

电商平台刷单诈骗的法律分级预警机制研究

张桐¹, 王希²

¹贵州大学法学院, 贵州 贵阳

²贵州省毕节市威宁县人民检察院数字办公室, 贵州 毕节

收稿日期: 2025年6月27日; 录用日期: 2025年7月18日; 发布日期: 2025年8月15日

摘要

当前刷单返利诈骗犯罪呈现技术赋能化、链条隐蔽化与侵害复合化特征, 而传统治理模式面临预警滞后与效能不足的困境。基于犯罪学日常活动理论框架, 聚焦犯罪形成三要素中的两大核心要素: “合适的侵害目标”与“缺乏有效监控”, 深入分析被害成因, 并提出在该理论的三级预防框架下被害人特征识别与平台监管漏洞监测的双轨预警、高危被害识别及行为链阻断的动态响应机制, 形成多维度、立体化的协同治理闭环。研究为数字时代犯罪预防治理提供兼具理论创新与实践效能的方案, 推动治理范式向分类分级精准化转型。

关键词

刷单返利诈骗, 日常活动理论, 分类分级预警, 三级预防, 协同治理

A Study on the Legal Hierarchical Early-Warning Mechanism for Brush Order Fraud on E-Commerce Platforms

Tong Zhang¹, Xi Wang²

¹Law School, Guizhou University, Guiyang Guizhou

²Digital Office, Weining County People's Procuratorate of Bijie City, Guizhou Province, Bijie Guizhou

Received: Jun. 27th, 2025; accepted: Jul. 18th, 2025; published: Aug. 15th, 2025

Abstract

Current brush order rebate fraud exhibits characteristics of technologically-driven evolution, concealed criminal chains, and compound victimization, while traditional governance models face challenges including early-warning lags and insufficient efficacy. Based on the Routine Activity Theory framework in criminology, this study deconstructs victimization causes by analyzing two core

elements of the three elements of crime form: “suitable targets” and “lack of capable guardianship.” It proposes a dual-track early-warning mechanism integrating victim risk profiling and platform regulatory loophole monitoring under a three-tiered prevention model, coupled with dynamic responses for high-risk victim identification and behavior chain interruption. This forms a multidimensional, holistic collaborative governance framework. The research provides a theoretically innovative and practically viable solution for digital-era crime prevention, propelling the transformation of governance paradigms toward classified and hierarchical precision.

Keywords

Brush Order Rebate Fraud, Routine Activity Theory, Classified and Hierarchical Early-Warning, Three-Tiered Prevention, Collaborative Governance

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

近年来,电信网络诈骗案件的发案数量以每年 20% 的速度增长[1],当前仍呈现整体高发态势[2]。其中,刷单返利类诈骗犯罪形势严峻,在五类主要电信网络诈骗犯罪中,刷单返利类诈骗发案率最高,占发案总数的三分之一左右¹。“刷单”按照目的可分为声誉型、财产型、竞合型三类,但不论何种“刷单”,其本质都是一种虚假宣传的虚构交易行为[3],其生存土壤的灰色属性,致使“刷单”行为从诞生之日起便游离于传统监管治理体系边缘。“刷单返利诈骗”则是指“犯罪嫌疑人运用通讯工具、互联网等技术手段,诱导不特定多数人刷单,通过返还小额佣金骗取被害人信任,使受害人陷入正常交易的错误认识,最后利用先行充值或垫付资金、事后交易的方式诈骗受害者垫资款的行为。”[4]按照犯罪对象通常可分为“个人被骗型”、“商户被骗型”和“平台被骗型”三种类型[5]。鉴于“个人被骗型”在发案量和社会危害性上的突出地位,本文研究主要聚焦于此类型。一方面由于“刷单”行为自身的“灰色”属性和非接触性,构成了诈骗犯罪的天然温床;另一方面随着信息技术发展的突飞猛进,传统治理模式面对高新技术赋能的“刷单返利”诈骗,在预警精准度、响应时效性及跨平台协同层面均陷入效能困境。因此,亟需构建一种能够有效应对其新型特征、精准识别风险并快速响应的预警机制,日常活动理论为解构此类犯罪的成因和设计针对性预警干预措施提供了有力的理论支撑。

