Proceedings of ICILLP 2025 Symposium: Digital Governance: Inter-Firm Coopetition and Legal Frameworks for Sustainability
DOI: 10.54254/2753-7048/2025.BR26611

Research on the Identification of "Scienter" in the Crime of Assisting Information Network Criminal Activities

Jiatong Ye

School of Law and Sociology, Xihua University, Chengdu, China
2265068324@qq.com

Abstract. The judicial identification of the "scienter" element in the Crime of Assisting Information Network Criminal Activities (hereinafter "the Crime") has long faced problems such as unclear standards, generalized presumptions, and divergent rulings, becoming a core difficulty in the governance of cybercrime. In practice, issues like vague conditions for initiating presumptions, weak evidential support systems, and inconsistent judicial reasoning logic plague the identification of "scienter" in this Crime. These problems stem from ambiguous legislative expression and the lagging nature of evidence rules. To address this, a tiered framework for identifying subjective intent should be constructed, clarifying the boundaries of "scienter" application and evidentiary requirements to form clear identification standards. A quantified scoring index system for electronic evidence should be refined to enhance quantitative assessment capabilities. Systematic training for judicial personnel on technical literacy and practical rules should be promoted. These measures are essential to effectively resolve the judicial identification difficulties of the Crime and safeguard citizens' rights.

Keywords: Crime of Assisting Information Network Criminal Activities, Scienter Requirement, Identification Rules

1. Introduction

With the rapid evolution of digital technology, information network crimes exhibit increasingly concealed and chain-like development trends. Correspondingly, the identification of the "scienter" element in the Crime of Assisting Information Network Criminal Activities faces greater challenges. In judicial practice, while presumption rules alleviate the difficulty of proof caused by a lack of direct evidence to some extent, the unclear boundaries of presumption application and differences in direct evidence standards often lead to significant divergences in adjudication outcomes [1]. Within the ambiguous zone between "should have known" and "could have known," identification standards often vary case by case, increasing the complexity and uncertainty of judging the accessory's subjective knowledge state [2]. Currently, the mainstream academic view generally divides "scienter" into three cognitive levels: "actual knowledge," "should have known," and "could have known." These correspond respectively to the actor's direct cognition of the criminal facts, inferred cognition based on a reasonable duty of care, and a subjective state where the facts should have been foreseeable in the specific context but were not actually recognized [3]. Existing research focuses

DOI: 10.54254/2753-7048/2025.BR26611

primarily on the reasonable boundaries of the presumption mechanism, standards for admitting electronic evidence, and practical manifestations of sentencing disparities concerning these divisions. However, there is a lack of systematic analysis of the logical relationships, application conditions, and evidentiary requirements among these three cognitive forms, leading to significant discretionary space in the application of identification standards [4]. This paper argues that the "scienter" element should be placed under the jurisprudential framework of "knowledge-based intent." A structured evidentiary path should be constructed based on cognitive levels, and identification standards should be refined, evidence rules clarified, and a quantified presumption index system introduced to transform "scienter" from an abstract label into measurable, verifiable judicial content.

2. The connotation of "scienter" in the crime

The "scienter" element in the Crime of Assisting Information Network Criminal Activities is a crucial factor in determining the actor's subjective intent. At both legislative and judicial levels, a unified and clear definition has yet to be formed. The Criminal Law Amendment (IX) established the presumption mechanism for "scienter." Subsequent judicial interpretations further subdivided it into two levels: "should have known" and "could have known." However, the logical structure, application conditions, and order of proof for these two levels lack clear norms in both statutory provisions and judgments, leading to significant divergences in adjudicative practice and overly broad interpretive space [5].

