligns with the expansion and deepening of financial markets. As the Internet financial market burgeons, instances of financial malfeasance become more prevalent and pronounced (Liu, 2022).

Unlike conventional crimes, Internet financial crime and associated offenses constitute a distinct category of criminal activity. With Internet financial activities assuming a pivotal role in the economy and society, the burgeoning Internet financial market injects vitality into the economy while concurrently introducing new risks in the form of financial cybercrime. Augmenting statutory penalties for Internet financial crime can mitigate its occurrence and uphold the order and security of the Internet financial market (Liu, 2022).

The proliferation of modern technology allows criminals to seamlessly transition traditional crimes into cybercrime, facilitated by devices like laptops, smartphones, gaming consoles, and Internet-enabled televisions (Wang, 2020). Scholars like Morsch (2023), underscore the pressing need to address economic crimes amidst the proliferation and evolution of virtual realms, while Hasibuan (2022), advocates for bolstered Internet financial supervision in China to uphold stability and sustainability. Wang (2019), observes that the rapid evolution of Internet technology reshapes the landscape of financial crimes, with Technology Law striving to address ensuing challenges. Brealey, Myers, Marcus, Mitra, & Gajurel (2020), applie Routine Activity Theory (RAT) to dissect cyber-enabled advance fee fraud in Nigeria, Sharma (2020), emphasizes the imperative of combating cybercrime, and Button and Gee (2019), proposes electronic device monitoring as a deterrent to cybercrime.

The swift evolution of the Internet has ushered in a paradigm shift in traditional financial crimes, now manifesting in network-centric and multi-stakeholder contexts facilitated by emerging digital platforms (Cheng, 2023). However, Cheng (2023), notes that existing criminal

legislation in China fails to adequately address such crimes, which encompass offenses utilizing digital tools like computers and smartphones to illicitly accrue gains.

China has witnessed a progressive escalation in anti-Internet financial crime awareness, evolving from a narrow focus on banking stability to a broader understanding of its impact on market fairness, economic security, and national stability (Wang, 2024). This shift has propelled Internet financial crime to the forefront of national security strategy, both domestically and internationally, necessitating comprehensive institutional design and cooperation frameworks (Wang, 2024).

Scholarly and practical research on financial crime within the digital economy offers diverse perspectives and countermeasures, yet a comprehensive legal framework for addressing Internet financial crime remains elusive (Liu, 2020). In summary, financial activities are pivotal in modern market economies, with Internet finance representing a cutting-edge manifestation of financial activity (Iu & Wong, 2024). Evaluating and deliberating on the features and emerging patterns of Internet financial crime is paramount to safeguarding economic and financial order and averting associated risks for a prosperous economic future.

Internet Financial Crime: Challenges and Risks in China

The rapid development of Internet finance in China has met the growing demand for convenient and efficient financial services. However, this advancement has also brought to light a number of critical issues and risks. As Internet finance continues to evolve, it has become increasingly evident that the industry lacks expertise, standardized systems, and effective regulation (Jian, 2024).

1) Credit Risk Issues

The accessibility of the Internet, particularly through mobile devices, has led to a surge in virtual financial transactions with a broad geographic reach and limited counterparty information. This has resulted in significant information asymmetry and increased the likelihood of unfavorable choices, giving rise to credit risk. The lack of a fully popularized Internet credit system in China has further exacerbated this issue. Without an efficient credit investigation system, Internet financial platforms struggle to fully assess borrower information, leading to heightened credit risk (Ma & Li, 2018). Additionally, concerns about investor credit have emerged, particularly in the context of P2P online lending platforms, where the frequent occurrence of credit risk has raised widespread apprehension (Tsai, Shen, Song, & Niu, 2019).

2) Technical Security Issues

The nature of Internet finance necessitates robust security measures, including advanced technologies such as cloud computing and big data. However, the occurrence of serious system failures or security incidents on Internet financial platforms has resulted in substantial property losses for investors and customers (Haddad & Hornuf, 2019). In some cases, the pursuit of an ideal customer experience has led certain Internet financial platforms to compromise critical review processes, thereby exposing users to security risks.