2. 利用电商平台实施刷单返利诈骗犯罪呈现显著时代特征

2.1. 新兴技术深度赋能驱动犯罪模式智能化迭代

伴随数字时代的技术升级,各类犯罪均呈现出不同程度的技术赋能化趋势,就本罪而言,犯罪主体主要依托大数据分析、自动化脚本工具及即时通讯技术,精准筛选潜在受害人并模拟正常交易流程,通过云端服务器实现“一人多机”远程操控,利用智能算法动态调整诈骗话术,规避平台风控系统,大幅提升犯罪效率与反侦查能力。2025 年以来,智能体的广泛应用为社会各部门生产活动提供了过去难以想象的便利²,但同时其带来的“低代码”乃至“零代码”犯罪工具开发,也更进一步降低了犯罪门槛,使得本罪犯罪模式呈现出显著的智能化迭代特征。这要求预警机制必须具备更强的数据挖掘能力和智能分

¹中华人民共和国公安部:公安部公布五类电信网络诈骗案件(2022)。

²环球网:《2025 会是 AI 智能体爆发元年吗?多位人工智能领域专家解读》。<https://china.huanqiu.com/article/4Lp8Sgb5ir3>

析水平, 以识别高度模拟正常行为的异常模式。

2.2. 非接触性与跨平台协作促成黑色产业链隐蔽化重构

由于本罪依托电商平台实施犯罪, 犯罪活动全程通过数字空间完成, 行为人与受害者无物理接触。犯罪分工依托通讯软件、地下论坛等实现跨地域协作, 形成“引流推广-账号租赁-资金转移-洗钱变现”的模块化黑色产业链条。各环节采用独立加密通道联络, 利用第三方支付、虚拟货币等多层跳板切割资金流向, 极大增加犯罪溯源难度。平台监管的碎片化进一步导致跨平台犯罪制度漏洞, 使得本罪所依托的黑色产业链呈现愈发隐蔽的发展趋势, 进而对预警机制提出了跨平台数据融通、资金流协同监测和快速追溯的迫切需求。

2.3. 侵害法益从单一财产权向复合化法益双重叠加演变

受害人在财产损失基础上, 因参与刷单提供身份证、银行卡、生物识别信息等敏感数据, 导致个人信息权遭受侵害。部分犯罪团伙进一步利用上述信息实施冒名贷款、虚假注册, 直接损害受害人信用记录与社会评价, 形成财产损失与人格权益侵害的双重叠加。犯罪行为通过海量虚假交易扭曲电商平台信用评价体系, 破坏正常商业竞争秩序, 侵蚀消费者对电商平台信用评价体系的信任基础。规模化诈骗活动推高了市场交易的信任成本与风控成本, 削弱社会成员间的普遍信任, 冲击诚信经济伦理基础。同时, 黑色产业资金流动助长洗钱、非法集资等衍生犯罪, 形成对社会治理体系的系统性风险, 这就要求预警机制不仅要关注资金损失风险, 还需识别信息泄露风险及信用损害风险, 并考虑其对社会经济秩序的广泛影响。

