

谁偷了98万部老人机的话费?

核心提示

诚信经营是商家的“立业之道,兴业之本”,也是社会主义核心价值观的应有之义。尤其在流量驱动的网络社会,商家与消费者隔空交易的时代,商家更应当坚持明码标价、信息互通,通过诚信经营取信于消费者。当前手机市场上的老人机,由于具有电池续航时间长、字体大、辐射低、使用简便、抗摔耐用、价格低廉等优势,成为受广大老年消费者欢迎的非智能老款手机,然而即便功能单一的老款手机也频频被不法分子盯上。江苏省常州市两级法院近日审结一起涉老人机话费被窃案,不法分子通过在老人机的主板中恶意植入扣费软件,私设服务器平台,远程控制手机进而通过秘密扣取话费的手段非法获利。这起犯罪同时符合盗窃罪及非法控制计算机信息系统罪的构成要件,法院最终以处罚更重的盗窃罪对涉案人员定罪判刑。

老人机扣费异常为哪般?

几年前,家住常州市金坛区的姚某为方便与母亲联系,为其母亲购买了一部老人机,主要用于接打电话。2022年2月,姚某为母亲的老人机充值100元话费,然而短短几天后该老人机就因欠费而无法继续拨打电话。

“母亲平常就用手机接电话,呼出电话很少,加之这款手机无法使用流量,不可能消费这么多的话费。”姚某觉得不对劲,当即拨打客服电话询问扣费明细,结果被告知该老人机订购了几个增值服务套餐,所扣费用为套餐费用。

然而,考虑到姚某及其母亲从未用该老人机订购过任何套餐,手机上也从未有过订购套餐的短信提示,姚某觉得该老人机可能被做了手脚,导致手机话费被不明不白地定期扣取,于是在2022年11月报警。

无独有偶,同住金坛区的江某也遇到过同样的闹心事。2021年左右,江某在当地一家移动营业厅帮其外婆购买了一部老人机。江某的外婆平时仅用该手机打电话,但江某却发现每月结算下来的话费大大超过了正常通话费用,查询账单后发现,该老人机也被莫名其妙地“订购”了手机增值业务。

金坛区警方调查后认为这不是孤立的个案,遂对全区范围内老人机话费支出情况进行调查,发现有50余部老人机均存在上述情况。这些老人机被人为非法远程控制后“自动订购”了增值业务套餐。

警方采用技术手段分析发现,这些手机的网络数据指向一台架设在广东

深圳的服务器,欧阳甲、毛某、蒋某杰等7人有重大作案嫌疑。后警方开展抓捕行动,将7名犯罪嫌疑人抓获归案。

警方经调查发现,被这台服务器远程控制的手机遍布全国各地,共涉及全国98万部老人机,机主共被窃取话费347.98万余元。

谁订购了增值业务套餐?

上述老人机的增值套餐并非机主主动订购,而是因手机被远程控制而被动“订购”,且机主并不知情。那么,是谁在暗地里订购并收取了话费呢?

案卷显示,现年39岁的欧阳甲是这起老人机扣取话费犯罪的始作俑者。欧阳甲早年曾做过手机增值业务代理商,熟悉手机开通增值服务的流程。欧阳甲明白,正常订购套餐需要机主本人操作,并对运营商发出的短信予以确认才能完成,因此要以订套餐的方式扣取话费,就需要远程控制机主的手机,且确保订购套餐的短信不发送到机主手机上,这样才能确保机主在不明就里的情况下被多扣话费。

早年,欧阳甲曾在网上购买了一份手机增值业务代码,发现只要将此代码植入到手机中,再通过服务器远程发出指令,就能达到在无需机主主动订购和确认的情况下暗扣话费的目的。

2018年,欧阳甲获取了一款暗扣话费的程序,后其委托他人将该带有恶意代码的程序烧录在功能机主板上,交给生产厂商生产后投入市场。不久后,其又找人制作了控制手机的后台程序——手机销售管理系统,准备远程控制

老人机后暗扣话费敛财。

2021年8月,欧阳甲与毛某、蒋某杰合谋,通过给被远程控制的手机设置短信和语音任务,操控手机订购SP业务并屏蔽相关短信,并利用订购的SP业务实施暗扣话费操作。

三人经商议,由毛某与SP运营商对接,获取增值业务通道号码、控制指令等参数,由欧阳甲将上述参数配置到其指使他人搭建的手机销售管理系统平台,该平台向带有恶意扣费代码的手机发送短信、拨打语音电话并通过二次确认参数拦截扣费信息,从而得以扣取被害人手机话费。之后由蒋某杰负责对接SP运营商收取违法所得,制作对账单与欧阳甲按照约定比例进行分成。

