跨境『洗白』保税仓『镀金』

检察机关全链条打击新型直播售假产业链

□ 通讯员 苏双丽

“海外正品”“保税仓直发”……直播间里的诱人宣传，背后竟是一场精心设计的骗局。不法分子将境内生产的假冒品牌服饰，经港澳跨境转运、正规报关“洗白”，再以“海外专营店”名义在直播平台大肆销售，形成一条隐蔽性极强的新型侵犯知识产权犯罪链条。

近日，静安区人民检察院依法办理一起涉案金额逾3000万元的跨境销售假冒注册商标的商品案，斩断了“境内制假—跨境洗白—直播售假—资金回流”黑色产业链。

消费维权牵出假货谜团

2024年8月中旬，上海市公安局静安分局接到消费者举报，称其在某直播平台“海外专营店”花费800余元购买的2件知名品牌服饰，做工粗糙、LOGO与正品差异明显，经品牌方鉴定确系假冒注册商标的侵权产品。公安机关于同年8月下旬立案侦查，12月抓获犯罪嫌疑人匙某、孙某、陈某等人，在匙某住处查获假冒品牌服装340件，同步查扣其存放在国内某保税仓内的服装22000余件。

侦查初期，一个反常现象让办案民警陷入困惑：所有服装均从保税仓发出，报关手续齐全、入境流程完备，服装却是假冒品牌的。经多方核查，报关单和入境手续均真实有效，这让假货来源变得扑朔迷离。侦查人员随即调取涉案网店资金流水后，结合1名犯罪嫌疑人供述曾协助运送假冒品牌服装至珠海某指定地点，推测涉案商品可能是境内生产、转运出境后，再回流入境，利用合法跨境流程为侵权商品“洗白”“镀金”。面对作案手法新颖、侵权商品流转复杂等问题，公安机关主动商请检察机关介入。

2024年12月底，静安区检察院检察官依法介入，快速锁定案件矛盾点，并明确侦查方向。2025年1月，公安机关以涉嫌销售假冒注册商标的商品罪将匙某、孙某、陈某移送静安区检察院审查逮捕。

戳破“不知情”谎言

“李某给我看相关品牌授权资质，我以为货物是真的，就和他开始合作。”审查逮捕阶段，匙某一脸“无辜”地辩解。孙某、陈某也纷纷以“不知情”推脱罪责，案件侦办一度陷入僵局。

经查，该案由两个犯罪团伙协作实施：以匙某为首的团伙，靠着自行直播和与网红达人合作，在各大平台大肆推销“品牌服装”；以李某（另处）为首的团伙，则负责“幕后操盘”，伪造品牌授权资质注册海外专营店，联系假冒货源，统筹货物调拨，甚至通过报关入境的方式，为假货披上“正品”外衣。两个团伙分工明确、合作密切，借“海外专营店”直播噱头大肆实施售假骗局。

主观明知的认定，是破解本案的关键。承办检察官从客观证据入手，双管齐下还原真相。一方面，结合客服潘某等人供述、平台投诉记录、处罚决定书、闭店通知等书证，证实4名员工均知晓售假事实。“员工都能察觉的问题，作为团伙首领、负责出资和直播销售的匙某，不可能一无所知。”承办检察官结合证据链，反向坐实匙某知假售假的主观故意。另一方面，经海量数据核查，成功提取到关键证据，证实孙某和陈某在网店运营初期，就对售假事实心知肚明。

2025年1月，静安区检察院依法以涉嫌销售假冒注册商标的商品罪对匙某、孙某、陈某作出批准逮捕决定。同时，检察官围绕“核实各人分工、明确销售金额、深挖制假源头、查清货物流转模式”四大重点，引导公安机关补充侦查。

还原完整犯罪模式

2025年6月、8月，公安机关先后将匙某、孙某、陈某等十余人移送审查起诉。根据调查，匙某负责出资、直播销售、采购部分假货；孙某根据李某指令，伪造资质注册海外专营店、货物调拨和入境报关；陈某负责资金结算、换汇转账；其余8人组成直播团队，分别承担客服、运营、主播等工作，各环节紧密衔接，形成完整售假链条。

审查起诉阶段，匙某突然以“网店存在刷单，销售金额不实”为由辩解。检察官双管齐下开展核查，最终证实所谓的“刷单”仅为刷好评、提升店铺知名度，并未虚增销售金额，平台数据均为真实交易，匙某的辩解不成立。在此基础上，检察官还精准界定各嫌疑人知假售假的起始时间。