3. 基于日常活动理论的被害成因解构与预警切入点

3.1. 日常活动理论的分析框架及其在本研究中的应用

科恩与费尔森于 1979 年提出日常活动理论^[6], 并总结了犯罪形成的三要素, 即有“动机的犯罪人”、“合适的侵害目标”、“缺乏有效监控”^[7], 鉴于本研究的预警导向与可操作性需求, 从司法实践的经验出发, “有动机的犯罪人”具有弥散性, 分布于社会各结构维度, 对其进行有效监控的成本过高, 在实践中难以进行针对性犯罪预警, 其中仅有再犯预警可依托司法机关卷宗档案对潜在再犯罪人进行精准定位, 但由于本罪再犯可能性不同于典型再犯高发犯罪, 如性侵类生理犯, 因此在实践中基于“有动机的犯罪人”进行风险预警难以落地。相比较而言, “合适的侵害目标”与“缺乏有效监控”这两个要素具有更高的可识别性与干预可行性, 成为本研究构建预警机制的核心理论支点。具体到刷单返利诈骗犯罪预警领域, 一方面, 本罪被害人自身具有显著的受侵害风险特征, 具有相对较高的可识别性; 另一方面, 督促平台加强源头监督管控具有现实可行性。因此, 本研究预警模型将围绕识别“合适的侵害目标”和监测“缺乏有效监控”这两个关键维度展开。

3.2. 基于“合适的侵害目标”的被害人特征分析

《2021 年电信网络诈骗治理研究报告》数据显示³, 被害人群体呈现三类具有较高可识别性的被害风险特征。一是经济脆弱性, 以学生、全职主妇、灵活就业人员为主体的潜在受害人, 普遍存在收入不稳定或可支配资金有限的特征^[4], 对“低门槛高回报”的刷单宣传抵御能力薄弱。二是风险认知偏差, 多数受害人缺乏对刷单行为违法性的基础认知, 误判其为平台默许的灰色兼职, 部分群体虽意识到风险,

³江汉大学党委保卫部、保卫处:《2021 年电信网络诈骗治理研究报告》。
<https://bwc.jhun.edu.cn/61/71/c1929a156017/pagem.htm>

但在“首单返现”等即时正向反馈下产生侥幸心理[8], 低估资金被套牢概率。三是数字素养局限性, 中老年及低学历群体对复合型诈骗话术的辨识能力不足[2], 易被伪造的商户资质、转账记录等虚假背书误导, 主动配合完成多轮资金操作[9]。这些特征为构建被害人侧的风险识别指标, 如经济状况画像、风险认知评估、异常操作行为模式等, 提供了直接依据, 是预警模型“被害人特征预警维度”的基础。

3.3. 基于“缺乏有效监控”的治理缺位分析

当前, 在应对刷单返利诈骗方面, “缺乏有效监控”在电商平台场景下主要表现为平台监控机制的技术性失灵与协同性不足[10]。基于阻断被害的目标, 就平台监控机制失灵而言, 具体体现在事前预防失效和事中干预滞后两个关键环节。一是电商平台对商户资质审核流于形式化, 对异常交易行为模式缺乏高效的实时动态监控, 无法及时识别虚假交易集群[11]。二是平台风控系统对隐蔽资金流转模式响应迟缓⁴, 对跨平台跳转的诈骗链接拦截率较低。以上平台侧的漏洞, 如准入审核缺陷、异常交易识别算法不足、跨平台协同机制缺失等, 正是预警模型“平台监管预警维度”需要量化和监测的核心对象, 也是平台企业落实风险管控责任的关键着力点。

4. 构建基于日常活动理论的分类分级预警模型

4.1. 基于被害人被害风险因素分析的二维识别体系

基于被害人群体呈现出的可识别高风险属性, 就其外在表现特征集进行归纳总结, 运用 K-means++ 算法, 对特征集进行聚类[12], 提炼出被害人被害风险的两大核心维度。一是主体脆弱性, 即通过对受害人自身主体脆弱性特征进行分析, 识别出经济脆弱性与认知能力局限是构成被害人易感性的两大关键风险因子; 二是行为异常性, 即通过对被害人受害前和受害中的异常操作和行为进行分析, 得出操作频次和平台跳转的异常是典型风险信号的核心识别特征。

