

电子支付安全与电子商务法律风险管理

黄钰丹¹, 谢清元²

¹贵州大学法学院, 贵州 贵阳

²贵州堂镜律师事务所, 贵州 贵阳

收稿日期: 2024年6月12日; 录用日期: 2024年9月23日; 发布日期: 2024年9月30日

摘要

本文讨论了电子支付安全与电子商务法律风险管理的相关问题。电子支付虽然方便快捷, 但也存在系统安全问题, 如系统漏洞、病毒攻击和黑客入侵, 这些威胁用户资金安全。电子支付安全问题的成因包括用户安全意识不足、技术手段落后和法律法规不完善。另一方面, 电子商务法律风险源于法律法规滞后、监管缺失和技术漏洞。电子支付安全监管体系不完善, 法律法规和标准待健全, 监管部门间协调不足。电子商务企业法律风险意识淡薄, 可能涉及用户隐私侵犯、违规促销和逃税等问题。为解决这些问题, 需要完善电子支付安全监管体系, 建立健全电子商务法律法规体系, 并提升企业法律风险意识。

关键词

电子支付安全, 电子商务法律, 风险管理

Electronic Payment Security and E-Commerce Legal Risk Management

Yudan Huang¹, Qingyuan Xie²

¹College of Law, Guizhou University, Guiyang Guizhou

²Guizhou Tangjing Law Firm, Guiyang Guizhou

Received: Jun. 12th, 2024; accepted: Sep. 23rd, 2024; published: Sep. 30th, 2024

Abstract

This paper discusses the issues related to electronic payment security and e-commerce legal risk management. Although electronic payment is convenient and fast, there are also system security issues, such as system vulnerabilities, virus attacks, and hacker intrusions, which threaten the safety of user funds. The causes of electronic payment security problems include insufficient user security awareness, backward technical means, and imperfect laws and regulations. On the other

文章引用: 黄钰丹, 谢清元. 电子支付安全与电子商务法律风险管理[J]. 电子商务评论, 2024, 13(4): 121-126.

DOI: 10.12677/ec.2024.1341130

hand, the legal risks of e-commerce stem from lagging laws and regulations, lack of regulation, and technological loopholes. The electronic payment security supervision system is not perfect, laws, regulations and standards need to be improved, and the coordination between regulatory departments is insufficient. E-commerce enterprises have a weak awareness of legal risks, which may involve issues such as user privacy violations, illegal promotions, and tax evasion. In order to solve these problems, it is necessary to improve the security supervision system of electronic payment, establish and improve the legal and regulatory system of e-commerce, and enhance the awareness of legal risks of enterprises.

Keywords

Electronic Payment Security, E-Commerce Law, Risk Management

Copyright © 2024 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

首先, 随着互联网技术的快速发展和普及, 电子商务在全球范围内得到了迅猛发展, 成为推动经济增长的重要力量。电子支付作为电子商务交易的关键环节, 其便捷性、高效性受到广泛认可, 使用频率不断提高[1]。然而, 随着电子支付的普及, 支付安全问题也日益凸显, 成为制约电子商务进一步发展的关键因素。其次, 电子支付系统涉及大量的用户账户和资金信息, 其安全性直接关系到用户的财产安全和个人隐私保护[2]。因此, 银行业电子支付系统的安全性问题显得尤为重要。对于银行而言, 保障电子支付系统的安全不仅是维护用户权益的需要, 也是保障自身安全运营的必要条件[3]。此外, 随着电子商务的蓬勃发展, 相关的法律风险与合规问题也日益凸显。电子商务活动涉及电子合同、电子支付、物流配送、税收征管等多个方面, 这些领域都存在着一系列法律风险与合规挑战。例如, 知识产权保护、消费者权益保护、数据安全等问题都需要得到妥善解决, 以保障电子商务行业的健康发展[4]。因此, 对电子支付安全与电子商务法律风险管理的研究具有重要的现实意义和理论价值。通过深入研究和探讨这些问题, 可以为电子商务支付安全和风险控制提供有效的解决方案和策略, 推动电子商务行业的健康发展[5]。同时, 也可以为电子商务企业更好地了解和应对法律风险与合规问题提供指导, 保障企业的合法权益[6]。

