利用“短信嗅探”技术实施网络侵财犯罪行为的定性研究

姚山春

(华东政法大学 刑事法学院,上海 200042)

摘要:近年来,利用“短信嗅探”技术进行网络侵财的案件频频发生,相较于传统的网络侵财案件,此类案件在行为上更具隐秘性和技术性。然而,考察该类案件的技术原理和行为模式,不难发现,该类犯罪行为定性的内核仍然是信用卡诈骗罪和盗窃罪的界分。在定性时,应当先明确“嗅探”盗刷行为的对象是信用卡账户还是第三方支付平台账户,如果为信用卡,应定性为信用卡诈骗罪;如果是第三方支付平台账户,应定性为盗窃罪。

关键词:短信嗅探;第三方支付平台;信用卡;诈骗罪;盗窃罪

中图分类号:D924.35 **文献标志码**:A **文章编号**:1672-349X(2021)04-0046-07

DOI:10.16160/j.cnki.tsxyxb.2021.04.006

Qualitative Research on Property Crimes on the Internet with SMS Sniffing Technology

YAO Shan-chun

(School of Criminal Law, East China University of Political Science and Law, Shanghai 200042, China)

Abstract: In recent years, there have been so many cases where “SMS sniffing” technology are used for property infringement on the Internet. Compared with the similar traditional cases, they are more secretive and technical in behavior. However, by examining their technical principles and behavioral patterns, it is not difficult to find that the qualitative core of such crimes is still the distinction between credit card fraud and theft. When they are classified, it should be clear whether the“sniffed”object is a credit card account or a third-party payment platform account. Correspondingly, it should be classified as a credit card fraud when the object is the former one and a theft for the latter one.

Key Words: SMS sniffing; third-party payment platform; credit card; fraud; theft

一、引言

传统的网络侵财犯罪模式大都表现为,受害人点击一个钓鱼网站的链接,键入自己的账户和密码,钓鱼网站的设立者,也就是犯罪行为人,借此让受害人误以为双方达成了交易,而划走受害人账户内的款项。但近年来,随着移动支付以及手机号码实名制的推广,使用短信验证码进行用户身份验证,进而完成网络支付的形式被普遍应用于各大软件平台,由此犯罪行为人使用“嗅探”技术获取用户短信内容,并结合其他渠道获取用户身份信息、银行卡号,从而实施盗刷银行卡、转移支付平台账户资金的新

作者简介:姚山春(1997—),女,广西玉林人,硕士研究生,主要从事刑法、刑事政策、刑罚学研究。

型网络侵财犯罪模式则开始出现。2018 年 12 月 31 日,到广西柳州出差的李某,在入住的酒店醒来后,发现银行卡内的 7 万多元不翼而飞;两天后,家住柳州市荣军路某小区的何某,也在一夜之间被盗刷了 3 万多元[1]。相较于普通的网络侵财案件,“短信嗅探”案件转移财产的行为表现得更为隐秘,往往在受害人未察觉的情况下,钱款就已经被转移。

由于“短信嗅探”类侵财案件行为具有隐秘性与独特性,在实践中,于公安机关而言,在侦破上有技术难度;于检察机关、法院而言,在罪名认定上尚有理论争议。因此,本文通过阐释“短信嗅探”的技术原理与行为模式,并结合具体案件所呈现出的裁判争议,对利用“短信嗅探”技术实施网络侵财犯罪的行为进行具体的分析,具有一定的理论与实践价值。故以此文作抛砖引玉之用,为当前尚无定论的此类案件的定性提出微薄建议,以助力于此类案件的治理与防控。

二、“短信嗅探”的技术原理及行为路径、模式

(一)技术原理

“短信嗅探”技术是在不影响用户正常接收短信的情况下,通过植入手机木马或者借助伪基站的方式,截获用户短信内容的一种技术手段。现下多发的“短信嗅探”侵财案件主要表现为在受害人毫不知情的情况下,相关联的银行卡或移动支付平台中的资金被盗刷或转出①,换句话说,“短信嗅探”的过程不与手机和受害人产生物理接触,此类“嗅探”行为需要借助伪基站等特殊设备进行。故笔者在此仅简要介绍伪基站类“嗅探”行为的技术原理。