3) Disclosure of Personal Data

The proliferation of Internet finance has led to the storage of a vast amount of users' personal information on various platforms. The frequent incidents of personal data leakage pose significant risks to users' personal, social, and national security (Hasibuan, 2022).

4) Fraud and Fraud Issues

Instances of false business and fraud are rampant in online financial services, particularly in newer forms of Internet finance such as P2P lending and crowdfunding (Zeng, Chen, Zhu, & Gupta, 2017). The opacity of platform information has allowed perpetrators to distort project benefits and mislead investors with inaccurate information about financing platforms, sources of funds, and their intended use (Maimon & Louderback, 2019). The proliferation of illegal Internet platforms offering unrealistically high returns on investment poses a significant threat to the sustainability of these platforms.

5) Maintenance of Decentralized Investor Interests

The relative novelty of Internet finance in China, coupled with a lack of investment expertise among investors, has made them susceptible to irrational behaviors such as the “herd effect”. Individual investors' limited understanding and ability to accept risks in the realm of Internet finance have further compounded this vulnerability (Ma & Li, 2018).

6) Security Issues of Transaction Information

Internet financial companies rely heavily on vast amounts of data and information for their operations. The transmission of transaction information over the Internet necessitates stringent network security standards (Bakker & Fiebrandt, 2016). In the absence of adequate information protection measures, criminals may exploit user information for illicit activities or leak transaction details for personal gain, resulting in substantial losses for users, customers, and the Internet finance industry as a whole. In extreme cases, this may even lead to the collapse of Internet finance.

7) Legality of the Platform and Products

The emergence of numerous online financial institutions, platforms, and products has raised questions about their legality. The lack of clarity regarding the business scope of new Internet financial institutions has created discrepancies between their actual operations and their initial representations (Muktar & Marie, 2020). Additionally, the absence of an independent regulatory agency dedicated to overseeing Internet finance in China has made it challenging to ascertain the reliability of online financial institutions and products (Hu, 2019).

In conclusion, the development of Internet finance in China has undoubtedly brought about significant benefits for consumers seeking convenient financial services. However, the industry's rapid growth has also exposed numerous challenges and risks that must be addressed through enhanced expertise, standardized systems, and more effective regulation. Failure to address these issues could undermine the long-term viability and trustworthiness of Internet finance in China.

Research Methodology

This study adopts a qualitative research approach, incorporating both desk research and in-depth interviews to delve into the background and challenges associated with Internet financial crime.

Desk research, which involves gathering information from existing sources such as books and journals, was utilized to provide a comprehensive overview of the topic. While desk research is often considered cost-effective, its effectiveness hinges on the researcher's understanding of research methodologies to avoid fruitless use of resources (MSG Management Study Guide, 2023).

Additionally, in-depth interviews were conducted to gain detailed insights from individuals with expertise in Internet financial crime. This research method allows for comprehensive discussions, delving into the subjective experiences, beliefs, and opinions of the interviewees (Yin, 2016).

The qualitative research design employed in this study involved interviewing five lawyers with an average of 9 years of legal practice experience in Henan Province, China (Table 1). Content analysis was used to analyze the interview data, which included both closed-ended and open-ended questions. Ethical considerations were paramount, with respondents informed of the research's purpose and guaranteed confidentiality and the right to withdraw without repercussions (Sibinnuosha & Chen, 2019).

Table 1
Lawyer Respondent Characteristics

Lawyer	Age	Gender	Occupation	Education Level	Experience	Place	Interview Date	Address
Lawyer 1	50	Male	Lawyer	Master of Law	10 years	Law Firm	10-3-2024	Xinxiang City, Henan Province, China
Lawyer 2	45	Male	Lawyer	Master of Law	8 years	Law Firm	10-3-2024	Zhengzhou City, Henan Province, China
Lawyer 3	40	Male	Lawyer	Master of Law	7 years	Law Firm	11-3-2024	Xinxiang City, Henan Province, China
Lawyer 4	48	Male	Lawyer	Master of Law	9 years	Law Firm	11-3-2024	Zhengzhou City, Henan Province, China
Lawyer 5	42	Female	Lawyer	Master of Law	10 years	Law Firm	11-3-2024	Zhengzhou City, Henan Province, China

Through in-depth interviews, participants provide insights into their familiarity with existing legislation, key challenges in prosecuting Internet financial crime, and recommendations for legislative enhancements on Internet financial crime. The qualitative nature of in-depth interviews allows for a comprehensive exploration of the experiences and perspectives of legal professionals, shedding light on the challenges faced by lawyers with Internet financial crime in China.