There is significant academic controversy on this issue. Scholars supporting the presumption mechanism argue that cybercrimes are characterized by complex interpersonal chains, concealed criminal operations, and the ease with which data can be deleted. Insisting rigidly on the traditional "direct evidence priority" approach to evidence collection would severely weaken the enforceability of criminal law in cyberspace. Applying presumption rules under specific conditions helps strike a balance between combating crime and evidential difficulties, enhancing judicial efficiency [6]. For example, some scholars point out that reasonably inferring the actor's subjective knowledge state through external indicia such as transaction patterns, account associations, and big data comparisons is an institutional response to the reality of information asymmetry. Cases involving "silent encouragement" in common law jurisdictions also demonstrate that inferring subjective intent based on presence and behavioral context is practically feasible in the absence of explicit statements. Opponents of the mechanism argue that without clear application standards, presumption rules risk sliding into a path where "experience substitutes for legal principle" [7]. Against this backdrop, some scholars propose moving beyond the binary opposition of "presumption vs. non-presumption" and returning to the normative basis of "knowledge-based intent," viewing "scienter" as a structure of subjective cognition [8]. This approach emphasizes balancing judicial efficiency and substantive justice by clarifying the object of "scienter" (i.e., knowledge of the criminal facts) and its degree (whether it reaches the standard of reasonable foreseeability), combined with a dynamic judgment framework utilizing both direct evidence and auxiliary presumptions. Furthermore, scholars advocating a normative path suggest refining the "scienter" identification standards into contextualized operational guidelines and constructing liability determination models categorized by typical types of assistance behavior. This aims to alleviate judicial inconsistency caused by differences in adjudicators' experience [9]. Scholars emphasizing jurisprudential unification propose that systematic judicial interpretations or guiding cases should integrate "actual knowledge," "should have known," and "could have known" into a unified proof structure, establishing corresponding

DOI: 10.54254/2753-7048/2025.BR26611

evidence-matching rules to achieve consistency in identification logic at both jurisprudential and practical levels [10].

Despite differing views on the applicability of the "scienter" presumption mechanism, most studies have reached a preliminary consensus on the following points: First, "scienter" should transcend the assessment of a single subjective state of mind, encompassing the actor's reasonable cognition of the illegality and consequences of the assisted conduct. Second, the presumption mechanism can serve as a supplementary tool when evidence is insufficient, but it must have clear boundaries to prevent abuse. Third, presumption rules and direct evidence should be incorporated into a unified jurisprudential framework, jointly serving the objective identification of the actor's subjective intent and the attribution of responsibility.

3. Analysis of dilemmas and causes in identifying "scienter" in the crime

3.1. Dilemmas in identifying "scienter" in the crime

In the case of Dong Mouwei et al. for the Crime heard by a Hebei court, three defendants provided bank cards successively at the same time and place to participate in fund flows, with "funds involved exceeding 600,000 yuan." The court relied solely on the fact that the "anti-fraud big data platform linked [the cards] to nine fraud cases" to determine that the three had "scienter." However, it sentenced the principal offender, Dong Mouwei, to one year and six months imprisonment with a fine of 20,000 yuan; Wang Mouxian to eleven months imprisonment with a fine of 10,000 yuan; and Fu Mouqi to seven months imprisonment with a fine of 5,000 yuan. The judgment did not explain the differences in the defendants' subjective cognition, nor why similar transaction patterns led to such disparate sentences.In the case of Shi Moujie for the Crime, the defendant applied for multiple bank cards and traveled to another location to complete facial recognition for the principal offender, involving nearly 100,000 yuan. While the court cited direct evidence such as a bank notice and on-site recordings to confirm his "scienter," sentencing him to one year imprisonment with a fine of 5,000 yuan, it failed to explain the application logic distinguishing "actual knowledge," "should have known," and "could have known," or why "could have known" was excluded as a basis for determination.

