Proceedings of ICILLP 2025 Symposium: Property Law and Blockchain Applications in International Law and Legal Policy
DOI: 10.54254/2753-7048/2025.LD28549

Correcting Judicial Misconceptions Regarding the "Knowing" Element in Payment Settlement-Related Cybercrime Cases Involving Helping Information Network Crime

Yuxin Zhan

Law School, Tiangong University, Tianjin, China
2312610222@tiangong.edu.c

Abstract. In judicial practice concerning the crime of assisting and facilitating information network crimes, cases involving "payment and settlement" scenarios account for the highest proportion. Among these, the determination of the subjective element of "knowing" is the most contentious, directly impacting the distinction between criminal and non-criminal conduct, as well as the delineation between this crime and others. To address these issues, this paper aims to explore corrective measures for judicial determinations of "knowingly" in payment settlement-related aiding and abetting of cybercrime cases. First, guided by the principle of "unifying subjective and objective elements," it proposes establishing precise and operational rules for determining "knowingly" to prevent the crime from becoming a "catch-all." Second, it accurately distinguishes between aiding and abetting cybercrimes and related offenses through comprehensive assessment of multiple factors, including the perpetrator's stage of involvement in the crime. Finally, based on a rebuttable presumption rule, it establishes a "rebuttable presumption" mechanism to prevent the improper expansion of the crime's scope. This provides theoretical support and adjudication guidance for judicial practice while safeguarding citizens' legitimate rights and interests and maintaining the order of online financial activities.

Keywords: Crime of Helping Information Network Crime, Payment and Settlement, Knowing, Rebuttable of Presumption

1. Introduction

With the rapid advancement of information network technology, cybercrime has evolved into a complex, industrialized, and chain-based phenomenon. As a key offense in combating the black and gray industries of cybercrime, the crime of aiding and abetting information network criminal activities is being applied in judicial proceedings with increasing frequency. According to relevant data, since the launch of the "Card Cutting" campaign in 2020, the number of cases involving the crime of aiding and abetting telecommunications fraud has surged, making it one of the most frequently applied criminal charges in China's judicial practice. Among these, payment settlement-

© 2025 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-7048/2025.LD28549

related assistance information crimes, involving critical stages of fund flows, hold significant weight in judicial determinations. "Knowing" as the core element of the subjective component for this offense directly determines guilt versus innocence and delineates distinctions between offenses—making its establishment a challenging and contentious issue in judicial practice.

The "knowledge" element in the crime of payment settlement-related cybercrime cases differs both from the explicit awareness of specific criminal facts in traditional crimes and from the general understanding of typical helping conduct. According to Article 287-2 of the Criminal Law and relevant judicial interpretations, payment settlement activities specifically refer to substantive operations such as fund transfers, cash-outs, and withdrawals that facilitate cybercrimes. The determination of "knowing" must be assessed based on multiple factors including the perpetrator's cognitive capacity, transaction patterns, and profit-making circumstances. However, academic circles have debated the precise meaning of "knowing," with interpretations ranging from "explicit knowledge" to "likely knowledge." Judicial practice faces numerous challenges, potentially leading to either an unduly broad scope of enforcement or the failure to address certain socially harmful behaviors.

In-depth research on the judicial determination of "knowing" in payment settlement-related helping information network crimes holds significant theoretical and practical importance. This paper examines the judicial determination of "knowing" in payment settlement-related helping information network crimes. It summarizes theoretical interpretations of "knowing" and, in light of current judicial practices, proposes a standardized approach for its determination. This aims to provide guidance for regulating judicial application and achieving precise targeting in the judicial practice of combating cybercrime.

