

工本费10元的临牌为何“市场价”上千？

这起部督案中竟有全国多名“内鬼”参与

本报记者 陈佳妮 通讯员 胡湘

我国《机动车登记规定》明确,以购买等方式获得的机动车,在办理正式牌照前,须申领临时牌照(以下简称临牌)才能上路,但申请不得超过3次。可有人却盯上临牌的市场需求,做起了“灰色生意”,制作、倒买倒卖临牌,一张正规流程申领工本费10元的临牌,其“市场价”竟高达1200元。而这中间经手的不仅有中间商,还有公安系统的“内鬼”。

24日,永康警方发布这起部督案件。目前,专案组已抓获并采取刑事强制措施犯罪嫌疑人51人,扣押涉案电脑14台、涉案手机等移动设备63部,收缴违规临牌1000余张,追缴违法所得30余万元。

贩卖个人信息牵出秘密

2017年9月,永康警方收到线索,有人通过车牌号码查询公民身份信息,并予以贩卖。一路追查,警方发现贩卖个人信息的,是杭州人陈某。

陈某在上海经营一家公司,主要从事车辆买卖、抵押、代办上牌等业务。深入调查后,警方发现,陈某与多家中间商、多名车行业务员和微商以及同类型的车行除了凭车牌查询车主信息外,还存在制作、倒买倒卖临牌的违法行为。

按照规定,对于无正式车牌又已申领满3次临牌、属于报废车等的机动车,无法再申领临牌。陈某等车行人员就瞄准了这个“商机”,伪造、买卖临牌。他们将需要制作临牌的信息如车主的身份证复印件、发票扫描件、车辆合格证等,通过中间商传递到在车管所工作的“内鬼”处,等临牌制作好再寄回到最下游人员。这样一张临牌的制作费,经过层层加价,价格高达上千元。

而且,中间商为了向陈某等人证明临牌

的真实性,还会找其他地方的“内鬼”进入公安系统查档,调取该临牌的档案图留存。

警方发现,“内鬼”涉及全国多个省市。

“临牌”“查档”构成犯罪网

陈某在这个行业里只是个“二道贩子”,他有个河北上家贾某,人称“贾老板”,手里的资源号称“贯通”全国。

每天,“贾老板”的微信都跳个不停,大多是“车务代办”等微信群和微信好友,内容或是制作临牌所需的信息,或是收到微信转账的提醒,或是查档反馈的照片。各路消息从江西、广东、上海等地通过网络汇聚河北,又在“贾老板”的转发下被传递到全国各地。而一条条信息,在来来往往中,最终变为一张张临牌。

至被抓时,“贾老板”在3个月内经手的临牌已达50余张、查询公民信息1200条,共获利50000余元。

通过“贾老板”的手机,警方找到了帮他查档的“内鬼”——广东梅州一派派出所辅警孔某。他利用自己的职务之便,仅帮“贾老



板”查档,一个月就能非法获利5000元。同时,孔某还将每条公民信息以4元至15元不等的价格,出售给“贾老板”等中间商。

与孔某在同一单位工作的辅警赖某也是“内鬼”。由于在交警部门工作,他能查到的车辆信息也更多。两人便与一些车辆抵押贷款公司“合作”,帮公司查询车辆的登记信息、车辆状态、抵押信息等,方便这些公司能够“精准”地开展车辆贷款业务。从警方调查来看,这两人至少从2017年12月便开始出售公民个人信息,目前已查实销售公民信息4000余条。

奔赴15省市抓获51名嫌疑人

今年3月,永康警方在河北石家庄抓获贾某后,随即成立专案组进行侦查,以“临牌”“查档”为两条主线,揪出涉案的“内

鬼”、中间商,并于4月初抽调精干民警,组成5个抓捕组分赴江西、河北、江苏、上海、广东、海南6省市开展行动。

在贾某、孔某等13人相继落网后,专案组提取、分析犯罪嫌疑人的微信聊天记录、交易往来等,将上下家的关系梳理、汇总,并随着侦查的深入,不断补充新的目标。

今年6月,该案被公安部列为挂牌督办案件。经过调查,永康警方7月再次以永康为起点,赶赴湖南、湖北、福建、陕西等14省市开展抓捕。

在这6个月的专案经营中,永康公安共派出100多名警力、20个抓捕组,分赴全国各省市,行程上万公里。

目前,抓获的51名犯罪嫌疑人因涉嫌侵犯公民个人信息罪,伪造、变造、买卖国家机关的公文、证件罪被永康警方采取刑事强制措施。案件还在进一步深挖中。

销售抢红包作弊神器敛财逾千万

“新发明”用错地方被追刑责

《检察日报》沐杰 包婧

近日,经江苏省泰州市姜堰区检察院提起公诉,一起涉案金额逾千万元的编写、销售微信“抢红包”外挂程序案宣判,戴某、郑某等10名被告人因犯提供侵入、非法控制计算机信息系统程序、工具罪均被宣告缓刑,各并处罚金,同时追缴犯罪所得合计1000余万元。