However, this study,s limitation lies in its focus solely on Internet financial crime in China without comparative analysis with other countries. Moreover, the research scope is confined to Henan Province, and the number of respondents was limited due to time constraints.

Results and Discussion

The first lawyer highlighted that dealing with Internet financial crime cases involves challenges in staying abreast of existing legislation related to financial crime in China. There is also a clear need for more comprehensive laws to regulate Internet financial crime effectively. Among the major challenges in prosecuting such crimes in China are difficulties in gathering digital evidence and navigating cross-border jurisdiction issues. To improve the situation, the lawyer suggested enhancing cooperation among law enforcement agencies, updating laws to cover new forms of cybercrime, and increasing penalties for offenders.

The second lawyer pointed out that handling Internet financial crime cases presents challenges, particularly with familiarity with China's current financial crime and Internet-related legislation, and questioned whether there are sufficient laws to regulate such crimes. The rapid updating of technology and the difficulty in tracking cross-border crimes were cited as major hurdles in combating Internet financial crime. The lawyer believes that improvements can be made by enhancing legislation, strengthening collaboration among law enforcement agencies, and intensifying efforts to combat cybercrime.

The third lawyer mentioned that one of the significant challenges in dealing with Internet financial crime cases is the insufficient familiarity with China's current financial crime and Internet-related legislation. The main challenges China faces in combating Internet financial crime include the need for more flexible and targeted legal responses due to the upgrading of technical means and the diversification of criminal methods. The lawyer recommended improving legislation, such as strengthening the supervision of Internet financial platforms and the network security legal system.

The fourth lawyer emphasized that dealing with Internet financial crime cases presents several challenges, including the complexity of existing legislation related to financial crime and the need for more comprehensive laws to tackle emerging cyber threats effectively. The major challenges in prosecuting such crimes in China include jurisdictional issues, the difficulty in collecting electronic evidence, and the necessity for international cooperation. The lawyer suggested that improvements can be made to the current legislation by increasing penalties for offenders, regulating online financial platforms more effectively, and promoting inter-agency cooperation.

The fifth lawyer identified challenges stemming from the international nature of the Internet, jurisdictional issues, and the anonymity of perpetrators. Major hurdles in prosecuting Internet financial crime in China include the need for specialized technical expertise and the rapid evolution of cybercriminal tactics. To better address these challenges, the lawyer recommended updating laws to include new types of cybercrime, increasing resources for law enforcement agencies, and enhancing international cooperation.

Table 2 sheds light on the situation, revealing that the challenges faced by lawyers with Internet financial crime in China.

1) Familiarity with Legislation

Findings reveal varying levels of awareness among legal professionals regarding the intricacies of laws related to Internet financial crime in China. While some lawyers demonstrate a high level of familiarity with existing legislation, others express the need for continuous education and training to keep pace with evolving cyber threats. This disparity underscores the importance of ongoing professional development and knowledge exchange within the legal community to effectively address Internet financial crime.

2) Challenges in Prosecution

Participants identify major hurdles in prosecuting Internet financial crime, including jurisdictional issues, complex digital evidence collection, and the transnational nature of cybercrimes. Jurisdictional challenges arise due to the borderless nature of the internet, making it difficult to attribute criminal activities to a specific geographic location. Moreover, the collection and authentication of digital evidence present formidable obstacles, requiring specialized expertise and resources. The transnational dimension further complicates prosecution efforts, necessitating enhanced cooperation between law enforcement agencies across jurisdictions.