2. The implications and controversies of "Knowing" in payment settlement-related helping information network crimes

2.1. Meaning of payment and settlement types

According to Article 287-2 of the Criminal Law and the provisions of the meeting minutes on legal application issues in the "Card Cutting" campaign, "Where a person knowingly provides technical support such as internet access, server hosting, network storage, or communication transmission to facilitate another person's use of information networks for criminal activities, or provides assistance such as advertising promotion or payment settlement, and the circumstances are serious, the offender shall be sentenced to fixed-term imprisonment of not more than three years or criminal detention, and shall also be fined or be subject to a fine alone." Where a credit card rented or sold by the perpetrator is used to receive funds from telecommunications network fraud, it shall not be deemed an act of "payment settlement" if the perpetrator did not engage in actions such as transferring funds on behalf of others, cashing out, or withdrawing cash, or did not provide verification services like facial recognition to facilitate others' fund transfers, cashing out, or cash withdrawals. This delineates the criminal law concept of payment settlement. Simply renting or selling bank cards without participating in transfer, cash-out, or similar operations does not constitute payment settlement activities. However, if the perpetrator further engages in transfers, cash-outs, or provides facial recognition verification, and the circumstances are serious, it may constitute the crime of helping information network crime.

DOI: 10.54254/2753-7048/2025.LD28549

2.2. Theoretical analysis of "Knowing" in payment settlement-related helping information network crimes

2.2.1. The implications and controversies of "Knowing"

The academic community holds two distinct theoretical positions: "explicit knowledge" versus "likely knowledge." One view asserts that the crime of helping information network crime requires explicit knowledge based on concrete possibility, thereby excluding "likely knowledge." The other view maintains that "knowledge" in this crime does not necessitate explicit awareness of the specific crime itself, but requires recognition of the illegality of the upstream conduct [1,2]. The point of contention between the two viewpoints lies in whether "Knowing" requires reaching the level of criminal intent or merely recognizing illegality. As pointed out by Langtao Bai, the object of awareness regarding illegality is the prohibitive nature of criminal law. Therefore, "knowing" must encompass a comprehensive understanding of the criminal illegality of the act, rather than merely being aware of administrative illegality [3].

2.2.2. The specific nature of determining "Knowing" in payment settlement activities

As a downstream crime in cybercrime, the payment and settlement process involves a hierarchical division of labor from low to high levels, such as: Card farmers (providing bank cards) → Card dealers (buying and reselling bank cards) → platform operators (establishing payment channels) → the layer of upstream criminals. Among these, "card farmers" primarily profit from selling personal bank cards, often possessing only a vague understanding of upstream crimes—merely recognizing that "selling cards can make money"—and lacking the ability to accurately foresee the criminal activities occurring at higher levels [4]. In practice, when dealing with individuals who have low levels of education and lack legal awareness, one cannot directly infer their "knowing" based solely on the objective factor of "abnormal transaction methods" without considering their cognitive capacity. Such an approach would lead to subjective attribution of guilt.

3. The judicial dilemma in determining "Knowing" in payment settlement-related helping information network crimes

3.1. Improper expansion of the scope of "Knowing"

In practice, the presumption of "subjective knowing" tends to be mechanically applied. For example, in one case, defendant Mouxin Kan lent his bank card and related information to another individual for use. The bank card was subsequently used in telecommunications fraud activities, with payment settlements totaling over 7.37 million yuan. However, defendant Mouxin Kan did not receive any compensation. The court held that Mouxin Kan knew or should have known that lending his bank card to others could potentially facilitate criminal activities such as telecommunications fraud, yet proceeded to lend the card anyway. Therefore, his subjective intent should be deemed as knowing [5]. This case exhibits a misguided tendency to equate "pure card provision" and "small-scale fund transfers" with payment and settlement, mechanically applying the threshold of "payment and settlement amounts exceeding 200,000 yuan." However, directly classifying card provision activities that do not involve fund operations as payment and settlement violates the "substantive assistance" characteristic. This leads to the abuse of the "may have known" standard, equating "should have foreseen" directly with "knowing" [6].