新发明成非法获利武器

戴某和郑某是福建省某高校计算机系在读学生,关系不错,都对计算机编程非常感兴趣。

近年来,微信群“抢红包”游戏兴起,其中一种叫“捕鱼”的玩法更是吸引了不少玩家。群成员发出固定数额红包,并约定一个数字为“雷”,若某个玩家抢得红包金额的末位数为“雷”,则要全额返还红包给发包人。2016年7月,郑某接触到这种游戏后觉得新奇,便找戴某一起琢磨。随后,两人编写出一套用于微信“抢红包”外挂程序代码,不仅可以自动抢红包,还能自动识别红包金额、避免抢中“雷”。两人尝试后屡试不爽,收益颇丰。

2016年9月,戴某在与网友杨某闲聊

中提到了“秘密武器”,杨某当即觉得有利可图,极力建议通过网络销售赚一笔。

杨某的话让戴某很动心,便与郑某商量后搭建了专门的服务器用于软件管理维护。由杨某作为“总代理”,通过网络招募下级销售“代理”团队,并约定了利益分成。同时,他们还给这款外挂程序起名“教父”。杨某等通过各网络社交平台,以广告推广的形式推荐“教父”,形成了一条灰色“产业链”。

“教父”外挂程序本身是免费安装的,但是由于戴某、郑某加了密,玩家必须向“代理”购买授权码才能正常使用。“教父”授权码最初以100元价格由“代理”对外销售,收益逐级分成。后来团队成员看销路不错,又将每个授权码的价格涨到了120元。短短9个多月时间里,累计销售金额达1000余万元。

核查犯罪数额 审查报告长达8万字

2017年5月,公安机关在办理系列“抢红包”赌博案件中发现相关线索,先后对戴某、郑某、杨某等“教父”程序编写、销售团队成员立案并采取强制措施。由于涉案人员较多、交易数据庞杂,加之犯罪主要通过线上交易方式,在证据把握和数额认定上较为困难。同年9月,该案移送姜堰区检察院审查起诉。

要做到事实清楚、证据确实充分,犯罪嫌疑人的账目往来必须要查清。根据涉案人员身份信息,检察官将他们的支付宝账号、微信账号、银行卡的注册信息、登录日志、转账记录和流水账单等全部调取到位,但面对一大摞资料,还是让人感到无从下手。

提审过程中,“教父”销售团队成员刘某的一句话引起了检察官的注意。他供述称,为了理清成员各自应得的“收益”,团队组建后不久即约定销售所得由他统一收发。

是否可以将刘某的账户往来情况作为核查犯罪金额的突破口?检察官行动起来,调取其所有账单流水,并将其他人的资金往来情况与之对应起来,制成表格,再一项项核算。很快,每个人的获利情况逐渐明朗起来。

在审查网上转账记录时,检察官意识到,既然是线上交易,很可能存在相关聊天记录。他们根据聊天内容、账户往来情况确定销售记录,再将40多名证人的证言与调取的聊天记录、犯罪嫌疑人供述等相互印证,形成完整的证据链,厚厚的一本审查报告长达8万余字。

多方研究论证 确定案件性质

编写、销售“抢红包”外挂程序系新类型案件,目前尚无明确的司法解释可参考,也没有案例判决可循。检察官多方查找资料,将相关计算机网络犯罪案件的审判情况反复研究,还将案件全部争议焦点一一列出,逐个分析。最终,检察官认定相关被告人的行为均涉嫌提供侵入、非法控制计算机信息系统程序、工具罪,应当追究刑事责任。

该案办理期间,检察官专程前往腾讯公司听取技术部门负责人意见;实地查看鉴定流程演示,直观了解微信数据保护机制和“抢红包”外挂程序代码的运行方式。在庭审中,检察官主动申请鉴定人出庭,就专业领域问题发表意见。经多次开庭举证、质证和法庭辩论,面对有力的证据和充分的说理,该案被告人均当庭认罪,于判决前主动退还部分犯罪所得。