网络犯罪资金支付转移的查控与治理

程 科,王佳旋
(江西警察学院,江西 南昌 330100)

摘要:现代网络犯罪充分依赖非法网络支付手段进行资金结算,非法网络支付模式快速迭代发展,呈现出专业化、团伙化、智能化、国际化趋势。除传统卡对卡转账和第三方支付转账方式,网络犯罪资金新型转账方式包括通过非法第四方支付平台、"跑分"平台、虚拟货币充值等进行支付结算。网络犯罪黑色产业团伙利用互联网新兴技术与商业模式创新支付手段,逃避监管和风控,较典型的方式有限制资金交易时间、交易金额的化整为零、及时在支付方式上灵活调整,从而避开监管风头。针对非法支付结算乱象,公安机关在巩固对传统银行卡转账、第三方支付工具转账查控的同时,应根据各类非法网络支付手段,完善资金查控与预警监测;应严厉打击侵害公民个人信息犯罪;应推动相关部门协同治理,加强防范和监控;同时要加强网络犯罪危害的宣传,提高群众防范意识。

关键词:网络犯罪;网络犯罪资金;非法支付结算;第四方支付;"跑分"平台;虚拟货币
中图分类号:D918 **文献标志码**:A **文章编号**:2095-2031(2022)02-0032-06

当前,网络犯罪高发频发,网络诈骗、网络赌博、网络色情、网络水军、网络黑客、侵犯公民个人信息等违法犯罪活动严重侵害人民群众利益,影响我国政治经济安全和国家社会稳定。各类网络犯罪盘根错节,紧紧依托互联网上的推广、技术、物料供应、支付等关键环节,滋生进化出复杂的网络犯罪生态体系,形成了组织严密、分工明确、彼此依赖的网络犯罪黑色产业(简称网络黑产)。

一、资金支付转移在网络犯罪生态体系中的作用

网络犯罪黑色生态体系主要分为以下五大环节:一是宣传推广环节,重点包括搜索引擎竞价排名推广、微信公众号等即时通讯软件广告推广、短信群发推广、短视频App推广、软件分发平台推广等黑灰产业;二是信息类物料供应环节,重点包括银行卡四件套、企业八件套类资料、精准公民个人信息、计算机信息系统数据等信息类物料提供商等黑灰产业;三是工具类物料供应环节,重点包括手机黑卡、物联网卡、网络黑号、猫池、卡池、多卡宝、VOIP、GOIP、嗅探设备等工具类物料提供商等黑灰产业;四是技术支撑环节,重点包括违法犯罪App制作研发、网站开发维护、CDN加速服务、虚拟定位、服务器租赁商、网站域名技术服务、App加壳技术服务、伪客户端工具平台等黑灰产业;五是资金结算环节,重点包括第三或第四方支付渠道、"跑分"平台、卡商平台、电商平台、话费充值、地下钱庄、虚拟货币充值等黑灰产业。

在网络犯罪生态各环节中,资金结算环节为各种违法犯罪资金提供非法支付结算业务,在各类违法犯罪活动中起到了转移非法所得、隐匿犯

收稿日期:2022-02-27
项目基金:2020年度江西警察学院科研项目"违法资金新型转账方式与查控途径研究"(2020YB001);2020年度江西警察学院教学改革研究课题"公安信息化与大数据应用通识课建设"(202019B)

作者简介:程科(1981-),男,江西永新人,江西警察学院科技与信息安全系讲师,江西省经济犯罪侦查与防控技术协同创新中心副研究员,从事公安大数据应用相关研究;王佳旋(1983-),女,山西长治人,江西警察学院警察政治学院助教,从事心理学研究。

罪收益的基础性作用。非法支付和结算的地下金融生态复杂多元,与骗税、虚开、骗汇、逃汇、非法集资、涉恐、电诈、网赌、贪腐等上游犯罪交织,已成为其他犯罪链条的组成部分,危害日益加深加剧。在网络犯罪侦查中,资金支付转移是侦查部门关注的重点,通过对违法犯罪资金的数据调取、分析、研判、取证,回溯资金的来源,追踪资金的去向,顺藤摸瓜,打击黑灰产业链上下游,查控非法资金支付平台和工具,是公安机关实现"净网"的关键。但是,近两年来,违法犯罪分子为了逃避资金查控与追踪,实施了很多新型资金支付转移方式,非法第四方支付平台、"跑分"平台、利用虚拟货币转账充值、"卡密"转账等方式花样翻新,极大地增加了公安机关调查取证的难度。

二、网络犯罪新型资金支付转移方式

(一)非法第四方支付平台

非法第四方支付平台是指未获得国家支付结算许可,违反国家支付结算制度,依托支付宝、财付通等正规第三方支付平台,通过大量注册商户或个人账户非法搭建的支付通道。其一般方式为:先通过注册或购买空壳公司、个人第三方支付账号,以逃避监管,然后利用技术搭建聚合平台,为黑灰产收单,并从中赚取手续费。聚合支付企业本身一般并不持有人民银行颁发的支付牌照,因此游离在监管体系之外,其风险主要体现在信息安全、业务突破合法经营、资金结算、代理链条风险四个方面。聚合支付本身不违法,但如果聚合支付平台从事了资金结算业务,对商家的资金进行了截留,形成所谓的"资金池",就是违法行为,成为非法第四方支付平台。