Comparing these two cases reveals three dilemmas faced by the "scienter" element in practice: First, arbitrary identification. The conditions for initiating presumptions often rely on transaction frequency, associations, or big data prompts. Judges lack quantifiable criteria, easily resorting to experiential intuition to determine subjective intent. Second, inconsistent judgments for similar cases (similar facts, different judgments). Despite highly comparable circumstances and evidence, different trial divisions show significant divergence in assessing accessory liability and sentencing scales, reflecting inconsistent recognition of "scienter" levels and the weight of evidence. Third, insufficient reasoning. Judgments often conclude with generalized statements about "scienter," failing to elaborate on the logic of applying presumption rules or utilizing direct evidence. They also frequently fail to address the defendant's differing understanding of core facts, thus inadequately explaining the basis for identification and boundaries of responsibility to society and the parties involved.

3.2. Analysis of causes for the identification dilemmas

First is legislative ambiguity. While the Criminal Law Amendment (IX) endowed "scienter" with a presumption function, it did not clarify the conditions for initiating presumptions or the types of

DOI: 10.54254/2753-7048/2025.BR26611

admissible evidence, resulting in broad discretion in conceptual application. Subsequent judicial interpretations distinguished between "should have known" and "could have known" as two levels but failed to detail their logical relationship or order of proof. Consequently, judges lack unified operational guidance in handling cases, often relying on experiential judgment or big data prompts for presumptions, leading to high uncertainty in fact-finding.

Second, the lag in the evidence rule system. Electronic data faces technical barriers in collection, preservation, and examination. Existing rules lack quantitative standards for determining the probative value and relevance of new types of evidence like online payment records, communication logs, and platform logs. This results in similar evidence being assigned drastically different probative weight in different courts. Furthermore, presumption clauses are often applied in isolation, detached from the specific evidentiary system, evolving into abstract judgments based on "objective case circumstances," further fostering arbitrariness.

Third, imbalanced judicial mechanisms and insufficient professional resources exacerbate the application difficulties. Courts in developed regions, equipped with relatively complete technical and appraisal conditions, tend to adopt more cautious evidence review approaches. In contrast, courts in central and western regions and at the grassroots level, limited by manpower, equipment, and training, are more prone to falling into a simplified adjudication mode of "use if available," thereby aggravating regional disparities in judgment standards.

Finally, differences in judges' reasoning abilities, technical understanding, and reasoning expression also contribute to inconsistent judicial logic. In the Shi Moujie case, the court formed a relatively complete "should have known" identification path by combining the behavioral chain, duty of notification, and facial verification operations. In contrast, the Dong Mouwei et al. case primarily relied on indirect signs like fund flows and big data prompts to presume "scienter," lacking specific classification and explanation of the subjective levels among different defendants, presenting a judicial structure where facts are similar but reasoning is fractured. Simultaneously, an effective feedback mechanism between academia and practice is lacking. A disconnection exists between research findings and judicial interpretations, preventing timely translation of theoretical results into adjudicative rules and limiting their effect in mitigating identification divergences.

4. Paths for improving the identification of "scienter" in the crime

4.1. Reconstruction of "scienter": actual knowledge, should have known, and could have known

In identifying "scienter" for the Crime, it is necessary to divide the actor's subjective cognition into three levels to balance judicial operability with the principle of proportionality between culpability and punishment. The first level is "actual knowledge", meaning the actor has clear awareness of the information network crime being assisted and its illegal consequences. At this level, evidence often manifests as direct communication records between the actor and the principal offender, written commitments, or direct instructional evidence, requiring a presentation of highly certain subjective intent. This standard should only be applied when the judge can confirm the actor's incontrovertible knowledge of the criminal facts.

Situated between extreme certainty and presumptive ambiguity is "should have known". It uses objective social experience and professional skills as the measuring stick, requiring the actor to fulfill a reasonable duty of care under the same circumstances. This level can rely on objective indicators such as abnormalities in electronic payment flows, frequency of communication exchanges, and the degree of conformity between transaction behavior and criminal activities,