了解短信传输的过程是理解“短信嗅探”原理的基础。简单来说,短信的传输呈现这样一条路径:短信－短信业务中心－手机所在范围内的基站－手机,故而,通常情况下,用户需要通过接收运营商基站所发送的信号进行通信,基站在短信传输的过程中担任着重要的角色。然而,国内的短信运营商在提供短信服务时使用的是 2G 信号,2G 信号存在着单向鉴权②的漏洞,在 2G 通道内,用户的短信是不被加密的,因此给了“短信嗅探”可乘之机[2]。犯罪行为人借助伪基站,利用 2G 移动通信网络的缺陷,截获该区域内手机用户的短信内容[3]。尽管 5G 时代已经到来,手机用户基本告别了单向鉴权,但是犯罪行为人仍然可以实施“短信嗅探”,原因在于,行为人利用“强制降网”的技术手段来使伪基站的作用得以发挥。通常,行为人使用一台经过改造的 2G 手机,将其与电脑连接,进而通过这种特殊的电磁设备实现通信信号干扰,将 4G,5G 等信号强制转为 2G 通信模式,然后开始进行“短信嗅探”[4]。

总体而言,“短信嗅探”的技术原理在于,利用 2G 信号单向鉴权的漏洞,打击一定范围内的网络信号,将其强制降维至 2G 通信模式,进而使用户误以为伪基站为运营商基站,短信的内容便被伪基站截获。

(二)行为路径

“短信嗅探”主要的行为路径分为四步。

第一步:找寻目标号码群。由于将网络信号进行降维的区域有限,伪基站对运营商信号的干扰也就只能维持在一定范围内,所以意欲进行“短信嗅探”的行为人首先要获取作案区域的目标号码群,来锁定作案对象。一般而言,从截获的信号中,行为人并不知晓短信接收方的号码,所以行为人在作案前会先通过其他“黑色”途径购买到某个区域的号主信息,进而锁定目标号码群。

第二步:信号干扰。如前所述,大部分地区的网络信号为 2G 以上,因此,要使伪基站发挥

① 如在河北省唐山市的一起案件中,犯罪嫌疑人交待,他们是趁受害人夜间熟睡时,使用“短信嗅探”设备截获了用户手机短信内容。

② 单向鉴权,即只有网络对用户手机的鉴权认证,用户手机无法识别出基站的真伪,只能进行回应,这样伪基站就可以获得用户手机的识别码,可以向其发送短信并拦截收到的短信。

作用,需要在锁定作案区域后,通过改造过的设备干扰该区信号,将信号转为 2G 无加密模式。

第三步:截获短信内容。当作案区域的信号降为 2G 后,短信内容就能被伪基站截获,行为人就此获取运营商和平台发给用户的短信验证码。

第四步:盗刷账户内资金。行为人利用先前购买的号主个人信息,以及某些网上银行或第三方支付平台的安全验证漏洞,登录这些 APP,进而对银行卡或第三方支付平台的账户资金进行盗刷。

(三)行为模式

在现实生活中,"嗅探"盗刷的行为模式大致分为两种。

1.通过手机验证码登入银行账户,进而进行交易,再利用退款机制获得钱款

在高晓特盗窃案中,被告人高晓特利用"嗅探"设备拦截了受害人卜某手机银行登录验证码,伙同网上联系的同伙盗刷卜某卡内的 10 200 元后,通过北京途牛国际旅行社有限公司网购 5 张机票,然后又通过退票将 10 200 元退到指定账户上,高晓特分得赃款 4 350 元;而后高晓特采用上述相同的方式伙同其网上同伙盗刷受害人丁某某 2 000 元,通过"高阳捷迅"给加油卡分两次充值 2 000 元,再进行退款,高晓特分得 800 元。审理法院认为,被告人高晓特盗窃他人财物,数额较大,其行为已构成盗窃罪①。