DOI: 10.54254/2753-7048/2025.LD28549

3.2. Confusion with the "Knowing" element in the crime of concealing and disguising criminal proceeds

The distinction between the crime of helping information network crime and the crime of concealing or disguising criminal proceeds is unclear. For example, in one case, Pan, Wang I, Tian, and others knowingly collected bank cards to facilitate fund transfers for upstream crimes despite being aware that others might use information networks to commit crimes. Wang II provided his bank cards and other information to others for use while accompanied by others and cooperated in the transfers [7]. The primary court ruled that existing evidence failed to prove the four defendants subjectively knew they were transferring illicit funds, thus convicting them of helping information network crime. However, following the prosecution's appeal, the Shanghai No. 2 Intermediate People's Court, upon review, determined that the four defendants were aware that "money laundering" facilitated the transfer of funds for criminal activities. Consequently, the court overturned the original verdict and convicted them of concealing and disguising criminal proceeds. Both offenses involve the transfer of funds, with the "payment and settlement" conduct under the crime of helping information network crime and the "transfer of criminal proceeds" conduct under the crime of concealing and disguising criminal proceeds exhibiting certain overlaps in their objective manifestations. Additionally, both crimes require the perpetrator to have "subjective knowing." However, the "knowing" in the crime of helping information network crime for purposes refers to knowing or having reason to know that others are using the information network to commit crimes. The "knowing" in the crime of concealing proceeds of crime refers to knowing or having reason to know that the property is the proceeds of crime and the benefits derived therefrom. In practice, it is often difficult to accurately determine whether the perpetrator was subjectively aware of the nature of the funds or the stage of the crime, which has led to confusion between the two offenses.

3.3. Deviations from norms in the practice of "presumed knowing"

The core feature of rebuttable presumption is that it permits the defendant to overturn it with counterevidence [8]. In practice, however, the failure of rebuttal mechanisms has rendered presumptions nearly "final determinations," undermining the very purpose for which presumption rules were established. Article 11 merely stipulates "unless there is contrary evidence," but does not specify the standard of proof required for such contrary evidence. In judicial practice, some courts have imposed excessively high standards on defendants' rebuttals. For example, the defendant claimed that the bank card was not voluntarily provided to upstream criminals but was accidentally lost, and submitted proof of its loss report. However, the court still rejected this defense on the grounds that "it was not proven that there was no criminal intent" and "the defendant should have known" [9]. In essence, this places the entire burden of proof on the defendant, requiring them to "prove their own innocence."

4. Establishing rules for determining "Knowing" in payment settlement-related helping information network crimes

4.1. Adhere to the criterion of unifying subjective and objective elements in determination

Accurately determining the "knowing" element in payment settlement-related helping information network crimes requires a comprehensive assessment based on both objective and subjective factors. This includes the perpetrator's profession, educational background, cognitive abilities, the duration

DOI: 10.54254/2753-7048/2025.LD28549

and methods of providing technical support or assistance, and the extent of profits gained [10]. For instance, the threshold for "Knowing" should differ between financial professionals and the general public. Given their professional background, financial practitioners are more likely to recognize unusual fund movements, so the standard of proof for demonstrating their "general awareness" may be appropriately lowered. Conversely, individuals with lower educational attainment often lack the capacity to assess the "possibility of recognizing illegality," necessitating a stricter standard of proof in such cases.

4.2. Typology of "Knowing"

According to the Opinions on Handling Criminal Cases Involving Aiding and Abetting Information Network Crimes and Related Issues issued by the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security in 2025, the enumerated presumptive circumstances can be categorized as follows:

1. Knowingly Persisting Type: Where the perpetrator continues payment and settlement activities after receiving a report or being subject to restrictions, "Knowledge" may be directly presumed.

2. Transaction Anomaly Type: Based on empirical rules, certain anomalous transaction behaviors are summarized and abstracted to form foundational facts indicating "knowing." For example, cross-provincial transactions involving credit cards and bank cards, or high-value transactions without reasonable justification, constitute anomalous activities that, under the rule of thumb, are typically associated with deliberate criminal intent. Such patterns strongly indicate a high probability of harm to legal interests. In specific cases, they also serve as concrete grounds for individuals to recognize the risk of criminal liability.

