

# 虚假注册牟利 AI变脸诈骗

正值国家网络安全宣传周,上海法院解码电子商务网络犯罪新动向

案件  
虚构新用户身份骗取「首单优惠」

上海二中院辖区法院此前审理过一起以借助技术手段虚构新用户身份,骗取电商平台“首单优惠”为代表的直接侵害电子商务平台权益的犯罪案件。

被告人付某在深圳经营一家科技公司,从2018年初起,付某与上海一信息科技有限公司股东曹某接洽,知悉该公司运营一家电商平台,需要巨量手机号码和对应验证码,付某遂与深圳另一家科技公司的股东唐某、赖某、王某三人合谋,打算以此牟利。

几人经商议,决定唐某、赖某、王某均先以他人代持股的方式入股付某所在公司,再分别利用三人在本公司任股东及软件、硬件、销售业务主管的便利条件,将非法程序与正常手机系统整合,通过生产端批量植入手机主板后在市面上发售。

据悉,被安装该非法程序的手机终端,在机主插入SIM卡连接网络后,手机号码会自动上传到付某所在公司的数据库,并传输至电商平台数据库内。当下游用户使用该号码提交相关注册申请后,含有验证码的短信在手机端即被截获、提取、上传,再以相同方式同步至电商平台销售给下游用户使用,由付某公司和曹某公司共分所获收益。付某再将获得的不法收益分予被告人唐某、赖某和王某。

经审计,付某等人从曹某所在的上海信息科技有限公司获取违法所得500余万元。后经补充侦查,新增认定获取违法所得900余万元,经审计共计获取违法所得1467万余元。

法院审理后认为,被告人付某、唐某等人违反国家规定,对计算机信息系统实施非法控制,情节特别严重,其行为均已构成非法控制计算机信息系统罪,最终判决付某、唐某等人有期徒刑1年8个月至4年不等,并处罚金2万元至100万元不等。

“我们梳理了我院辖区法院过去3年审结的涉电子商务网络犯罪案件723件,发现这些案件呈现出较为明显的类型化趋势,一部分就是以借助技术手段虚构新用户身份骗取电商平台‘首单优惠’为代表的直接侵害电子商务平台权益的犯罪案件;另一部分为以电商平台为作案媒介,实施非法吸收公众存款、帮助信息网络犯罪活动以及组织、领导传销活动等扰乱市场经济秩序和社会管理秩序的犯罪案件。”

上海二中院刑庭庭长任素贤介绍,从数据来看,其中,直接侵害电子商务平台权益的犯罪案件530件,占比73.31%;以电子商务平台为作案媒介的犯罪案件193件,占比26.69%。

在侵害电子商务平台权益的530件案件中,从涉案罪名看,以诈骗罪居多,总计489件,占比达到92.26%。从判处刑罚看,判处3年以下的轻刑案件数量较多,适用缓刑的比例较高,被判处3年以下有期徒刑、管制、拘役的被告人有837人,所占比例高达98.94%,缓刑适用率达78.22%。从涉及平台类型看,涉及货运、客运、外卖、网络购物等多种平台。

任素贤介绍,在以电子商务平台

□法治报记者 季张颖

编写非法程序植入终端,冒充新用户用户在电商平台注册骗取“首单优惠”……像这样直接侵害电子商务平台权益的犯罪案件,正成为涉电子商务网络犯罪的主流。

正值国家网络安全宣传周,近日,上海市第二中级人民法院发布了《2019-2022年涉电子商务网络犯罪案件审判白皮书》(以下简称《白皮书》)。记者获悉,3年来,上海二中院辖区法院共审结涉电子商务网络犯罪案件723件,涉及被告人1240人,案件数量整体呈现下降趋势,其中直接侵害电商平台权益案件占比超7成。

《白皮书》通过梳理进一步发现,涉电商网络犯罪案件主要集中在侵财类犯罪中,聚焦于外卖、网约车、网络购物等日常生活的应用场景中,且犯罪手段日渐多样,犯罪分子借助AI变脸、变声、改号等新型手段进行规避,涉案受害者往往遍布全国各省市。



上海二中院发布《法治化营商环境建设系列审判白皮书》

为作案媒介的193件案件中,涉及被告人394人,其中以直播平台为媒介进行犯罪的情况较为突出。

从犯罪手段看,此类犯罪对技术的依赖性强。有52件系被告人利用“爬虫”“撞库”等技术,窃取平台数据资源和用户个人信息,为下游犯罪快速供应作案物料;有39件系被告人使用“刷单”软件,人为影响电商卖家的销售量和信誉度;有21件系建立专门的网上购物商城等,巧借合法平台宣传名目,实际上隐秘充斥着网络色情、赌博、传销等违法犯罪行为,归集发展成一个个网络技术黑灰产业链。