2.利用验证码,借助支付平台或他人信用卡平台转账直接获取钱款

在"于永胜、杨俊航、虞利龙信用卡诈骗、盗窃案"中,被告人于永胜使用从被告人杨俊航处取得的作案工具"嗅探器"等设备,在北京市大兴区、河北省唐山市等地,非法获取他人手机号码及验证码,窃取他人信用卡及其他财产账户内钱款,并将其中部分钱款直接转至被告人杨俊航的支付宝账户,由被告人杨俊航从中提取好处费后再转回至被告人于永胜的支付宝账户。被告人虞利龙与被告人于永胜共同实施上述活动,并帮助被告人于永胜取现。被告人于永胜、杨俊航窃取他人信用卡信息通过互联网、通讯终端使用的金额共计人民币 29 325.63 元,窃取他人财产账户内钱款金额共计人民币 57 355.37 元;被告人虞利龙参与窃取他人信用卡信息通过互联网、通讯终端使用的金额共计人民币 27 928.63 元,窃取他人财产账户内钱款金额共计人民币 51 474.37 元。审理法院认为,被告人于永胜、杨俊航、虞利龙以非法占有为目的,冒用他人信用卡,进行信用卡诈骗活动,数额较大,其行为均已构成信用卡诈骗罪,依法予以惩处;被告人于永胜、杨俊航、虞利龙以非法占有为目的,盗窃公私财物,数额较大,其行为均已构成盗窃罪,依法予以惩处②。

不难发现,"嗅探"盗刷的行为实质,就是使用获取的验证码破除第三方支付平台或手机银行的认证障碍,再利用受害人安全验证的漏洞,将钱款转移,占为己有的行为过程。尽管案件的表现形式各有不同,其行为内核却相去无几,然而对于行为的定性,裁判观点却因理论立足点的不同而大相径庭。如前述第一个案例,行为人的行为就被定性为盗窃罪;而在第二个案例中,审理法院将信用卡盗刷与第三方支付平台侵财两个行为分开定性,认为盗刷信用卡定性应为信用卡诈骗罪,而转移其他终端内账户余额则属于盗窃罪。因此,厘清"嗅探"侵财类案件的行为定性,对于司法实践而言,有其必要性和实践意义。

三、争议点的厘清

在实践中,关于利用"嗅探"技术侵犯他人财产行为的定性争议主要集中在信用卡诈骗罪与盗窃罪上,而对于这类行为如何进行认定,仅凭借直观的事实表象去对号入座现有的法条,或者参考大部分案件的处理方式进行判断是不合理的。要对一个行为进行认定,解开此罪与彼罪之

① 参见高晓特盗窃一审刑事判决书(2019)冀 0102 刑初 270 号。

② 参见杨俊航等信用卡诈骗一审刑事判决书(2019)京 0115 刑初 255 号。

间的纠缠,还需要从罪名的构成本身去论证。在进行构成要件符合性分析之前,对于一些争议点的把握,也直接影响着行为定性的正确性。

(一)信用卡是否局限于现实持有

对于银行借记卡同样属于刑法中“信用卡”的范畴,理论和实务中并无疑义,但随着移动支付方式的普及,信用卡是否仅指具有实体形式的电子支付卡,是需要明确的。在移动支付方式出现之前,信用卡支付主要是实体支付或通过网上银行等方式进行,所以,对于行为中使用信用卡的认定不应当仅仅局限于实体的电子支付卡,此行为对信用卡的使用实际上是对信用卡资料的使用。例如,甲盗窃了乙的借记卡与身份证,记下相关信息后将借记卡物归原处。随后,甲持乙的身份证冒充乙向银行挂失,因信息准确,使工作人员信以为真,帮助甲将乙卡中的余额尽数转入甲的另一借记卡中,尽管甲没有现实地持有乙的借记卡,但实际上使用了乙的信用卡资料,宜认定为冒用他人的信用卡[5]。因此,当行为人破解了受害人的信用卡资料,然后通过网上银行的方式进行盗刷、转账,行为人的侵财行为并不因为其无法现实持有实体的信用卡而无法进行。同理,在移动支付方式出现之后,各大银行方出台了拥有无卡支付功能的APP,用户只需要在 APP 上绑定自己的银行卡信息,在支付时输入密码或手机安全验证码即可进行消费、转账等活动,在这个意义上,“信用卡”实际上已经在网络空间内被延伸,故而,在对网络侵财案件的定性上,不应当拘泥于信用卡是否被行为人实际获得,而应当讨论行为人是否对信用卡资料进行了掌握。此外,对于这一点,在最高人民法院、最高人民检察院《关于办理妨害信用卡管理刑事案件具体应用法律若干问题的解释》(下称《信用卡解释》)中也予以了肯定的答复。