经审计，匙某销假金额2800余万元，孙某参与销假金额2800余万元，陈某参与销假金额2000余万元，其余8人参与销假金额1700余万元至230余万元不等，扣押假货货值金额291万余元。

为彻底揭开假货“洗白”内幕，检察官顺着跨境回流线索，逐步还原犯罪过程：涉案海外专营店需依托境内、外2家公司注册，并绑定境外账户，消费者支付人民币后，平台以美元结算且仅能通过境外账户提现，销售款经换汇后全部流入匙某、李某个人账户，用于支付货款、店铺运营等各项成本。境内生产的假冒服饰，先转运至珠海等地，再转运至港澳地区，后通过正规报关入境“洗白”身份，最终以“海外正品”名义，在直播间以进货价3至4倍高价售卖，隐蔽性极强。此外，综合全案证据，检察官判定本案属于个人犯罪，依法应当追究各涉案人员的刑事责任。

2025年11月、12月，静安区检察院以涉嫌销售假冒注册商标的商品罪，分别对匙某、孙某、陈某等11人提起公诉，涵盖资金提供、直播销售、货款结算、跨境转运等全环节人员。

无限技能、“一血”秒杀？销售游戏外挂获刑

□ 记者 王葳然 通讯员 尹逸斐

“花点小钱解锁无限技能，这款游戏外挂体验拉满！”游戏世界本应公平“对战”，却有人铤而走险销售非官方“外挂”，企图走捷径、赚快钱。近日，杨浦区人民法院审理了一起提供侵入、非法控制计算机信息系统程序、工具案件。

2022年5月至2025年3月，邓某为非法牟利，在未经某游戏权利人许可的情况下，伙同他人通过网店对外销售该游戏外挂软件，累计交易1万余笔，非法销售金额共计10万余元。经鉴定，上述针对外挂软件可使玩家角色在运行该游戏时，直接获得“超级无敌”“无限技能”“‘一血’秒杀”“100倍伤害”等违规特权，这些功能不仅破坏游戏平衡、干扰正常运营，也损害了普通游戏玩家权益。

杨浦法院经审理以提供侵入、非法控制计算机信息系统程序、工具罪判处邓某有期徒刑3年，缓刑3年，并处罚金3万元。

说法 >>>

随着网络游戏产业的快速发展，各类游戏外挂层出不穷，部分行为人误以为销售外挂仅属“灰色地带”，但事实上，此类行为不仅侵害相关权利人合法权益，还可能触犯法律，需承担相应刑事责任。

● 销售游戏外挂软件可能获刑

根据《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》的规定，专门用于侵入、非法控制计算机信息系统的程序、工具包括以下三种情形：（一）具有避开或者突破计算机信息系统安全保护措施，未经授权或者超越授权获取计算机信息系统数据的功能的；（二）具有避开或者突破计算机信息系统安全保护措施，未经授权或者超越授权对计算机信息系统实施控制的功能的；（三）其他专门设计用于侵入、非法控制计算机信息系统、非法获取计算机系统数据的程序、工具。

游戏外挂软件通常属于能够在游戏终端使用的由一系列代码集合编译而成的程序产品，在未经权利人许可的情况下，避开、突破计算机信息系统安全保护措施或者专门设计用于侵入、非法控制计算机信息系统、非法获取计算机系统数据的，即属于上述侵入、非法控制计算机信息系统的程序、工具。

● 违法所得达到一定数额属“情节特别严重”

根据《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》的规定，提供侵入、非法控制计算机信息系统程序、工具，违法所得达到人民币2.5万元以上或者造成经济损失人民币5万元以上的，应当认定为“情节特别严重”，处三年以上七年以下有期徒刑，并处罚金。

本案中，被告人邓某违法销售游戏外挂软件，涉案累计金额10万余元，已达到“情节特别严重”的数额标准，且交易1万余笔，覆盖范围广，其行为不仅破坏游戏正常运行秩序、侵害游戏权利人经营利益，更损害广大普通玩家的公平游戏体验，扰乱网络空间秩序。

法官提醒，网络游戏不应成为滋生犯罪行为的“温床”，任何试图通过破坏计算机信息系统安全、损害他人合法权益牟取非法利益的行为，都将受到法律的严惩。

责任编辑/徐荔 E-mail:fzb_zhoukanbu@163.com