上海二中院举行推进法治化营商环境建设发布会

## 特点 借助AI变脸 侵入日常生活应用场景

《白皮书》显示,涉电商网络犯罪案件主要集中在侵财类犯罪、妨害社会管理秩序类犯罪中,其中侵财类犯罪共543件,占比75.10%。侵财类案件中又以诈骗类案件最为常见,主要包括:通过“接码平台”虚构新用户身份或虚构交易,骗取电商平台“首单优惠”、抵用券等谋取不法利益;以股权、区块链、虚拟货币等为对象进行投资诈骗;虚构学历、工作等身份情况进行“通关系”“谈对象”诈骗,这些案件中个案的涉案金额普遍较低。

上海二中院通过梳理还发现,在以电商平台为作案媒介的193件案件中,32件为5人以上的团伙作案。此类犯罪案件,上下游之间存在关联性,多形成以网络平台为基础、上中下游交织互联的犯罪体系。除组织、领导传销活动犯罪案件外,团伙内部一般无明显的层级结构,成员流动较为频繁,多表现为跨地域分布,犯罪链条也呈碎片化分散于各地。

“从犯罪手段来看,也呈现出类型多样的特点,网络犯罪各罪名之间交错重叠。”任素贤指出,“聚焦被告人的具体作案手法,我们发现,犯罪分子不仅开

发、制作和运行专门的诈骗网站、网络钓鱼软件、后台篡改程序、自动交易刷单软件等,还不断翻新作案手段,借助AI变脸、变声、改号等技术进行反侦查,规避电商平台的自我检测系统和公安侦查预警系统的防控打击,降低平台对于可疑的诈骗网站、广告植入、违法链接的识别准确率。犯罪分子借助这些智能化隐蔽化的犯罪手段,不断扩大网络犯罪的规模,涉案受害者往往遍布全国各省市。”

《白皮书》指出,此类案件的另一特点是涉及平台多元,聚焦下沉市场的高频应用场景。数据显示,在侵害电商平台权益的网络犯罪案件中,涉及外卖、网约车、网络购物等日常生活场景的达到了320件,占比60.38%。

“在国民消费转型和县域经济发展的大背景下,电商平台纷纷通过研发社区团购、拼团购等新颖模式,以生鲜、社交等为切口进入下沉市场跑马圈地。犯罪分子在这一市场充分竞争的窗口期,在群众日常生活中高频使用的电商平台上,借助优惠政策、社交推广的东风,利用各种技术手段触碰犯罪红线牟取非法利益。”《白皮书》中这样总结道。

## 建议 强化跨域司法协作 加强联动防控

上海二中院发现,网络犯罪中的犯罪行为以数字化实施、数字化留痕、数字化证明为主要方式,证据的收集固定、转化及审查均面临新的挑战。

在追赃挽损上也难度较大,无形资产受损严重。“像利用‘接码平台’等方式骗取首单优惠等犯罪案件中,单笔犯罪金额普遍较小,但整个系列案、集团案的总体涉案金额庞大。”

《白皮书》指出,在以电商平台为作案媒介的案件中,被害人分布在全国各地甚至境外,大量被害人的身份和损失难以确定,被害人维权成本高昂。这些案件中犯罪所得往往通过“跑分”的形式在不同空间和人员中层层流转,追踪的难度很大,平台和消费者的损失均难以弥补。

从平台自身管理手段来看,目前,电商平台仍然存在知识产权保护薄弱、用户隐私信息泄露、成为犯罪行为引流工具等问题,对于不断扩大的平台义务仍缺乏较强的针对性控制手段,无法对部分平台商家的错误行为进行纠正,无法及时防范和阻断相关网络犯罪行为。

对此,从优化电子商务法

治化营商环境的角度,《白皮书》建议要强化跨域司法协作,发挥长三角一体化示范效应,同时充分发挥司法能动,积极参与网络犯罪综合治理,并加强涉电商网络犯罪联动防控。

“要联合互联网企业,加强大数据和人工智能技术的应用,提高治理效能。加大投入建立强有力的预警拦截体系,完善网络账号检测、预警、监督平台,充实高危网站、APP样本数据库,主动监测涉电商网络犯罪中的行为,从源头上遏制网络犯罪蔓延。电商平台自身要建立起涉案网络、域名以及可疑资金封堵机制,一旦发现网络违法犯罪行为,及时进行预警、资金冻结。”

在另一个层面,应由通信管理部门牵头、公安机关配合,严格落实网络实名和备案溯源等制度,重点针对物联网卡、海外卡采取有效监管措施,坚决杜绝“实名不真人”的问题。并大力整治恶意批量注册账号、冒用盗用他人账号信息等行为,综合采取多种生物特征识别、认证用户身份,确保登记信息真实准确、可溯源。

下一步,要全面推进网络犯罪治理法治化工程,坚持依法监管、依法自治、依法惩处相结合,帮助实现平台内部制度、平台风险管控、国家法律法规和政府网络监管的统一。

数据  
直接侵害电商平台权益案超七成