DOI: 10.54254/2753-7048/2025.BR26611

placing the actor in a position where knowledge should reasonably be inferred. In judicial practice, determining "should have known" emphasizes both the objective verifiability of the factual state and the actor's reasonable foreseeability of risks given their specific identity or professional position.Finally, "could have known"serves as a supplementary judgment level to fill the gap between direct evidence and presumed facts. In this scenario, judges can reasonably infer the actor's subjective state of mind based on multi-dimensional clues such as role assignments within a group, habits of using network platforms, and the technical difficulty of tool operations. However, the application of "could have known" must be moderate; it cannot pile up numerous uncertain factors to form the basis of criminal liability, as this easily leads to excessive punishment.These three levels are not isolated but should form a dynamic complementarity during the trial process. When the chain of evidence is clear and direct cognition is provable, the "actual knowledge" standard should be prioritized. When evidence is incomplete but objective signs are strong, conforming to social experience without violating procedural justice, recourse can be made to "should have known." If factual gaps still exist and the case concerns significant public interest or group crime, "could have known" can serve as a last resort. This tiered design respects the subjective differences in actors' perception of facts and provides judges with a structured judgment framework when confronted with complex electronic evidence.

At the implementation level, corresponding situational examples can be added to judicial interpretations, matching typical assistance behavior patterns with each identification level to reduce standard drift caused by differences in judges' backgrounds and experience. This not only helps unify the adjudication scale but also gives defendants a clearer understanding of their risks during the pre-trial stage. In the long term, this layered framework will transform the "scienter" element from an abstract legal provision into refined practice, laying the foundation for accurate attribution of accessory liability and judicial fairness. Synthesizing the jurisprudential debates and level distinctions, and to build a clear bridge between theory and practice, this paper defines "scienter" in the Crime as follows: The actor has a clear understanding of the illegal nature and implementation methods of the information network crime committed by the assisted party and, while still able to fulfill a reasonable duty of care, intentionally commits acts of assistance to facilitate the completion of that crime, constituting a state of subjective intent.

4.2. Clarifying the definition standards for "scienter"

Within the structure of accomplice liability, the "scienter" element points to the actor's subjective intent and also acts as a link between rights protection and the severity of punishment. Firstly, although current legislation and judicial interpretations juxtapose "should have known" and "could have known," they fail to clearly explain their triggering conditions, application boundaries, and interrelationship. This leaves adjudication standards at the conceptual level, lacking practical operability. To address this, it is necessary to add a basic framework for the "scienter" element in the Specific Provisions of the Criminal Law and introduce contextualized guidelines in judicial interpretations based on typical assistance behavior scenarios.

Secondly, "scienter" can be deconstructed into two core components: (1) Clear cognition of the illegal nature and implementation process of the information network crime, used to measure the depth of the actor's understanding of the criminal project itself; and (2) Reasonable anticipation of the harmful consequences, used to judge the timing and psychological intensity of their subjective intent. Only when both components are present can the actor be deemed to possess genuine subjective intent. In situations like fund payment agency, backend operations, or technical circumvention, the existence of communication records, functional descriptions, or foreseeable