4.2. 基于平台监管漏洞风险因素分析的二维检测体系

基于平台监管漏洞分析, 主要关注事前和事中两个阶段。事前阶段, 准入机制缺陷, 电商平台商户资质审核存在三重漏洞, 一是主体真实性验证依赖静态证照核验, 对深度伪造的营业执照识别率不足, 需技术提升; 二是经营能力评估中缺失对动态现金流的有效分析, 致使空壳公司过审率高, 需数据建模; 三是跨平台关联审查缺位, 同一犯罪团伙可分散注册多家店铺规避风险阈值, 需协同机制。事中阶段, 风控响应迟滞, 现有监测系统存在双重功能短板, 一是异常交易识别算法仅关注单笔交易特征, 忽视集群行为模式, 需行为模式分析; 二是资金流监测缺乏跨平台协同机制支撑, 犯罪资金经第三方支付跨平台转移后难以溯源, 需跨平台协同。

4.3. “两类三级”数字化被害预警模型构建

当今信息革命深刻改变了人们的生产生活, 使人类迈进了数字化生存状态[13], 因此在犯罪预防治理领域, 应当有机融合新兴数字技术, 推动社会治理的数字化转型。基于日常活动理论的核心双要素即“合适的侵害目标”、“缺乏有效监控”和前述分析, 本文提出“两类三级”数字化被害预警模型构建的设想。“两类”指基于日常活动理论中“合适的侵害目标”与“缺乏有效监控”双核心要素, 构建被害人特征预警与平台监管预警的协同体系。一是被害人特征预警维度, 整合经济脆弱性、认知偏差度、行为异常性三大核心指标, 构建风险评分模型, 针对“合适的侵害目标”。二是平台监管预警维

⁴中国人民银行官网:《2023 中国反洗钱报告》。

<http://www.pbc.gov.cn/fanxiqianju/resource/cms/2025/04/2025040914154223843.pdf>

度, 量化工前准入缺陷与事中风控迟滞两大风险维度, 形成监管失效指数, 针对“缺乏有效监控”。“三级”指预防响应体系, 借鉴流行病学三级预防理论, 建立动态响应机制。一级一般预防层即潜在被害风险值较低且无异常行为记录, 推送反诈一般常识宣传即可; 二级临界预防层即潜在被害风险值中等偏高且触发平台异常行为信号, 干预措施为定点推送针对性反诈普法信息, 并强制人脸验证加交易延迟; 三级高危预防层即潜在被害风险值较高且异常行为频次高, 干预措施为平台客服人工精准介入加支付通道暂时冻结。

5. 基于数字化预警模型构建多维立体协同预防机制

5.1. 多维立体的整体预防思路

以司法机关为主导、平台企业为核心, 落实“有效监控”责任, 以用户自主防范为基础, 降低成为“合适目标”风险, 三主体共同构建三维协同预防体系。司法机关依托现有大数据法律监督系统接入平台, 对高危预警及时介入干预, 监督平台修复漏洞; 平台履行风险管控, 构建跨平台资金追溯渠道; 用户方面则通过针对性普法宣传教育, 强化风险认知[14], 形成“司法机关-平台企业-用户自身”的多维立体防御链。

5.2. 基于预警层级的纵向协同机制

针对三级预警构建阶梯式响应, 在一级一般预防层, 面向低风险群体推送场景化反诈知识, 重点强化经济脆弱群体的信用积分管理, 降低其成为“合适目标”风险; 临界预防层则聚焦平台监管责任, 触发异常信号时强制启动动态人脸验证及交易延迟机制, 增强“监控”有效性, 并利用跨平台溯源机制提升资金追溯效率应对隐蔽性; 高危预防层由司法机关主导应急处置, 通过 AI 语音实时劝阻、人工法律告知及洗钱账户冻结实现被害阻断。