3) Legislative Improvements

Suggestions for legislative enhancements encompass a broad spectrum, including the introduction of specific cybercrime laws, stricter penalties for offenders, improved data protection measures, and enhanced collaboration between law enforcement agencies and financial institutions. Legal professionals advocate for the development of comprehensive cybercrime legislation tailored to address the evolving tactics employed by cybercriminals. Stricter penalties are proposed to deter potential offenders and hold perpetrators accountable for their actions. Additionally, robust data protection measures are deemed essential to safeguard individuals and organizations from data breaches and identity theft. Collaboration between law enforcement agencies and financial institutions is highlighted as crucial for the proactive detection and prevention of Internet financial crime.

Table 2
Summary of the Feedback Provided by the Lawyers Respondents

No.	Question	Lawyer 1	Lawyer 2	Lawyer 3	Lawyer 4	Lawyer 5
1	Challenges Dealing with Internet Financial Crime Cases	Need for more laws, familiarity with legislation.	Coordination issues, familiarity with laws.	Insufficient familiarity with laws, need for regulations.	Complexity of laws, need for comprehensive legislation.	International nature of internet, jurisdictional issues.
2	Major Challenges in Prosecuting Internet Financial Crime in China	Digital evidence, cross-border jurisdiction.	Technological updates, cross-border crimes.	Technical upgrades, diversified methods.	Jurisdictional issues, electronic evidence collection.	Updating laws for new cybercrime types.
3	Suggestions for Improving Current Legislation	Enhance cooperation, update laws, increase penalties.	Improve legislation, cooperation, combat crimes intensively.	Update laws, improve supervision, enhance legal system.	Increase penalties, regulate online platforms more effectively.	Update laws for new cybercrime types, increase resources.

Conclusion

In conclusion, the study underscores the challenges faced by lawyers with Internet financial crime in China. The results can reflect the urgency to formulate a special legal framework for Internet financial crime in China to effectively combat cyber threats. The recommendations

put forth by legal professionals highlight the need for comprehensive legislative reforms, increased resources for law enforcement agencies, and proactive measures to mitigate the risks posed by cybercrimes. It is imperative for stakeholders, including government authorities, legal practitioners, and regulatory bodies, to collaborate in addressing the multifaceted challenges posed by Internet financial crime. By enhancing legislative provisions, fostering international cooperation, and investing in cybersecurity capabilities, China can bolster its resilience against cyber threats and uphold the integrity of its financial systems.

This research contributes significantly to the existing body of knowledge on Internet financial crime by providing a nuanced understanding of the unique challenges faced by legal professionals in China. It highlights the inadequacies of current legislation and the pressing need for specialized laws tailored to address the complexities of cybercrime in the digital age. By incorporating qualitative methodologies, including in-depth interviews with experienced lawyers, the study offers rich insights into the practical realities of legal practice in this evolving field. Contextually, this research underscores the urgent need for a collaborative approach among legal practitioners, regulatory bodies, and law enforcement agencies to enhance the effectiveness of legal frameworks in combating Internet financial crime. It serves as a foundation for future studies aimed at developing comprehensive strategies and policies that can adapt to the rapid technological advancements and the dynamic nature of financial crimes in China and beyond.

Acknowledgement
This study was helped by Dr. Hanna Binti Ambaras Khan and Prof. Dr. 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.

References

Bakker, S., & Fiebrandt, A. (2016). Law Enforcement Challenges in the Digital Age: International Cooperation Against Cybercrime. Hague Journal on the Rule of Law, 8(02), pp. 241-258.

Brealey, R. A., Myers, S. C., Marcus, A. J., Mitra, D., & Gajurel, D. (2020). Fundamentals of Corporate Finance. McGraw-Hill.

Button, M., & Gee, D. (2019). Financial crime: A beginner's guide. Routledge.

Chen, X., & He, X. (2021). An empirical study of online financial fraud in China's digital economy. Journal of Financial Crime, 28(2), 537-550.

China Internet Network Information Center. (2023, March 23). Netscape. “CNNIC: The 51st Statistical Report on the Development Status of the Internet in China (full text)”, available at: https://www.100ec.cn/detail--6625554.html (accessed 12 May 2023).

Guo, L., & Zhang, Y. (2020). Internet financial crime and regulation in China: A review. Journal of Financial Regulation and Compliance, 28(1), 102-115.

