

电商支付领域刑事电子证据可采性规则研究

陈河志

贵州大学法学院, 贵州 贵阳

收稿日期: 2025年9月13日; 录用日期: 2025年9月26日; 发布日期: 2025年10月28日

摘要

随着电子商务和电子支付的迅猛发展, 电商支付领域的刑事犯罪活动日益增多, 电子证据在该类案件中的关键作用愈发显著。本文聚焦于电商支付领域刑事电子证据的可采性规则, 探讨了该类证据的特殊性、可采性理论基础及其在司法实践中面临的实际问题。通过结合行业实际案例和现行法律法规, 分析了电子证据在真实性、合法性与关联性认定方面的具体困境, 并提出契合电商经济特征的完善建议。研究认为, 应构建适应电商支付业务逻辑的电子证据审查体系, 通过技术规范与法律规则有机结合, 提升电子证据的可采性与证明力。本文旨在为电商支付领域电子证据的司法认定提供理论参考与实践指引。

关键词

电子证据, 可采性, 电商支付, 证据规则, 电子商务经济

Research on the Admissibility Rules of Criminal Electronic Evidence in E-Commerce Payment Field

Hezhi Chen

School of Law, Guizhou University, Guiyang Guizhou

Received: September 13, 2025; accepted: September 26, 2025; published: October 28, 2025

Abstract

With the rapid development of e-commerce and electronic payments, criminal activities in this field have increased significantly, highlighting the critical role of electronic evidence in related judicial proceedings. This paper examines the admissibility rules of criminal electronic evidence in e-commerce payment, discussing its particularities, theoretical foundations, and practical challenges. By analyzing typical cases and current legal regulations, it identifies specific issues regarding the authenticity,

legitimacy, and relevance of electronic evidence, and proposes tailored improvement strategies aligned with the characteristics of e-commerce economy. The study suggests that the admissibility review of electronic evidence should incorporate industry-specific technical standards and legal norms to enhance its reliability and probative value. This paper aims to provide theoretical and practical guidance for the judicial adoption of electronic evidence in e-commerce payment contexts.

Keywords

Electronic Evidence, Admissibility, E-Commerce Payment, Evidence Rules, E-Commerce Economy

Copyright © 2025 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

电子商务与电子支付的深度融合不仅重塑了交易与支付模式，也带来了新型刑事犯罪风险。近年来，我国电商交易规模持续扩大，据商务部发布的《中国电子商务报告(2023)》显示，2023 年全国电子商务交易额已达 48.5 万亿元，同比增长 8.5%，其中电子支付渗透率超过 90%。伴随产业规模扩张，电商支付领域的犯罪活动也呈现高发态势，相关案件数量逐年上升。此类犯罪呈现出技术性强、隐蔽性高、跨区域协作等特征，电子证据因此成为认定犯罪事实的核心依据。学术界对电商支付相关法律问题的研究已形成一定积累。2012 年《中华人民共和国刑事诉讼法》将“电子数据”纳入法定证据类型，为相关司法实践提供了初步法律支撑。此后，《网络安全法》《数据安全法》《个人信息保护法》等法律法规相继出台，逐步构建起电子证据收集、提取与运用的基本规范框架。然而，现有法律框架在面对电商支付领域的复杂场景时仍显不足。电商支付领域的电子证据具有生成主体多元、交易链路复杂、技术依赖度高、数据实时性强等特点，导致其可采性认定在司法实践中面临诸多特殊挑战。

具体而言，电商支付电子证据的可采性问题主要体现在三个方面：一是如何验证多主体参与下电子证据的真实性与完整性；二是如何在复杂的技术环境中确保证据收集程序的合法性；三是如何在海量数据中精准识别与案件事实具有关联性的电子证据。这些问题的解决亟需结合电商支付业务特点进行深入探讨。

本文立足于电商经济发展现状，聚焦电商支付领域中刑事电子证据的可采性问题，系统分析其特殊性、审查标准及现实困境，并结合实际案例和行业特点，提出具有针对性的规则完善路径，以期为司法实践提供参考。