3. Investigation Evasion Type: The perpetrator prepares pre-scripted responses or uses encrypted communications to conceal their payment and settlement activities from judicial investigation. In the application of the "willful blindness" doctrine under U.S. criminal law, courts require that defendants take deliberate actions to avoid acknowledging the relevant facts as a condition for establishing "willful ignorance" [11]. In judicial practice, where it has been inferred that a perpetrator possessed specific knowing of the possibility, if they intentionally evade supervision or circumvent investigations, this demonstrates a heightened level of potential awareness and may be deemed as "Knowing" for the purposes of the crime of helping information network crime.

4.3. Distinguishing between the determination of "Knowing" in the crimes of concealing and disguising criminal proceeds

4.3.1. Accurately determine the time point of "Knowing"

The timing of "Knowing" directly impacts the classification of payment settlement-related helping information network crimes. For the crime of helping information network crime, the "Knowing" must arise either before or during the commission of the assisted cybercrime. Where the perpetrator participates in an upstream crime, they possess "Knowledge" of that upstream crime. Furthermore, the concealment of the crime after its commission lacks the requisite element of expectation, failing to meet the constitutive requirements of the crime of concealment. Therefore, it can only constitute the crime of helping information network crime. The crime of concealing and disguising the criminal proceeds requires "Knowledge" arising after the completion of the upstream cybercrime and the acquisition of criminal proceeds and their benefits. When the perpetrator engages in concealment activities such as transferring funds, cashing out, or withdrawing cash after the

DOI: 10.54254/2753-7048/2025.LD28549

upstream crime has been consummated, it can only constitute the crime of concealing proceeds, not the crime of helping information network crime.

4.3.2. Degrees of "Knowing"

The crime of helping information network crime requires factual knowledge that the assisted party's conduct remains uncompleted, and legal knowledge that the conduct is unlawful and the funds are illicit. The crime of concealing and disguising the criminal proceeds requires factual knowledge that the assisted party's conduct has been completed, and legal knowledge that the conduct constitutes a crime and the funds are proceeds of crime [12]. Therefore, in the crime of helping, "Knowingly" refers to a general awareness of the upstream crime—that is, recognizing its illegality suffices. In contrast, the crime of concealing and disguising the criminal proceeds requires the perpetrator to knowingly assist in concealing or disguising funds derived from criminal activities.

4.4. Establish a rebuttable presumption mechanism

The 2019 Interpretation and the 2025 Opinions established the principle of "presumed knowing," stipulating the "unless there is evidence to the contrary" clause, thereby confirming the rebuttable nature of the presumption of knowing in the crime of helping. To examine how "lack of knowing" is determined in judicial practice, conducting a search and analysis of non-prosecution cases, subsequently categorizing the rebuttable scenarios as follows:

1. If the individual lending, renting, or selling credit cards reasonably believes, based on relevant evidence, that the recipient intends to use them for legitimate purposes, such as applying for high-limit credit cards, increasing credit limits, or fulfilling work requirements. It is inappropriate to conclude that they were aware of the recipient's use of information networks to commit crimes.

2. Where the lender and borrower of a credit card share a familial, personal, or romantic relationship—and where the lending occurs based on general trust between them—a cautious and comprehensive approach should be taken in determining whether the lender acted with "knowing" of the circumstances.

3. The "knowing" required for the crime of helping does not encompass situations where knowing is acquired after the fact. If the perpetrator can prove that they only became aware afterward that the person they assisted might be involved in criminal activity, this precisely demonstrates that they were unaware at the time of providing assistance. Consequently, they lack both the subjective intent to commit a crime and the intent to participate in a joint criminal enterprise.