(二)第三方支付平台账户能否被认定为虚拟的信用卡

“嗅探”侵财行为的另一模式即为利用手机验证码在异地、异设备上登录受害人的第三方支付平台账户,然后将账户内的钱款秘密转出。而对于第三方支付平台账户如何认定,同样影响着对侵财行为的定性。有观点认为,第三方支付平台从事的业务具有金融业务的属性,可以帮助用户实现汇款转账、投资理财、消费借贷等,其资金来源于金融机构,业务的开展也与金融机构联系密切,因此,应当将第三方支付平台视作银行业务开展的新渠道,将其在刑法中的地位等同于金融机构,当第三方支付平台账户内钱款被窃取,可以认定为冒用他人信用卡[6]。

笔者认为,上述看法值得商榷。首先,将第三方支付平台的账户拟制为信用卡,混淆了金融机构和非金融机构的概念。尽管第三方支付平台的资金来源于金融机构,其业务开展也依赖于金融机构的支持,但是,这并不能说明第三方支付平台的账户能够被认定为虚拟的信用卡。首先,刑法解释应当在字义所具有的可能范围内进行,将信用卡解释为包括借记卡,符合“信用卡”所应当具有的含义射程,将第三方支付平台的账户解释为信用卡,则略显生硬。其次,第三方支付平台在功能上看似同信用卡并无二致,然而其业务的进行却依赖着与金融机构的合作,其转账、消费、借贷的前提,是用户在平台上绑定了本人所用的信用卡,在此意义上,第三方支付平台的账户更像是电子钱包或电子卡包,用户将钱款存储在账户内,就好比把现金放置于钱包之中。最后,当第三方支付平台账户内没有钱款,用户仅依靠绑定的银行卡进行消费,第三方支付平台账户就相当于已经放入电子支付卡的 ATM 机,因为用户在绑定银行卡时已经进行了验证,再输入账户支付密码只不过是类似现实生活中刷卡消费的过程,实际上受到影响的也仅仅是被绑定的银行卡。所以,第三方支付平台的账户,在这种情况下相较于虚拟的信用卡而言,更像是虚拟的 POS 机或 ATM 机,其工具价值远大于其象征价值。

(三)冒用他人信用卡与机器能否被骗

冒用他人信用卡,一般表现为非持卡人以持卡人名义使用持卡人的信用卡进而骗取财物。根据《信用卡解释》第 5 条第 2 款第 3 项的规定可知,冒用他人信用卡的情形分为以下几

种:拾得他人信用卡并使用的;骗取他人信用卡并使用的;窃取、收买、骗取或者以其他非法方式获取他人信用卡信息资料,并通过互联网、通讯终端等使用的;其他冒用他人信用卡的情形。然而,理论界对于冒用他人信用卡的界定,仍然存在着不同声音。有观点认为,冒用他人信用卡,只限于对自然人使用,在机器上使用他人信用卡取款的,符合盗窃罪的成立要件[6]。也就是说,需要限缩在行为人对自然人使用他人的信用卡这个情况中,至于行为人对 ATM 机、手机应用等机器或程式使用的情况,不能被认为是符合信用卡诈骗罪构成要件的冒用他人信用卡,而应该是盗窃罪的非法占有他人财物的手段。产生这种分歧的根本原因在于是否承认机器或人工智能的独立性,换言之,即是否承认机器或人工智能可以被欺骗进而产生错误认识。