DOI: 10.54254/2753-7048/2025.BR26611

consequences can be used to determine the degree of cognition and attribution of liability.Thirdly, the identification of marginal behaviors should also introduce a "reasonable duty of care" standard. For behaviors such as acting as an intermediary or forwarding links, an individual with a certain level of network experience should reasonably be able to recognize the risk of illegality, and thus "should have known" liability should not be easily excluded. Conversely, if the actor clearly lacks relevant knowledge, misjudgment of subjective intent due to generalized presumption should be prevented.Finally, to prevent "scienter" presumption from sliding towards expansion of criminal liability, typical exclusion scenarios should be added to statutory notes, such as providing neutral technical support gratuitously or granting platform permissions incidentally. It should be made clear that presumptions of "scienter" are not suitable for these behaviors. To ensure the implementation of these norms, it is recommended that judicial authorities formulate Scienter Identification Guidelines, compiling typical examples and evidence lists, clarifying types of admissible evidence, and establishing a scoring system for presumption bases. This will promote the formation of a clear and visible judgment framework for "scienter" identification, reducing the subjectivity and uncertainty of judicial discretion.In cases involving the Crime in cyberspace, electronic data has become the core support for identifying the "scienter" element, but the current evidence system has significant deficiencies in collection, preservation, and examination. Therefore, efforts should focus on improving two major types of evidence rules to safeguard procedural justice while maintaining substantive fairness.The first type involves clarifying direct evidence examination standards. Judicial interpretations should establish quantitative requirements for the integrity, traceability, and relevance of common electronic evidence, including chat records, payment flows, system logs, and platform backend reports. For example:Chat records must be preserved in an officially exported format, containing sender, receiver, timestamps, and message hash values, with an authenticity report issued by a third-party appraisal institution.Payment flow data should be provided by the bank as original data files, supplemented with flow serial numbers, statement seals, and electronic signatures.System logs must retain complete change records, ensuring the log chain is intact and unaltered from generation to the trial stage.Regarding the technical means for evidence preservation, it is recommended to introduce blockchain storage and electronic signatures to ensure the immutability and traceability of evidence during extraction, transmission, and storage. A unified electronic evidence preservation process template should be established, requiring investigative, appraisal, and trial stages to follow the same standards to avoid disputes over evidence validity due to format or procedural differences.

The second type involves constructing a quantified index system for presumptive scenarios. Presumption rules should move away from vague expressions like "based on feeling" or "objectively shown by the case." Instead, objective indicators such as the number of fund flows, the proportion of amount involved, and network group access frequency should serve as reference thresholds for initiating "should have known" presumptions. Specifically, judicial interpretations could stipulate:If the same account conducts three or more large transfers (or five or more per week) within 24 hours, and a single transfer accounts for 30% or more of the account's current balance, this may preliminarily establish the situational basis for the accessory to "should have known" about the activity.If the same user accesses the involved network group more than ten times via continuous logins, forwarding instruction texts, or participating in division-of-labor discussions, this may also be regarded as constituting reasonable foreseeability of criminal intent.Such quantitative standards should comprehensively consider differences in crime types and technical environments, and allow higher courts to make appropriate adjustments based on practical needs to maintain the flexibility and stability of the rules.To implement these two types of rules in court proceedings, a "classified

DOI: 10.54254/2753-7048/2025.BR26611

evidence list" should be appended to judicial interpretations or trial guidelines. This list would categorize direct evidence and indirect indicators, assigning a reference score to each piece of evidence or indicator. For example:Chat record authenticity report: 30 points,System log immutability report: 25 points,Fund flow count threshold: 20 points,Group participation frequency: 15 points.When the cumulative score reaches a set standard, it can serve as the basis for initiating a "should have known" presumption. If the cumulative score for direct evidence exceeds a certain critical value, "actual knowledge" can be confirmed. This "score + threshold" model provides judges with an intuitive review framework and enables prosecutors and defenders to clearly grasp the focus of their respective evidence presentation and cross-examination, reducing arbitrary judgments caused by unclear classification or inconsistent standards.Simultaneously, an "evidence mapping" session should be added to the trial procedure. Here, the judge or court assistant maps the electronic evidence and indicators submitted by both parties against the list according to the guidelines, and records the scores and identification conclusions for each item in detail in the trial record. This procedural design helps form a complete explanation of the evidentiary chain, not only strengthening the reasoning power of the judgment but also allowing the parties to understand the court's reasoning, balancing substantive justice and procedural transparency.