Haddad, C., & Hornuf, L. (2019). The Emergence of the Global FinTech Market: Economic and Technological Determinants. Small Business Economics 53 (1): pp. 81–105. Doi: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.

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.

Hu, S. X. (2023). Embassies of China, Thailand and Laos in Myanmar coordinate to crack down on gambling fraud. China Daily. https://world.chinadaily.com.cn/a/202308/22/WS64e48c5fa3109d7585e4a520.html

Hu, Z. Q. (2019). Theoretical and practical research on illegal fund-raising criminal law's response to illegal fund-raising. Law Press.

Iu, K. Y., & Wong, V. M. Y. (2024). The trans-national cybercrime court: towards a new harmonisation of cyber law regime in ASEAN. International Cybersecurity Law Review, 5(1), 121-141.

Jia, R. X. (2024). Supreme Prosecutor: Procuratorial organs to prosecute 27,000 people for crimes of financial fraud and undermining financial management order in 2023_Supreme People's Procuratorate of the People's Republic of China. Supreme People's Procuratorate of the People's Republic of China. https://www.spp.gov.cn/spp/2024zgjgzbg/202403/t20240308_647937.shtml.

Jian, J. (2024, February 20). Financial Crime Cases Present Five Characteristics. Supreme People's Procuratorate of the People's Republic of China. https://www.spp.gov.cn/spp/llyj/202402/t20240220_643787.shtml.

Liu, X. Q. (2020). Research on Credit Card Crimes. Shanghai People's Press.

Liu, X. Q. (2022). Internet Financial Crime Research. Shanghai People's Press.

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

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

Mao, X. X., Hanna, K. A., & Suhaimi, R. A. (2023, May 11). Internet financial crime security prevention and criminal law regulation optimization path. Russian Law Journal, available at: https://russianlawjournal.org/index.php/journal/article/view/1601 (accessed 12 May 2023).

Morsch, T. (2023). Shadow economies: The financial crisis and European TV crime series. Contemporary European Crime Fiction, 209–228. https://doi.org/10.1007/978-3-031-21979-5_12.

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, pp. 40-42.

Mustafa I. A. Khaled. (2019). Digital Environments and The Provisions of Theft Under Islamic Law. ARAB JOURNAL OF FORENSIC SCIENCES & FORENSIC MEDICINE, pp. 33-35.

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.

National People's Congress. (2024). Cybersecurity law of the People's Republic of China (effective June 1, 2017). DigiChina. https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.

Peng, K. J. (2023). Regulating FinTech: The perspectives of law, economics, and technology (Doctoral dissertation, Universitaet Hamburg (Germany)).

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

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

Wang, Y. (2018). Changes in Financial Crimes in the Internet Era and the Shift in the Criminal Law System. WeChat Public Platform. https://mp.weixin.qq.com/s/ON0P9sRY4FSRHKSis_MggA.

Wang, Y. H. (2024). A brief analysis of the implementation path and system construction of procuratorial organs' participation in Internet legal governance in the digital era. Modern Science and Technology Research, 3(12).

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

Wu, L. (2022). National public security organs cracked 240,000 cases of economic crimes in 3 years, recovering economic losses of 190.5 billion yuan,. China Net News Center. http://news.china.com.cn/2022-05/07/content_78205460.htm.

Xie. (2022). New Model of Internet Finance. New Century Weekly, 24.

Yang, K. Z. (2023). The Police of China, Thailand, Myanmar and Laos launched a Special Joint Operation to Combat Gambling Fraud Syndicates. China Daily.

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

Yu, C. (2023, August 21). Normative Interpretation and Theoretical Reflection on Helping Behavior of Cybercrime to Be Criminalized. Weixin public platform. https://mp.weixin.qq.com/s/59VmCS6nXBO2aM3w-s95pg.

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), pp. 881-893.

Zhang, P. Z. (2023). On Internet Financial Criminal Risk and Crime Prevention. Journal Of Western , 66. https://doi.org/2095-6916(2023)03-0066-04.

Zhou, Q. G. (2021). How to Solve Complex Criminal Law Problem. Peking University Press.