持机器可以被骗论的学者认为,并非所有机器都能被纳入侵财犯罪的语境当中去讨论,机器分为机械运作的机器、具有一定智能编程的机器和机器人三种类型。这些学者认为只有机器人才能够被骗,机器人是人们通过电脑编程赋予其部分人脑功能且能替代人脑开展相关业务的机器,例如 ATM 机等[7]。这些学者认为,ATM 机和第三方支付平台并非单纯机械运作的机器,它们经过了电脑编程,实际上承担着金融机构或支付平台的业务人员的任务。在移动支付并不普及时,柜台人员负责检验信用卡和持卡人的对应性,然后推进转账等业务的正常进行;移动支付普及后,经过电脑编程的机器在资金流转的过程中充当着柜台人员的角色,因此,这些机器实际上等同于柜台人员——柜台人员会被欺骗,这些机器当然也会被欺骗。

持机器不能被骗论的学者驳斥了上述观点。第一,对于机器来说,并不存在被欺骗的可能性,以 ATM 机为例,ATM 机通过读取电子支付卡上的信息,核对实际持卡人输入的密码与其被预设的信息库内的密码是一一对应之后,即默认该持卡人为卡主,此时,无论是谁,都可以从 ATM 机中取款。第二,诈骗罪的构成需要有权处分人产生错误认识进而对财产进行了处分,作为特殊法条的信用卡诈骗罪也不例外。此时,如果将机器拟人化,还需要机器产生错误认识,而机器本身按照预设的程序进行判断(我们可以理解为机器对取款行为做的是形式审查),无法产生错误认识。同时,还有学者认为,参照德日刑法理论,错误的意思表示需要立足于自然人而言,如果将财产处分意识的特性赋予智能机器,在实践上也很难界分盗窃罪与诈骗罪[8]。第三,在以对应卡号、密码为审核内容,而不是以卡号、密码、实际用户为审核内容的预设程序的前提下,行为人冒用他人的信用卡,并不属于诈骗罪构成要件所需要的虚构事实或隐瞒真相,所以智能机器完全不可能被骗[9]。

笔者认同机器不能被骗这一说法,但需要结合信用卡诈骗罪,对机器不能被骗的理解作一些修正。持机器可以被骗论的学者常以《关于拾得他人信用卡并在自动柜员机(ATM 机)上使用的行为的批复》(下称《批复》)①的认定来为我国《刑法》已经承认机器可以被骗进行背书,或者以《信用卡解释》第 5 条第 2 款第 3 项的规定来类推机器可以被骗,这是对司法解释的误读。《信用卡解释》,是解释主体根据立法精神、司法需要及社会政策对信用卡诈骗罪进行的诠释,不能应用到其他刑法条款之中,否则论证的逻辑将走向类推解释[8]。

四、行为定性

(一)“嗅探”盗刷银行卡构成信用卡诈骗罪

如前所述,利用“嗅探”技术对银行卡进行盗刷,除了直接使用手机银行外,还可以使用第三方支付平台转账进行盗刷。这两种行为模式下的“嗅探”侵财,都可构成信用卡诈骗罪。

第一,在现行的刑法框架之中,将“嗅探”手

① 《批复》认为,拾得他人信用卡并在自动柜员机(ATM 机)上使用的行为,属于《刑法》第 196 条第 1 款第 3 项规定的冒用他人信用卡的情形,构成犯罪的,以信用卡诈骗罪追究刑事责任。

机银行及其验证码进而盗刷银行卡,或者“嗅探”第三方支付平台及其验证码进而转移所绑定的银行卡内钱款的行为评价为冒用他人信用卡,符合信用卡诈骗罪对于冒用他人信用卡的规定,即可以评价为“窃取、收买、骗取或者以其他非法方式获取他人信用卡信息资料,并通过互联网、通讯终端等使用的”这一冒用的情形。第二,认为冒用的行为只能对自然人使用,有悖于信用卡诈骗罪罪名设置的初衷,也忽略了在冒用行为当中涉及的各方主体的关系。首先,信用卡诈骗罪被设置在《刑法》的“破坏社会主义市场经济秩序罪”一章中,其保护的法益不仅仅是公私财产,更重要的是社会主义市场的经济秩序。行为人“嗅探”截获了他人的账户和密码,一方面是对他人财产的非法占有,另一方面也是对金融机构与持卡人之间建立的金融秩序的破坏,单纯将此行为评价为盗窃罪并不能完整地体现对被该行为破坏的法益的保护。第三,当第三方支付平台仅仅作为转移他人信用卡内钱款的工具时,行为人所“嗅探”到的第三方支付平台的账户密码、手机验证码与手机银行的账户密码、验证码无异,第三方支付平台在这里仅仅作为支取信用卡的工具的延伸,故而,其行为内核也属于冒用他人的信用卡。