5.3. 基于要素联动的横向协同机制

建立数据融通中枢, 通过整合检察机关案件信息、电商平台行为日志及金融机构资金流水三类核心数据, 构建跨系统多元数据融合分析通道[15], 有效打通“被害人特征预警”与“平台监管预警”之间的数据壁垒, 消除信息孤岛。在责任配置层面, 平台企业对触发二级预警的情形承担首要处置责任, 直接弥补“监控缺位”, 需建立商户资质动态核验机制及异常交易实时拦截系统; 司法机关则主导三级高危预警的处置, 制定标准化应急响应处置流程, 协调支付机构实施资金快速冻结, 并通过效能评估反馈持续优化预警模型与响应流程, 形成预警-处置-优化的闭环管理。

6. 结语

本研究基于日常活动理论构建“被害人特征识别-平台监管漏洞监测”的双轨预警模型, 通过三级预防响应机制实现风险精准干预。司法机关主导三级处置、平台落实二级管控、用户参与一级防御的纵向协同, 与数据融通、责任配置明晰化、效能反馈机制化的横向联动相融合, 形成“分类分级、立体防控”的治理范式, 该范式遵循“早发现、早干预、早阻断”的预防原则, 有效回应了刷单返利诈骗技术化、隐蔽化、复合化的时代特征挑战, 为数字时代犯罪预防理论框架与实践方案的探索提供了新模式, 也为电商平台构建智能化、精准化的风控体系探索了理论方向和实践路径。

基金项目

贵州省 2024 年研究生科研基金项目: 新质生产力赋能贵州乡村文化旅游——反强迫购物数字预警机制研究(2024YJSKYJJ097)。

参考文献

- [1] 冯鸿波. 电信网络诈骗犯罪的侦查困境及打击对策[J]. 森林公安, 2020(3): 12-14.
- [2] 张帆锐, 石拓, 尤慧. 电信网络诈骗被害人群空间统计分布及风险特征研究——以刷单返利类为例[J]. 调研世界, 2024(9): 78-86.
- [3] 阴建峰, 刘雪丹. 网络刷单行为的刑法规制研究[J]. 知与行, 2016(8): 53-61.
- [4] 杨行, 王宏玉. 被害人学视角下刷单返利类诈骗犯罪的成因分析与防控[J]. 网络安全技术与应用, 2023(2): 137-139.
- [5] 皮子昕, 罗震雷. 刷单返利网络诈骗的心理诱导机制与防范策略[J]. 广西警察学院学报, 2023, 36(4): 82-89.
- [6] Eck, J. (2003) Police Problems: The Complexity of Problem Theory, Research and Evaluation. *Crime Prevention Studies*, 15, 79-113.
- [7] 李明琪. 犯罪学[M]. 北京: 中国人民公安大学出版社, 2016: 202-203.
- [8] 宋沛阳, 王世卿. 基于既有样本分析的刷单返利类诈骗犯罪的治理对策研究[J]. 公安教育, 2024(3): 41-46.
- [9] 张杰策, 刘云霄, 漆晨航. 刷单返利类诈骗被害特征与防控对策研究——基于 J 区 211 份被害人报案材料的分析[J]. 江西警察学院学报, 2022(4): 31-38.
- [10] 朱晓琛. 网络刷单返利类诈骗犯罪及治理对策研究[J]. 网络安全技术与应用, 2024(8): 153-155.
- [11] 张旭, 史云舟. 互联网平台的犯罪风险防控责任[J]. 中国特色社会主义研究, 2023(4): 61-71.
- [12] 王梦仙, 李银锁, 钟石根, 等. 基于 K-means 聚类的计算机网络信息安全风险评估方法[J]. 信息记录材料, 2025, 26(6): 36-38.
- [13] 马长山. 面向“三维世界”的数字法学[J]. 中国社会科学, 2024(11): 145-163+207.
- [14] 秦运来, 郭煜, 李萌. 提升大学生识别防范电信诈骗能力研究——以刷单返利诈骗为例[J]. 法制博览, 2025(10): 28-30.
- [15] 郭兆轩, 张学超. 数字时代犯罪技术治理的现状、困境与策略[J]. 中国人民公安大学学报(社会科学版), 2024, 40(6): 65-73.