5. Conclusion

The judicial determination of "knowing" in the Payment settlement-related cybercrime cases involving helping information network crime constitutes a critical component in combating cybercrime and safeguarding citizens' lawful rights and interests. Its core lies in accurately defining the boundaries of subjective cognition to prevent improper expansion of criminal penalties or the creation of "catch-all" charges resulting from flawed determinations. From a judicial practice perspective, current cases involving this category face challenges such as the improper expansion of the scope for establishing "Knowing," confusion with the "Knowing" required for concealing and disguising criminal proceeds, and irregularities in the presumption of knowledge norms. These issues fundamentally stem from misinterpretations of the essence of "Knowing," imbalances in the

DOI: 10.54254/2753-7048/2025.LD28549

standards for determining subjective and objective elements, and deficiencies in rebuttal pathways within the presumption mechanism. To address this, it is necessary to establish a recognition method that unifies objective and subjective principles. On the one hand, meticulously categorizing different scenarios of "Knowing" in payment and settlement contexts enhances case precision. On the other hand, strictly distinguishing these scenarios from the crime of concealing and disguising criminal proceeds prevents confusion in the application of criminal charges. Furthermore, the rebuttable presumption mechanism must be activated, with the evidentiary standard for the defendant's rebuttal set at "reasonable doubt." The rationality of the defendant's defense must be thoroughly examined to prevent subjective attribution of guilt. Only in this way can we effectively combat the facilitation of cybercrime in payment and settlement processes, uphold the order of online finance, and simultaneously safeguard the legitimate rights of individuals, thereby achieving the organic integration of criminal punishment and prevention functions.

References

[1] Xiaomin Liu. (2024) Intermediate Pathways for Determining Knowing in the Crime of Assisting Information Network Criminal Activities, Legal Application, Issue 6.
[2] Mingkai Zhang. (2016) On the Crime of Assisting Information Network Criminal Activities, Politics and Law, Issue 2,
[3] Langtao Bai. (2020) The Attribute Debate on the Recognition of Illegality: Premises, Logic, and Legal Basis, Legal Science, Issue 6, .
[4] Zongzhi Long, Jia Hu. (2024) Determining "Knowing" in the Crime of Assisting Information Network Criminal Activities, Journal of Southwest University for Nationalities, Issue 1.
[5] Traditional art often reflects the social background of its time and some important events, Criminal Judgment No. (2023) YI 0104 Xing Chu 889 Qiaoxi District People's Court, Shijiazhuang City, Hebei Province, 2024.3.5, 2025.8.20, https: //wenshu.court.gov.cn/.
[6] Shude Liu, Luoyi Jiang. (2025) Judicial Dilemmas and Solutions in Determining "Criminality" for the Crime of Aiding and Abetting, Journal of the University of Chinese Academy of Social Sciences, Issue 7.
[7] Traditional art often reflects the social background of its time and some important events, Criminal Judgment of the Second Intermediate People's Court of Shanghai (2023) Hu 02 Xing Zhong No. 1016, 2024.2.29, 2025.8.20, https: //wenshu.court.gov.cn/.
[8] Hongqi Wu. (2025) A Regulatory Review and Generalized Correction of the Rules for Determining Knowledge in Aiding and Abetting Crimes, Law Forum, Issue 2.
[9] Traditional art often reflects the social background of its time and some important events, Criminal Judgment No. (2024) Qing 0225 Xing Chu 18 Xunhua Salar Autonomous County People's Court, Qinghai Province, 2025.5.6., 2.25.8.20, https: //wenshu.court.gov.cn/.
[10] Bin Wang, Lu Wang, Pan Chen, Suzhi Wang. (2025) Understanding and Application of the Opinions on Handling Criminal Cases Involving Assisting Information Network Crime Activities, China Applied Jurisprudence, Issue 4.
[11] Justia U.S. Supreme Court Center, Global-Tech Appliances, Inc. v. SEB S.A., 563 U.S. 754 (2011), 2011.5.31, 2025.8.19, https: //supreme.justia.com/cases/federal/us/563/754/.
[12] Dai Xu, Liang Fu. (2025) Judicial Determination of the Crime of Facilitating Information Network Criminal Activities Through Payment Settlement, Journal of Soochow University (Philosophy and Social Sciences Edition), Issue 3.