2022年7月,欧阳甲让其弟弟欧阳乙负责与毛某对接,根据毛某获取的通道号码、二次确认短信等信息对服务器后台进行配置。

以犯盗窃罪判处刑罚

欧阳甲搭建的控制手机后台程序“手机销售管理系统”,可以查看任务下发记录、下发任务的种类(IVR业务或SMS业务),其中SMS任务可以设置永久拦截和截取扣费信息内容。

毛某证实称,屏蔽扣费信息是“暗扣行业”的规矩,因为如果下游不去屏蔽这些扣费信息,机主知道了就会投诉,暗扣SP业务就会因被运营商制裁而无法推进。毛某表示,其把这些增值业务代码和指令发给欧阳甲,就是为了屏蔽这些扣费信息,让机主看不到这些短信。

由于欧阳甲在功能机里内置了应用程序,其后续就可通过远程控制为机主订购SP业务。欧阳甲把毛某提供给他的SP业务代码和控制指令配置到扣费平台后,就可以在机主不知情的情况下订购SP业务,从而确保其通过暗扣话费赚钱。

据统计,2021年9月6日至2023年2月17日间,欧阳甲、毛某、蒋某杰等伙同丁某强、朱某庆等SP运营商(另案处理),共窃取被害人手机话费347.98万余元。SP运营商向毛某、蒋某杰转账“利润”206.95万余元,毛某、蒋某杰转账结算给欧阳甲“利润”167.9万余元。

2022年7月,欧阳乙受欧阳甲的指使,负责与毛某对接,根据毛某获取的通道号码、二次确认短信等信息对服务器后台进行配置,下发订购任务,其所涉盗窃罪犯罪金额共计218.06万余元,欧阳乙未实际获利。

该案经检察机关提起公诉后,江苏省常州市金坛区人民法院经审理认为,被告人欧阳甲、毛某、蒋某杰、欧阳乙伙以非法占有为目的,秘密窃取他人财物,数额特别巨大,其行为均构成盗窃罪,属共同犯罪。

2024年2月6日,金坛区法院作出一审判决,判决被告人欧阳甲、毛某、蒋某杰、欧阳乙犯盗窃罪,分别判处有期徒刑十二年、十年、八年和五年八个月,并处罚金人民币30万元、18万元、12万元和5万元。

一审宣判后,被告人欧阳甲、毛某、蒋某杰不服,提出上诉。江苏省常州市中级人民法院二审裁定驳回上诉,维持原判。

以案说法

触犯两种罪名 以盗窃罪定罪处罚

江苏省常州市中级人民法院刑二庭法官 戴明慧

本案四被告人基于非法占有手机机主话费的目的,通过非法侵入、控制手机信息系统,植入代码远程控制手机,在为机主提供增值服务的掩饰下,以机主不知情的方式秘密扣取机主话费,那么对四被告人通过技术手段恶意扣费的行为该如何定性呢?

首先,四被告人的行为构成盗窃罪。一方面,手机话费属于盗窃罪的犯罪对象。手机话费通过支付对价获得,由金钱购买所得,具有明显的财产属

性。另一方面,四被告人实施了秘密窃取公私财物的行为。欧阳甲指使他人将带有恶意扣费功能的代码植入手机,并通过服务器远程操控手机,自动发送短信、屏蔽扣费提示,在机主不知情的情况下为其秘密订购增值业务,扣取机主话费,符合盗窃罪的特征。

其次,四被告人的行为同时构成非法控制计算机信息系统罪。四被告人实施的写入恶意扣费代码并远程操控他人手机的行为,符合非法控制计算机信息系统罪的犯罪构成。

也就是说,本案四被告人实施犯罪的行为触犯了盗窃罪,其手段行为又触犯了非法控制计算机信息系统罪。按照我国刑法有关规定,非法控制计算机信息系统罪的最高刑为7年有期徒刑;相比较而言,犯盗窃罪数额特别巨大的,可以判处10年以上有期徒刑或者无期徒刑。

本案中,虽然四被告人针对某一机主的窃取金额尚未达到较大,但鉴于其持续对不特定对象实施犯罪,非法获利总额达数百万元,属于数额特

别巨大,符合犯盗窃罪“处十年以上有期徒刑或者无期徒刑”的量刑规定。因此,按“择一重罪处罚”的原则,本案应以盗窃罪定罪处罚。

针对当前手机消费市场存在的损害消费者权益的“隐形收费”现象,手机生产商、运营商、通信公司要坚持诚信经营,杜绝消费欺诈;各监管部门和司法机关应齐抓共管,形成合力,坚决打击各种违规收费现象,对于构成犯罪的违法经营行为露头就打,切实维护广大机主的合法权益。