所以,“嗅探”盗刷银行卡,无论是通过手机银行应用盗刷,还是通过第三方支付平台盗刷,均可构成信用卡诈骗罪。

(二)“嗅探”转移第三方支付平台内钱款构成盗窃罪

上文中已经对第三方支付平台的性质作了相应的梳理,笔者认为,第三方支付平台账户及其钱款类似钱包与现金,当行为人“嗅探”转移了第三方支付平台账户内的钱款,实际上就是破坏了用户对钱款的占有,窃取了用户的财产。

第一,该行为符合盗窃罪的犯罪构成。根据《刑法》第 264 条规定,盗窃罪是指以非法占有为目的,盗窃公私财物数额较大或者多次盗窃、入户盗窃、携带凶器盗窃、扒窃公私财物的行为。首先,“嗅探”的行为人对他人账户内的钱款主观上有非法占有的目的。

第二,将该行为评价为信用卡诈骗罪破坏了法秩序的统一性。有学者认为第三方支付平台的账户可以被解释为信用卡,所以有些案件的裁判基于这种观点,将此类“嗅探”行为定性为信用卡诈骗罪。然而,首先,如前所述,第三方支付平台账户并不属于我国法律规定的信用卡的范畴,其运营的机构也并非金融机构,若将第三方支付平台账户解释为信用卡,等于间接在《刑法》上认可了第三方支付平台属于金融机构,这便与其他部门法的规定相悖,破坏了法秩序的统一性。其次,该行为并没有侵犯社会主义市场经济秩序。信用卡诈骗罪的法益为社会主义市场经济秩序,如果将该行为定性为信用卡诈骗罪,需要理解的是,第三方支付平台账户间余额的移转会不会造成信用卡秩序的混乱。以支付宝为例,根据《支付宝服务协议》,用户账户内的余额并不是被存放在以用户的名义开户的银行账户内,而是被存放在支付宝方名下的银行账户内,用户账户内的余额仅仅是用户占有的预付价值或债权,账户与账户间的余额发生改变,对支付宝方的银行账户没有任何影响,也就不会产生对信用卡秩序的破坏一说。所以,将该行为评价为信用卡诈骗罪缺乏有力的论证。

第三,该行为不构成诈骗罪。首先,尽管相较于 ATM 机,第三方支付平台的设定更为智能或更具科技感,但是将《批复》中关于信用卡诈骗罪的特别规定推及至诈骗罪,从而认可机器可以被骗或人工智能可以被骗,难以形成证明链条;其次,将对 ATM 机使用他人信用卡认定为信用卡诈骗罪,实质上是一种法律拟制,而非法律的注意性规定,如果类推至一般的行为,将会导致定性错误。

第四,支持机器可以被骗论的学者高估了现下第三方支付平台的技术成熟度,同时又忽视了第三方支付平台为保护用户资金所作出的技术努力。同样以支付宝为例,根据《支付宝服务协议》,支付宝方通过身份要素识别用户的身份,其将使用身份要素进行的操作、发出的指令均视为用户本人做出的。可见,支付宝方对于用户身份的识别也是基于预设的程序或编码,