2. 电子支付安全现状分析

随着科技的飞速发展, 电子支付已逐渐渗透到我们生活的方方面面, 成为现代社会中不可或缺的一部分。然而, 随之而来的电子支付安全问题也引起了广泛关注。本文将对电子支付安全现状进行深入分析, 探讨其主要类型及成因, 以期提升电子支付安全提供借鉴与参考。

2.1. 电子支付安全问题的主要类型

电子支付安全问题多种多样, 主要包括以下几个方面:

2.1.1. 账户安全问题

这包括账户被盗用、密码泄露、身份信息被冒用等。攻击者通过非法手段获取用户账户信息, 进而进行非法操作, 如转账、购物等, 给用户带来经济损失。

2.1.2. 交易安全问题

在电子支付过程中, 交易安全问题也不容忽视。这包括虚假交易、交易欺诈、资金被拦截等。攻击者利用伪造交易信息、伪造支付页面等手段, 诱骗用户进行支付, 从而实现非法获利。

2.1.3. 系统安全问题

电子支付系统本身也存在一定的安全隐患。例如, 系统漏洞、病毒攻击、黑客入侵等, 都可能导致电子支付系统出现故障或数据泄露, 进而影响到用户的资金安全。

2.2. 电子支付安全问题的成因分析

部分用户对电子支付安全问题缺乏足够的认识, 未能及时采取有效的防护措施。例如, 使用弱密码、未及时更新软件版本、随意点击来源不明的链接等, 都可能导致账户被盗用或信息泄露。部分电子支付平台在技术手段上相对落后, 未能及时跟进新技术的发展。这使得平台在防范攻击、识别欺诈等方面存在一定的局限性, 从而增加了电子支付安全风险。目前, 关于电子支付安全方面的法律法规尚不完善, 尚未形成有效的监管体系。这使得部分不法分子有机可乘, 利用法律漏洞进行非法活动, 进一步加剧了电子支付安全问题的严重性。此外, 电子支付安全问题还受到网络环境、设备安全等因素的影响。网络环境的不稳定、设备安全漏洞等都可能给电子支付带来潜在的风险。综上所述, 电子支付安全问题已成为当前亟待解决的重要问题。为了提升电子支付安全, 我们需要从用户、技术、法律等多个方面入手, 加强安全意识教育、提升技术手段、完善法律法规等, 共同营造一个安全、可靠的电子支付环境。

3. 电子商务法律风险管理现状

随着信息技术的迅猛发展, 电子商务已成为现代社会经济活动中不可或缺的一部分。然而, 电子商务的快速发展也带来了一系列的法律风险问题。为了更好地应对这些风险, 我们需要对电子商务法律风险管理现状进行深入的探讨和分析。

3.1. 电子商务法律风险的种类与特点

电子商务法律风险主要包括合同风险、知识产权风险、隐私保护风险、网络安全风险等。这些风险具有多样性和复杂性的特点。首先, 合同风险是电子商务中最为常见的法律风险之一。由于电子商务的跨地域性和虚拟性, 合同双方往往难以面对面进行谈判和签署, 这就容易导致合同条款不明确、履行困难等问题。此外, 电子合同的法律效力问题也是合同风险的一个重要方面。其次, 知识产权风险也是电子商务领域的一个突出问题。在电子商务平台上, 大量的商品和服务信息涉及知识产权问题, 如商标、专利、著作权等。然而, 由于监管不力、维权成本高等原因, 知识产权侵权行为时有发生, 给权利人带来了巨大的经济损失。此外, 隐私保护风险和网络安全风险也是电子商务中不可忽视的法律风险。在电子商务交易过程中, 用户的个人信息和交易数据往往被存储在平台上, 一旦平台发生数据泄露或被黑客攻击, 用户的隐私和财产安全将受到严重威胁。

3.2. 电子商务法律风险的产生原因

电子商务法律风险的产生原因多种多样, 主要包括法律法规滞后、监管缺失、技术漏洞等。首先, 法律法规的滞后性是电子商务法律风险产生的重要原因之一。由于电子商务的发展速度远超过法律法规的制定速度, 现有的法律法规往往难以适应电子商务的新情况和新问题。这就导致了在电子商务交易中, 一些行为可能处于法律的灰色地带, 给交易双方带来了不确定性。其次, 监管缺失也是电子商务法律风险产生的一个重要原因。在电子商务领域, 由于跨地域性和虚拟性的特点, 监管难度较大。一些不法分