4.3. Strengthening professional talent development

Cases involving the Crime entail highly diverse technical details and evidence forms. Judges and prosecutors need composite capabilities encompassing electronic evidence collection methods and jurisprudential reasoning skills. Current in-service training often focuses heavily on legal provisions, lacking systematic teaching on the operation and examination of technical evidence. Therefore, specialized research programs on network assistance information crimes should be established in higher courts or judicial police academies. Course content should cover the extraction and preservation process of electronic evidence, the technical principles of blockchain evidence storage, the use of data analysis tools, and the reproduction of typical cases with simulated trials. The training model could adopt a combination of case-driven learning, scenario simulation, and role-playing, allowing trainees to experience the entire process of evidence classification, evidence challenge, and logical deduction in a simulated environment. Cybersecurity engineers and judicial appraisal experts should be invited to co-teach. Simultaneously, academia and practitioners should engage in regular seminars through platforms like the "Research Association on Liability for Network Assistance Information Crimes" to translate the latest academic research findings into draft judicial interpretations and trial guidance. Higher courts at the provincial level could pilot the selection of exemplary cases, issuing guiding adjudication principles combined with academic recommendations. These typical cases and adjudication rules should be incorporated into a nationally unified case law database, assisting basic-level courts in obtaining timely and authoritative references during trials and promoting the sustainable improvement of "scienter" identification.

5. Conclusion

The identification of the "scienter" element in the Crime of Assisting Information Network Criminal Activities is not only crucial for the precise attribution of accessory liability but also concerns legal predictability, the appropriateness of criminal policy, and the rebuilding of judicial credibility. This paper has discussed the definition of "scienter," the dilemmas in judicial identification, and paths for institutional improvement, attempting to build a logical bridge between abstract jurisprudence and

DOI: 10.54254/2753-7048/2025.BR26611

concrete practice. By clarifying the three-tier cognitive structure of "actual knowledge—should have known—could have known," it advocates for a meticulous division of the actor's subjective state to transform the "scienter" element from a vague label into a refined assessment. The aim is to achieve a balance between jurisprudential rigor and practical operability.

References

[1] Liu Shude, Jiang Luoyi. Judicial Dilemmas and Solutions in the Determination of "Crime" for the Crime of Assisting Information Network Criminal Activities [J]. Journal of the University of Chinese Academy of Social Sciences, 2025, 45(07): 103-118+143-144.
[2] Chen Guanzhi. Controversies in Identifying "Scienter" for the Crime of Assisting Information Network Criminal Activities and the Construction of Regulatory Paths [J]. Forest Police, 2025, (02): 14-18.
[3] Zhao Ruixiang. Normative Reshaping of Judicial Reasoning for "Scienter" in the Crime of Assisting Information Network Criminal Activities: Oriented towards Precise Adjudication and the Principle of Legality [J]. Legal Expo, 2025, (16): 25-27.
[4] Research Group of Beijing No.2 Intermediate People's Court, Jin Xuejun. Judicial Application and Governance Measures for the Crime of Assisting Information Network Criminal Activities in "Two-Card" Cases [J]. Digital Rule of Law, 2025, (01): 103-119.
[5] Lao Dongyan. The Protected Legal Interest of the Crime of Assisting Information Network Criminal Activities J. Legal Forum, 2025, 40(02): 5-16.
[6] Wu Hongqi. Normative Review and Correction of Generalization in the Identification Rules for "Scienter" in the Crime of Assisting Information Network Criminal Activities [J]. Legal Forum, 2025, 40(02): 17-27.
[7] Wang Yanqiang. Research on Issues of Concurrence Related to the Crime of Assisting Information Network Criminal Activities [J]. Legal Forum, 2025, 40(02): 28-41.
[8] Tang Xiner. Analysis of the Path to Refine Judicial Practice for the Crime of Assisting Information Network Criminal Activities [J]. Legal Expo, 2025, (05): 148-150.
[9] Chen Jing, Zhang Yumin. Jurisprudential Analysis and Application Approach for the Crime of Assisting Information Network Criminal Activities [J]. Journal of Dalian Maritime University (Social Science Edition), 2025, 24(01): 37-45.
[10] Wang Chao. An Empirical Study on the Characteristics of Judicial Application of the Crime of Assisting Information Network Criminal Activities [J/OL]. Journal of Henan Police College, 1-14 [2025−08−04]. https://doi.org/10.16231/j.cnki.jhpc.20250205.004.