2. 电商支付领域电子证据可采性的理论基础

2.1. 电商支付领域电子证据的特殊性

电商支付领域电子证据是指在电子商务交易和电子支付过程中形成的，以数字化形式存储、处理、传输的，能够证明案件事实的数据。根据这一定义，电商支付领域电子证据主要包括以下类型：电子支付指令、交易记录、资金流水、用户身份认证信息、风险控制日志、跨境支付数据等。

与传统电子证据相比，电商支付领域电子证据具有以下几个显著特征：多主体参与性：电商支付涉及消费者、商户、支付机构、银行、清算组织等多个主体，证据分布分散且相互关联；交易链条完整性：电子支付证据往往形成完整的交易链条，包括交易发起、身份验证、支付授权、资金清算等环节；实时性与高频性：电商支付具有实时处理、高频发生的特点，证据生成速度快、数量大；跨境流动性：跨境电

商支付涉及不同法域，证据可能存储在不同国家或地区的服务器上；监管合规性：支付机构需遵循金融监管规定，形成相应的合规监控证据。

2.2. 电商支付电子证据可采性的内涵

电商支付领域电子证据的可采性是指该领域电子证据能够被法庭采纳为认定案件事实的依据的资格。这是一个法律问题，涉及证据的准入资格。根据我国刑事诉讼法的规定，证据必须具有真实性、合法性和关联性，才能作为定案的根据。因此，电子证据的可采性审查也应当从这三个方面进行[1]。

真实性审查需要重点关注电商支付证据的完整性和不可篡改性。由于支付交易涉及多系统、多环节，需要确保从交易发起、执行到清算的全链条证据完整性。特别是在跨境支付场景下，需要验证不同司法管辖区存储的证据是否一致且完整[2]。合法性审查需要特别关注跨境取证和数据隐私保护的平衡。支付数据包含大量个人敏感信息和商业秘密，收集提取此类证据需要严格遵守《个人信息保护法》《数据安全法》等法律规定。同时，跨境电子证据的提取需要遵循国际司法协助程序或相关国际公约。关联性是指电子证据与案件事实之间必须存在逻辑上的联系，能够证明案件事实的存在或不存在。关联性的审查需要结合案件的具体情况，判断电子证据是否与案件事实相关，以及相关的程度如何[3]。

电子证据的可采性审查是一个复杂的过程，需要综合运用法律知识和技术手段。法官在审查电子证据的可采性时，应当保持开放和谨慎的态度，既不能因为电子证据的技术性而盲目采纳，也不能因为电子证据的易篡改性而一概排除。

3. 电商支付领域刑事电子证据可采性规则的现状与问题

3.1. 现行法律规定

我国目前针对电商支付领域电子证据的可采性规则主要散见于多部法律法规和部门规章中。《电子商务法》《电子支付指引》《非银行支付机构网络支付业务管理办法》等对电商支付数据的保存、提供等方面作出了规定。《刑事诉讼法》及配套司法解释规定了电子证据收集提取的基本规则。

值得注意的是，中国人民银行发布的《金融机构客户尽职调查和客户身份资料及交易记录保存管理办法》规定支付机构应当保存客户身份资料和交易记录至少五年，这为电商支付领域刑事案件的证据获取提供了制度保障。

此外，《网络安全法》《数据安全法》《个人信息保护法》等法律对网络运营者、数据处理者的数据安全保护义务作出了规定，同时也为电子证据的收集提取设置了边界和限制。

3.2. 司法实践中存在的问题

电商支付领域电子证据的可采性认定在司法实践中面临一些特殊问题。首先，跨境电子证据提取困难。电商支付往往涉及跨境交易，证据可能存储在境外服务器上。由于不同法域的数据本地化要求和数据出境限制，侦查机关难以直接获取境外存储的电子证据[4]。虽然《国际刑事司法协助法》提供了跨境取证的法律途径，但程序复杂、耗时较长，难以适应打击电商支付犯罪的紧迫性需求。以 2023 年浙江省杭州市中级人民法院审理的案子为例，该案涉及境内人员通过境外支付平台进行资金结算，关键交易数据存储于新加坡服务器。侦查机关依据《国际刑事司法协助法》向新加坡方面提出取证请求，但整个司法协助流程耗时近 11 个月，严重延误案件审理进度。据最高人民法院司法统计数据显示，2022~2023 年度涉及跨境电子支付的刑事案件中，平均跨境取证周期为 9.6 个月，超过普通刑事案件侦查期限的 2 倍以上。其次，多主体证据协调复杂。电商支付涉及多个参与主体，证据分散在不同的机构系统中。例如，一笔跨境支付可能涉及支付机构、银行、清算组织等多个主体，每个主体只掌握部分证据片段，需要协