子利用监管漏洞进行违法活动, 如虚假宣传、欺诈销售等, 给消费者带来了极大的损害。此外, 技术漏洞也是电子商务法律风险的一个重要来源。电子商务平台往往依赖于各种技术手段来保障交易的安全和顺利进行。然而, 由于技术本身存在缺陷或漏洞, 可能导致平台遭受黑客攻击或数据泄露等安全事件, 从而引发法律风险。综上所述, 电子商务法律风险管理现状面临着诸多挑战和问题。为了有效应对这些风险, 我们需要加强法律法规的制定和完善, 提高监管力度和技术水平, 同时加强消费者权益保护和维权机制建设。只有这样, 才能确保电子商务的健康发展和社会经济的稳定运行。

4. 电子支付安全与电子商务法律风险管理存在问题

4.1. 缺乏电子支付技术安全防范

当前, 缺乏电子支付技术安全防范已成为一个亟待解决的问题。电子支付作为现代支付方式的代表, 涉及大量的个人信息和资金流动, 因此, 技术安全防范显得尤为重要。然而, 现实中, 一些电子支付平台在技术研发和维护方面存在不足, 导致平台存在技术漏洞, 容易受到黑客的攻击。这些攻击往往会导致用户信息的泄露和资金的损失, 给用户带来极大的困扰和损失。此外, 部分电子支付系统还缺乏有效的身份验证和授权机制。一些平台对用户的身份验证过于简单, 使得不法分子能够轻易地通过伪造身份信息进行非法操作。同时, 授权机制的不完善也导致了一些用户账户被他人恶意使用, 造成资金损失。这些技术安全防范的缺失, 不仅影响了电子支付的安全性, 也阻碍了其进一步的普及和应用。为了解决这些问题, 电子支付平台应加强技术研发和维护, 提高平台的安全性能。同时, 应建立完善的身​​份验证和授权机制, 确保用户身份的真实性和操作的合法性。此外, 监管部门也应加大对电子支付平台的监管力度, 确保其符合相关法规和标准, 保障用户的合法权益。

4.2. 电子支付安全监管体系不完善

电子支付安全监管体系的不完善也是当前面临的一大挑战。随着电子支付的快速发展, 其安全问题也日益凸显。然而, 目前我国对于电子支付的监管还处于摸索阶段, 相关的法规和标准尚未完全成熟。这使得电子支付的安全风险难以得到有效控制, 给不法分子提供了可乘之机。此外, 监管部门之间的协调不够紧密也是导致监管体系不完善的原因之一。目前, 涉及电子支付监管的部门众多, 但各部门之间的沟通和协作不够顺畅, 导致监管空白和重复监管的现象时有发生。这不仅影响了监管效果, 也增加了企业的合规成本。为了完善电子支付安全监管体系, 首先需要加强相关法规和标准的制定和完善。政府应加快出台针对电子支付的专项法规, 明确各方责任和义务, 规范市场秩序。同时, 还应建立统一的监管标准, 确保电子支付平台符合安全要求。其次, 加强监管部门之间的协调和沟通也至关重要。各部门应建立信息共享和联合执法机制, 共同应对电子支付安全问题。此外, 还应加强国际合作, 借鉴其他国家和地区的成功经验, 共同推动电子支付安全监管体系的完善。

4.3. 电子商务法律法规体系不健全

电子商务法律法规体系的不健全也是当前面临的一个突出问题。虽然我国已经出台了一系列关于电子商务的法律法规, 但仍然存在许多空白和模糊地带。这导致了一些电子商务活动缺乏明确的法律规范和指导, 给企业和消费者带来了一定的风险。例如, 在跨境电子商务方面, 目前还缺乏专门针对该领域的法律法规。这使得跨境电子商务活动在一定程度上存在监管空白, 不法分子可能利用这一漏洞进行非法活动。此外, 对于消费者权益保护、网络交易纠纷解决等方面, 也需要进一步完善相关法律法规。同时, 电子商务的快速发展也带来了许多新的法律问题。例如, 数据保护和隐私权保护在电子商务中显得尤为重要。然而, 目前我国在这方面的法律法规还不够完善, 难以有效保障用户的合法权益。为了健全

