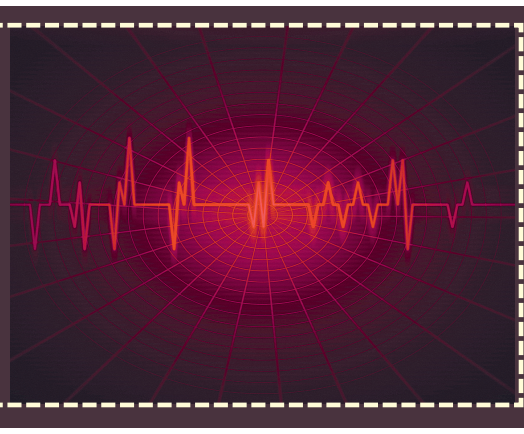
## 小伙应聘厨师偷渡境外,加入诈骗团伙成为“枪手”,落网后说自己没骗过人

# 声纹鉴定让他当庭认罪

《扬子晚报》刘浏 孟杰 陆吟秋

偷渡出境做了一个多月厨师的陈某,嫌收入太低,主动加入诈骗团伙成为“枪手”,7个月非法获利20余万元。然而,被抓后的陈某,却矢口否认在境外团伙中从事过诈骗。江苏警方经声纹鉴定比对后,确认了陈某的犯罪事实。近日,经江苏省海安市检察院提起公诉,海安市法院一审采信声纹鉴定比对的结果,以陈某犯诈骗罪,判处其有期徒刑3年,并处罚金5万元。



### 境外诈骗团伙厨师,改行做了“枪手”

2020年9月,时年33岁的陕西省安康男子陈某,被某网站一则“高薪招聘厨师”的广告吸引,乘坐飞机到达云南芒市后,又坐出租车到达瑞丽,在与招聘人“阿亮”见面后,他才知道工作地点在缅甸。为了高收入,加上云南离缅甸也不远,陈某便一口答应。

随后,在“阿亮”的引导下,陈某来到中缅边境,跟一名缅甸人碰头后,穿越一片树林和一条河沟,最终偷渡至缅甸,并被接应人带至一门前有人扛着AK枪站岗的院子里,开启了切菜、炒菜、上菜的厨师工作。

一段时间后,陈某逐渐熟悉了院子里的情况。他入职的这家公司,是一个境外电信诈骗团伙,院门前站岗的是雇佣兵,专为团伙看门把风,收取保护费。

一天,陈某看到有员工就餐时,直接把100万元人民币垒放在餐桌上,互相吹嘘一个月赚了多少万。想到自己一个月只拿7000元的工资,陈某也动起了歪心思。之后,他跟一个叫“阿贵”的员工套近乎,求“阿贵”带着他加入诈骗团伙,正式转行做起了诈骗团伙的“枪手”。

### 国内“断卡”及严厉打击,诈骗团伙“树倒猢狲散”

起初,陈某在“阿贵”手下做话务员,主要是根据公司提供的个人信息表,打电话给国内的“客户”(即被害人),询问是否有贷款需求,让有意向需要贷款的“客户”添加公司提供的QQ号,在“客户”添加后便将信息推给“客户经理”(团伙内称“枪手”),负责后续跟踪实施诈骗。

由于陈某口才较好,每天能打几百个电话,成功率也较高,每天会有七八个“客户”推送。一个月后,陈某就升级为“客户经理”,主要任务是引诱“客户”下载APP进行注册办理贷款。在“客户”注册并申请完毕后,通过更改银行账号,以“输错账号被银监会冻结、需要缴纳解冻金”等理由对“客户”实施诈骗。诈骗成功后,陈某会从“客户”转账金额中获取12%的提成。

至2021年4月底,因缅甸新冠肺炎疫情加重,陈某所在诈骗团伙内的大部分人感染了新冠肺炎,加上国内开展“断卡”行动,严厉打击电信网络诈骗犯罪,该团伙老大及骨干成员或感染新冠肺炎死亡,或纷纷跑路。该团伙运转不下去后,自行解散。而收不到保护费的雇佣兵,把陈某及未跑路的同伙包围起来。每人交了数千元保护费后,才得以离开院子。

在看到抖音上的反诈及回国自首的宣传短视频后,走投无路的陈某遂向云南瑞丽某派出所以非法出境为由投案自首,但隐瞒了自己的犯罪事实。

### 提前介入引导侦查,声纹鉴定成关键证据

而在陈某实施诈骗期间,海安市公安局接到市民小晨被网络诈骗14000元的报警电话。警方立案后,通过大数据锁定了犯罪嫌疑人陈某,陈某被抓获归案。到案后,陈某却矢口否认在境外有诈骗行为。

为此,海安市检察院及时提前介入该案,提出提取陈某的声纹通过全国信息库进行鉴定比对的意见,以引导公安机关侦查。今年年初,海安市公安局以陈某涉嫌诈骗罪移送海安市检察院审查起诉。期间,外省市公安机关比对出另外7起诈骗案中的录音声纹与陈某一致,警方决定并案处理。

承办检察官认为,声纹具有唯一性,且具有同一性,实验证明无论是故意模仿他人的声音或语气,还是故作耳语、低声说,即使模仿得再惟妙惟肖,声纹始终相同。从陈某的另外7起案件中提取多段语音,经过鉴定均系陈某一人所说,可认定为犯罪事实。