调多个机构才能获取完整的证据链条[5]。这不仅增加了取证难度，也影响了证据的完整性和一致性。在上海市浦东新区人民法院 2022 年审理的“电商平台诈骗案”中，为查明一笔虚假交易的资金流向，办案机关需分别向支付宝、微信支付、招商银行及银联等四家机构调取数据，由于各机构数据格式和接口标准不统一，证据整合耗时长达三个月，导致部分关键证据因超出保存期限而灭失。第三，技术标准不统一。不同的支付机构采用不同的技术系统和数据标准，导致电子证据的格式、内容存在差异。这种技术标准的不统一给电子证据的比对、认证带来了困难，也影响了证据的可采性认定。中国人民银行 2023 年发布的《非银行支付机构技术安全管理规范》虽对支付系统技术安全提出要求，但未对数据存储格式、接口标准等作出统一规定。实践中，支付宝、微信支付、银联云闪付等主流支付平台采用各自的数据结构，以交易时间戳为例，有的采用 UTC 时间戳，有的采用本地时间戳，还有的采用自定义时序编号，导致证据比定时经常出现时间偏差[6]。第四，隐私保护与侦查需要的平衡。电商支付数据包含大量个人敏感信息，如身份信息、交易习惯、资金往来等。侦查机关收集提取此类证据时，如何平衡犯罪侦查需要与个人隐私保护，是一个亟待解决的问题[7]。在 2023 年广东省深圳市中级人民法院审理的“第三方支付平台侵犯公民个人信息案”中，侦查机关为取证需要，调取了涉案平台近百万条用户交易记录，但未进行匿名化处理，引发用户集体诉讼。

4. 电商支付领域刑事电子证据可采性规则的完善路径

4.1. 真实性审查的完善

真实性是电子证据可采性的基础。为了保证电子证据的真实性，应当采取以下措施：首先，针对电商支付多系统协作的特点，建立跨平台数据一致性验证机制，要求支付机构、银行和电商平台采用统一的交易流水号和时间戳标准，确保全链路数据可追溯、可比对。例如，可借鉴支付宝与微信支付在大型促销活动中的分布式事务协调方案，实现多系统间数据实时同步与验证。其次，推广区块链技术在电商支付存证中的应用，利用其分布式、不可篡改的特性，为电子证据提供技术保障。目前已有电商平台采用“区块链 + 电子存证”模式，将交易关键信息上链存储，司法机关可通过链上哈希值快速验证证据真实性。最后，制定电商支付电子证据提取专用工具的技术标准，要求取证工具必须支持主流支付平台的 API 接口和数据格式，确保数据提取的完整性和准确性。另外，也应当保证电子数据在复制转移时不会发生变化。在电子证据取证中，对于原始的存储介质运用介质克隆和镜像保存的方法实现的复制不会有任何变化[8]。

第三，引入技术专家辅助人制度。电子证据的真实性审查往往涉及专业的技术问题，法官可能缺乏足够的技术知识来判断。因此，可以引入技术专家辅助人制度，由技术专家对电子证据的真实性提出意见，帮助法官做出准确判断。技术专家辅助人可以是公安机关的技术人员、科研机构的专家学者或者社会上的技术人员。然而，我国技术专家出庭作证率极低，在我国司法实践中，技术专家普遍不出庭作证，技术专家出庭作证的比例一般不会超过 5% [9]。所以在此方面的制度需要进一步完善。

4.2. 合法性审查的完善

合法性是电子证据可采性的保障。通过修订已有的证据法、使其能够将电子证据包含于其中，或者借助规范行业性活动而立法的契机来界定电子证据的概念及采纳、采信等问题，则不失为上策[10]。为了规范电子证据的收集提取程序，应当采取以下措施：首先，结合电商支付业务特点，制定专门的电子证据取证程序规范，明确第三方支付平台在证据提取中的权利义务。例如，规定支付机构应当建立专门的数据协查通道，为司法机关提供标准化数据接口，同时要求侦查人员必须通过双重认证和权限审批才能访问用户交易数据。其次，针对电商支付数据涉及大量用户隐私的特点，建立分层授权机制：对