并不能做出同自然人一样的反应。同时,为了应对用户信息被冒用的风险,支付宝方会基于不同的终端以及用户的使用习惯,采取多种验证措施进行识别,还会为登录设备添加数字证书或者使用一些生物识别信息进行身份要素的验证。然而,在用户对于保护措施的使用未能穷尽,仅仅采用手机验证码作为身份验证要素或支付指令时,对于支付宝方而言,是难以识别的,因为用户并没有完全开放支付宝方进行账号识别所需要的权限,比如在某些大额支付的场合,异设备登录的用户会被要求人脸识别,若此时用户没有开启允许"刷脸"的权限,支付宝方只能通过短信验证进行识别,这恰好使"短信嗅探"有了可乘之机。所以,应当看到,当信息的甄别途径已经物尽其用时,账户被冒用的可能性微乎其微。第三方支付平台基于预设的指令进行工作,实质上是在行使对用户指令的形式审查,将盗用者发出的符合预设程式的指令认定为第三方支付平台的"认识错误",是对第三方支付平台现下技术的错误预估,因为对于第三方支付平台而言,这是正确的运转模式,其不可能认识错误,也不能认识错误——第三方支付平台在用户注册之初便已经认可用户的身份,后续的冒用行为都只是基于第三方支付平台对用户身份的认可而借助第三方支付平台保障措施的漏洞,对用户账户内余额进行的秘密转移。

综上所述,"嗅探"转移第三方支付平台账户内的钱款的行为,应当定性为盗窃罪。

五、余论

除了盗窃罪与信用卡诈骗罪的纠葛,有时"嗅探"侵财案件还会涉及侵犯公民个人信息罪等。例如,在某些案例中,有行为人在共同实施盗窃的过程中专门负责提供手机号码机主的身份信息以及关联的银行卡信息,其行为已经符合侵犯公民个人信息罪的构成要件,且其行为是"嗅探"盗刷链条中的一环,此时,该行为人的行为构成牵连犯,侵犯公民信息是他的手段行为,"嗅探"盗刷是他的目的行为[10]。此外,在"短信嗅探"盗刷案件的侦办过程中,往往还会顺藤摸瓜牵扯出一些传授"嗅探"技术、贩卖"嗅探"设备的微信、QQ 群,因此,防治"嗅探"盗刷,不仅需要依靠用户对于安全保障措施的正确使用、平台和银行方身份验证环节的加强、移动通信方对于用户信息的保护,还需要公安机关对网络生态进行及时治理。

参考文献:

[1] 这种嗅探设备能隔空盗刷银行卡,有人一夜被盗刷 7 万[EB/OL]. (2019-08-22). https://www. chinanews. com/sh/2019/08-22/8934476. shtml.

[2] 熊纬辉,付樱. 利用"短信嗅探"技术实施网络侵财犯罪刍议[J]. 江苏警官学院学报,2019,34(3):53 - 59.

[3] 殷仁杰. 利用"短信嗅探"技术实施网络侵财犯罪初探[J]. 山西省政法管理干部学院学报,2020,33(2):98 - 101.

[4] 卡还在,钱没了! 小心"短信嗅探器"盗刷银行卡[EB/OL]. (2020-12-20). https://mp. weixin. qq. com/s/-gi6Ji1JPx_3h1Qm9tQaqw.

[5] 刘宪权. 新型支付方式下网络侵财犯罪性质认定的新思路[J]. 法学评论,2020,38(5):47 - 54.

[6] 张明楷. 刑法学[M]. 5 版. 北京:法律出版社,2016:803 - 804.

[7] 刘宪权. 论新型支付方式下网络侵财犯罪的定性[J]. 法学评论,2017,35(5):32 - 42.

[8] 赵运锋. 转移他人支付宝钱款行为定性分析:兼论盗窃罪与诈骗罪的竞合关系[J]. 华东政法大学学报,2017,20(3):90 - 96.

[9] 王榕. 诈骗罪与盗窃罪之厘清:私转他人支付宝账户钱款行为的定性研究[J]. 东南大学学报(哲学社会科学版),2019,21(S2):40 - 43.

[10] 利用短信嗅探设备获取手机短信南昌三被告人滥用高科技盗窃获刑[EB/OL]. (2020-11-20). https://www. pkulaw. com/pal/a3ecfd5d734f711d6e08f2bb9bb9896b524efb47ecfef751bdfb. html? keyword=%e5%97%85%e6%8e%a2.

(责任编校:李秀荣)