电子商务法律法规体系, 政府应加快制定和完善相关法规。针对跨境电子商务等新兴领域, 应出台专门的法律法规进行规范。同时, 还应加强消费者权益保护和网络交易纠纷解决等方面的法律制度建设。此外, 对于数据保护和隐私权保护等新型法律问题, 也应制定相应的法律法规进行规范和引导。

4.4. 电子商务企业的法律风险意识淡薄

电子商务企业的法律风险意识淡薄也是一个不容忽视的问题。一些企业为了追求短期的利益, 往往忽视了对法律法规的遵守和风险防范。他们可能忽视对用户隐私的保护、违规进行促销活动, 或者故意逃避税务等问题。这种行为不仅会对企业自身带来潜在的法律风险, 也会对整个行业的健康发展产生负面影响。首先, 忽视用户隐私保护是企业常见的法律风险之一。一些企业在收集和使用用户个人信息时缺乏透明度和合法性, 甚至将用户数据用于非法用途。这不仅侵犯了用户的隐私权, 也违反了相关法律法规的规定。其次, 违规进行促销活动也是企业容易触犯的法律风险点。一些企业为了吸引消费者, 可能会采用虚假宣传、误导性广告等手段进行促销。这些行为不仅欺骗了消费者, 也损害了行业的形象和信誉。此外, 故意逃避税务也是一些企业存在的法律风险。一些企业为了降低成本, 可能会采取隐瞒收入、虚报成本等手段逃避税务。这种行为不仅违反了税收法规, 也损害了国家的财政利益。综上所述, 当前电子支付和电子商务领域面临着诸多挑战和问题。为了保障电子支付的安全性和电子商务的健康发展, 需要各方共同努力, 加强技术研发、完善监管体系、健全法律法规并增强企业的法律风险意识。只有这样, 才能为电子支付和电子商务的持续发展创造良好的环境。

5. 电子支付安全问题的对策探讨

5.1. 加强电子支付技术安全防范措施

在电子支付的安全性保障方面, 技术安全防范措施的加强显得尤为重要。随着科技的不断发展, 传统的电子支付安全手段已经无法满足现代支付业务的需求, 因此, 我们迫切需要采用更加先进的技术手段来确保电子支付的安全。

首先, 我们需要加强加密技术的研发和应用。采用先进的加密算法, 如 AES、RSA 等, 对用户信息进行加密处理, 确保在传输和存储过程中, 用户数据不会被非法获取或篡改。此外, 我们还应积极推广量子加密技术的应用, 利用其独特的加密原理, 为电子支付提供更加安全的保障。其次, 生物识别技术的运用也是提升电子支付安全性的重要手段。通过指纹识别、面部识别、虹膜识别等生物识别技术, 可以实现对用户身份的精准验证, 从而提高电子支付的准确性和便捷性。这种技术不仅避免了传统密码的易泄露、易遗忘等问题, 还大大提高了支付的便捷性。此外, 建立多层次的安全防护体系也是保障电子支付安全的关键。这包括防火墙、入侵检测系统、安全审计系统等, 这些系统能够实时监控电子支付业务的运行情况, 及时发现并应对各种潜在的安全威胁。同时, 我们还应加强网络安全技术的研发和应用, 提高电子支付系统的抗攻击能力。

5.2. 完善电子支付安全监管体系

电子支付安全监管体系的完善对于防范金融风险、维护市场秩序具有重要意义。随着电子支付业务的快速发展, 政府应加大对电子支付行业的监管力度, 确保电子支付市场的健康有序发展。首先, 政府应建立健全相关法规和标准, 规范电子支付业务的发展。这包括制定电子支付安全标准、出台电子支付监管政策等, 为电子支付业务提供明确的法律依据和操作规范。其次, 建立电子支付安全监管平台, 实时监测电子支付业务的风险状况。通过收集和分析电子支付业务的数据信息, 监管平台能够及时发现潜在的安全隐患和风险点, 为政府决策提供有力支持。此外, 加强跨部门的协作和信息共享也是完善电子