于基础交易信息，支付机构可在用户协议授权范围内直接提供；对于敏感信息如用户身份资料、生物识别信息等，则需要司法机关出具正式法律文书。某头部支付平台已实施数据分类分级管理制度，为不同类型数据设置不同的取证门槛，这一做法值得推广。最后，建立电商支付领域电子证据合法性审查的负面清单，明确列举通过非法技术手段破解支付系统、未经授权爬取用户数据等取证方式为非法，所获证据不得采纳。

4.3. 关联性审查的完善

针对电商支付领域电子证据的关联性审查，应当采取以下专门措施：首先，针对电商支付交易链路长的特点，建立“资金流 + 信息流”双轨关联分析模式。不仅追踪资金流向，还要分析与之对应的商品流、物流和信息流，构建多维关联证据体系。在一起电商诈骗案中，办案机关通过同时分析支付数据、物流信息和平台评价数据，成功建立了完整的证据链。其次，利用大数据分析技术建立电商交易异常行为识别模型，通过机器学习算法识别虚假交易等可疑行为模式。某第三方支付平台研发的交易风险监测系统，能够实时分析数亿条交易数据，准确识别异常交易模式，为司法机关提供关联性判断参考。最后，制定电商支付领域电子证据关联性认定指南，明确不同场景下的关联性判断标准。例如，对于跨境支付纠纷，要求提供支付机构认证的汇率转换记录和跨境结算凭证；对于会员制电商平台，要求提供用户等级与交易权限的关联证明等。

5. 结论

电商支付领域刑事电子证据的可采性规则研究具有重要的理论价值和实践意义。本文通过对该领域电子证据可采性规则的研究，得出以下结论：首先，电商支付领域电子证据具有多主体参与、交易链条完整、实时高频、跨境流动和强监管合规等特殊性质，这些特殊性决定了其可采性规则需要区别于传统电子证据。

其次，电商支付领域电子证据的可采性审查应当遵循适应行业特点的“三性”原则，并通过专门技术标准和法律规范的结合，保障电子证据的证据资格和证明力。在真实性方面，应针对电商支付多主体、跨平台的特点，建立基于区块链和统一标准的数据验证机制；在合法性方面，需结合支付数据敏感性制定分层授权和负面清单制度；在关联性方面，要创新“资金流 + 信息流”双轨分析模式，利用大数据技术提升关联判断的准确性。最后，电商支付领域电子证据的可采性规则需要平衡多方价值。一方面要保障侦查机关有效打击电商支付领域刑事犯罪，另一方面要保护公民个人信息安全和商业秘密。

参考文献

- [1] 法安网. 从证据审查角度探析刑事诉讼中电子数据收集提取的规范化[EB/OL]. <https://www.faanw.com/quzheng/692.html>, 2025-09-15.
- [2] 李智. 跨境电子商务支付结算法律问题研究[J]. 国际金融研究, 2024(3): 23-24.
- [3] 易延友. 证据法学: 原则、规则、案例[M]. 北京: 法律出版社, 2017: 102-105.
- [4] 陈卫东. 跨境电子取证制度研究[J]. 中国法学, 2023(5): 34-38.
- [5] 张明楷. 电子支付领域刑事犯罪的证据问题研究[J]. 现代法学, 2024(2): 113-118.
- [6] 刘宪权. 互联网金融犯罪的刑法规制[J]. 法学, 2023(7): 45-49.
- [7] 曲新久. 个人信息保护与刑事侦查的平衡[J]. 政法论坛, 2024(1): 53-59.
- [8] 杨永川, 顾益军, 张培晶, 等. 计算机取证[M]. 北京: 高等教育出版社, 2008: 85-86.
- [9] 周晓宇. 从经济视角分析鉴定人出庭作证问题[J]. 铁道警官高等专科学校学报, 2012, 22(6): 39-40.
- [10] 何家弘. 电子证据法研究[M]. 北京: 法律出版社, 2002: 400-401.