审查起诉期间,检察官依法对陈某进行了讯问,告知相关事项。但陈某前后供述只承认诈骗过小晨,拒不承认其他犯罪事实。而海安市法院一审开庭审理时,公诉人当庭播放提取的语音,提交鉴定人就声纹鉴定科学性和唯一性的说明询问笔录和同步录音录像。经过庭审质证答辩,陈某认识到自愿认罪认罚对自己最为有利,遂放弃不承认犯罪的态度,当庭表示认罪认罚。最终,法庭采纳了检察机关所指控的事实和量刑建议,遂作出上述判决。

## 犯罪团伙非法入侵电商平台篡改数据

# 将100元的充值卡改成50元狂赚差价

《检察日报》汪宇堂 郝凤冕 蒋帅

一团伙利用技术手段非法入侵电商平台,修改交易数据,进而牟利。经河南省南阳高新技术产业开发区检察院(下称高新区检察院)提起公诉,张某强等17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,非法获取计算机信息系统数据、非法控制计算机信息系统罪,分别被法院判处有期徒刑四年至六个月不等的刑罚,各并处罚金。被告人周某不服一审判决遂上诉。近日,法院驳回上诉,维持原判。

### 提前介入研判,幕后黑客露真容

2020年12月,南阳市城乡一体化示范区公安分局(下称示范区公安分局)接到上级公安机关的线索核查指令:近期,市内有不少用户在购买游戏装备或充值时,经销商会使用一款名为魔童的APP软件,通过入侵电商平台数据接口,修改交易信息,赚取游戏装备或充值费差价牟利。示范区公安分局将案情通报高新区检察院,并商请检察机关提前介入,引导侦查取证。

鉴于该案专业性高、隐蔽性强、案情复杂,高新区检察院报请南阳市检察院后,派出蒋文等检察官提前介入侦查活动,并与公安机关建立案件沟通协调机制。

蒋文认为,犯罪嫌疑人具备专业的制作侵害计算机程序插件以及非法侵入计算机信息系统的能力,形成了一条软件开发、销售、控制手机、入侵拦截、篡改信息、转移资金等各个环节分工合作的利益链条。

后经过大量线索比对、甄别、追踪,侦查人员将目标锁定在其中两名犯罪嫌疑人的所在地——河北石家庄和江苏南京。为进一步查明疑犯身份,侦查人员先后赶赴广东深圳、江苏宿迁、湖南郴州等地,通过大量走访摸排,最终查明了犯罪嫌疑人张某强,北京某网站技术总监、程序员毛某锋等6人的真实身份。这条以张某强、毛某锋为主,利用恶意APP软件牟取暴利的黑色产业链条浮出水面。

### 转变策略跟进侦查,挖出背后同伙

2019年8月,张某强委托北京某网站技术总监毛某锋,开发了具有入侵性质的魔童APP软件。软件开发完成后,张某强、毛某锋伙同王某华、黄某旭等人,组成犯罪团伙,分别负责该软件的维护、推广等工作。

“作为犯罪团伙的主谋,张某强到案后不完全供述,不愿交代其下线犯罪行为,目的是隐瞒其犯罪所得,建议从张某强或毛某锋身上打开缺口。”在审查该案笔录时,蒋文向侦查人员提出了侦查意见。张某强认为与同伙定下“攻守同盟”的计谋被识破,终于低头认罪。

2021年5月,侦查人员奔赴湖南,在当地警方通力协作下一举收网,顺利挖出该网络犯罪团伙,并以涉嫌非法控制计算机信息系统罪对6人采取强制措施,扣押作案电脑23台、手机59部、银行卡28张。

经查,该犯罪团伙通过微信群向游戏充值代理商推广魔童APP软件,代理商购买软件安装后,在给客户办理游戏充值时,将平台售价100元的充值卡,通过软件非法入侵到电商平台的数据接口,拦截篡改交易价格为50元,然后按原价100元收取客户费用,通过低买高卖赚取客户的充值差价。

后又查证,广东省汕头市星空网络公司经营者黄某旭从张某强处购买了魔童APP软件,张某强收取220元月租及交易额5%的软件使用费,黄某旭通过该软件,利用上述手段给用户充值,从中非法获利37万余元。

### 边审查边补证,17名犯罪分子被依法判刑

2021年6月,该案移送高新区检察院审查起诉。高新区检察院邀请信息网络安全、网信犯罪侦查、电子数据取证、公安技侦大队的业务专家成立涉计算机专家咨询组,及时提供技术支持。

蒋文在审查中发现,与毛某锋有关的数据不连贯,便向公安机关发出调取证据材料通知书,要求公安机关恢复、调取相关数据,最终找到2020年1月至9月被毛某锋删除的价值达32.78万元的电子凭证。

由于张某强所涉犯罪数额的证据不充分,2021年7月,蒋文向公安机关再次送达补充相关证据的文书。警方从查获的电脑中及时调取了张某强等6人聊天记录和微信转账、网银交易明细,最终补全了对张某强量刑的证据材料。

针对该案,高新区检察院邀请专家咨询组召开案件讨论会,结合专家建议,办案人员对该犯罪团伙组织体系、运作模式、资金流向等进行认真梳理。

最终查实,该网络犯罪团伙共有17名犯罪嫌疑人,张某强等6人负责开发、维护、推广魔童APP软件;黄某旭等11人利用上述APP非法入侵电商平台数据接口,通过修改交易数据、赚取差价等方式,获取利润220万余元。检察机关依法对张某强等人提起公诉,法院作出上述判决。