支付安全监管体系的重要一环。各部门应加强沟通与合作, 共同制定监管政策和措施, 形成监管合力。同时, 通过信息共享机制, 实现监管信息的互通有无, 提高监管效率和准确性。

5.3. 建立健全电子商务法律法规体系

电子商务法律法规体系的建立是保障电子支付安全的重要保障。随着电子商务的快速发展, 政府应加快制定和完善电子商务相关法律法规, 为电子支付业务提供坚实的法律保障。首先, 政府应明确电子支付各方的权利和义务, 规范电子支付业务的操作流程。这包括明确支付机构、商户、消费者等各方的责任和义务, 规范电子支付业务的流程和要求, 确保电子支付业务的合法性和规范性。其次, 加大对违法违规行为的处罚力度。对于违反电子支付安全规定的行为, 政府应依法进行严厉打击, 提高违法成本, 形成有效的法律威慑力。同时, 加大执法力度, 确保法律法规的落地实施。此外, 加强国际合作与交流也是建立健全电子商务法律法规体系的重要途径。借鉴国际先进经验, 推动电子商务法律法规体系的不断完善, 为电子支付业务提供更加广阔的国际发展空间。

5.4. 提升电子商务企业的法律风险意识

电子商务企业在电子支付过程中扮演着重要角色, 因此提升企业的法律风险意识至关重要。企业应加强对电子支付相关法律法规的学习和培训, 确保员工了解并遵守相关规定。首先, 企业应建立健全内部管理制度, 规范电子支付业务的操作流程。通过制定详细的操作规范和安全管理制度, 确保员工在进行电子支付业务时能够遵循规定, 防范内部风险。其次, 加强与监管机构的沟通与合作。企业应积极与监管机构保持联系, 及时了解政策动态和监管要求, 确保企业电子支付业务的合规性。同时, 对于监管机构提出的问题和意见, 企业应及时整改并反馈情况。此外, 企业还应加强自身的风险管理和控制能力。通过建立风险评估机制、制定应急预案等措施, 提高企业对电子支付风险的应对能力, 确保电子支付业务的安全稳定运行。综上所述, 加强电子支付技术安全防范措施、完善电子支付安全监管体系、建立健全电子商务法律法规体系以及提升电子商务企业的法律风险意识是保障电子支付安全的重要措施。只有通过全方位的努力和合作, 我们才能为电子支付业务提供更加安全、可靠的环境, 推动电子商务的健康发展。

6. 结论

本文深入分析了电子支付安全问题, 探讨了其主要类型及成因, 并提出了提升电子支付安全的方法。同时, 本文还探讨了电子商务法律风险管理现状, 分析了电子商务法律风险的种类与特点, 以及产生原因。为保障电子商务健康发展和社会经济稳定运行, 需要加强电子支付技术安全防范、完善电子支付安全监管体系、健全电子商务法律法规体系。政府需明确电子支付各方权利义务, 加大处罚力度, 并推动国际合作与交流。同时, 提高电子商务企业的法律风险意识, 确保电子支付业务合法规范运行。通过全方位合作, 为电子支付业务创造安全可靠环境, 推动电子商务健康发展。

参考文献

- [1] 于昕彤. 《电子商务法》视域下的电子支付安全问题研究[D]: [硕士学位论文]. 锦州: 渤海大学, 2020.
- [2] 赵玉明, 侯新华, 李丽. 电子商务概论[M]. 南昌: 江西高校出版社, 2019: 264.
- [3] 杨立新. 电子商务交易中电子支付服务损害赔偿责任及其规则[J]. 中州学刊, 2019(2): 45-56.
- [4] 杨立新. 电子商务民事责任之立法基础与基本规则[J]. 甘肃社会科学, 2019(1): 100-107.
- [5] 杨东, 黄尹旭. 《电子商务法》电子支付立法精神与条文适用[J]. 苏州大学学报(哲学社会科学版), 2019, 40(1): 62-69+191.
- [6] 罗洪荣. 浅谈电子支付安全与隐患[J]. 电脑知识与技术, 2017, 13(25): 50-51.