在非法第四方支付平台中,犯罪分子采取注册多家"壳公司"的方式,向微信、支付宝等第三方支付机构套取支付通道,再将这些支付方式整合成一个二维码发给用户使用。犯罪分子通常以公司的名义与有大量转账需求的黑灰产上游签订了合作协议,约定手续费为转账金额的1%至3%不等,进行资金沉淀并不定期结算。为掩人耳目,犯罪分子通常将公司伪装成需要正常走账的生鲜超市、商城这样的普通商户,连接第三方支付平台,逃避第三方支付平台对接入的聚合支付的监管。[1]

(二)"跑分"平台

传统的网络支付方式,就是通过支付通道,把资金直接划转到对方的账号上。但2019年下半年,特别是央行发布85号文《中国人民银行关于进一步加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》,史称支付"最强监管"出台之后,第三方支付和正常的聚合支付通道被严厉监管,违法犯罪资金的转移只能另辟蹊径。这种背景下,类似"滴滴打车"的分布式的资金转移平台——跑分平台就兴起了。

1."跑分"平台架构设计。"最强监管"出台之前,假设一名赌客要往一个赌博网站充值10万元赌资,一般直接通过第三方支付工具转账给赌博平台的收款账户。如今,为了逃避监管和侦查,则需要一个中介平台找到多个账户帮他转账,而"跑分"平台就充当了这个中介平台的作用。"跑分"平台采取类似"滴滴打车"的方式,将大量上游犯罪产生的非法网络支付需求形成订单在平台上发布。比如上述赌客10万元的转账需求,"跑分"平台会将其分成10笔1万元的跑分订单在平台上发布,而注册了该跑分平台App的跑分用户,就在线上抢单(每单1万元),然后提供自己的支付通道(支付宝、财付通、云闪付账户等)为其转账,并获取佣金(约为1‰到5‰之间);而通过互联网上不特定的10位跑分用户的每笔1万元的支付转账,赌客总计10万的赌资以"化整为零、移花接木"的方式最终转给了赌博平台,不需要使用自己的账户就实现了赌资的充值。因为正常的支付通道被严厉监管,网络赌博等黑灰产对"跑分"平台的依赖性变得极强,愿意支付高额佣金。"跑分"平台从黑灰产(如赌博平台)的资金转账总额中将抽取约5%到10%份额的佣金。

跑分用户是互联网上不特定的网民,甚至有很多涉世未深的在校大学生。大量的跑分用户将自己的个人账户用于平台帮助转账,变成了"洗钱"和黑灰产的资金通道。通过这种架构设计,"跑分"平台作为支付中介,利用大量正常用户的金融账户进行收款,将违法犯罪资金(如赌资)隐藏在正常的资金流水中,从而逃避监管打击。[2]

2."跑分"的运营方式。从2019年至今,"跑分"的运营方式经历了"跑分App、网站、群组"等形式不断演化的过程。

犯罪分子最初采取开发平台和用户登录App的方式进行"跑分"运营,随着公安部的严厉打击,

2021 年“跑分”平台 App 基本下架,运营模式逐渐转变成“跑分网站”或“群组”。“跑分”网站涉及的资金量较“跑分”平台 App 相对小一些,但参与“跑分”的人员身份隐蔽性更强,犯罪分子通常在国外租用服务器,常年在国外运营;“跑分”用户必须通过翻墙软件才能登录这些“跑分”网站,相比“跑分”App 而言,其提供的“跑分”种类也少一些。

如今,又出现了大量无须建设网站,免去技术支持成本的跑分群组,群组是通过 QQ 群、微信、Telegram 等即时通信软件在网上联络,利用各种电商网站购物代付、点卡充值、平台打赏的漏洞进行“跑分”的违法犯罪组织。

3.“跑分”黑色产业链。目前,“跑分”这种资金支付转移方式已经形成以总代理、次级代理、上游犯罪、技术支持、码商、“跑分”用户、黑产、地下钱庄组成的完整产业链。其中,“总代理”是产业链核心,投入资金购买服务器、招募技术人员搭建支付平台,发展次级代理,寻找上游犯罪的资金支付业务;“次级代理” 向下发展码商并寻找需要通过支付平台进行洗钱的上游黑灰产接入平台,按交易金额的比例收取手续费;“上游犯罪”将付款、转账需求发布给支付平台,通过将付款链接跳转到“跑分”支付平台,收取从码商得来的保证金;“技术支持”为总代理搭建支付平台,并负责“跑分”平台(网站)的维护升级,按照平台功能收费;“码商”负责招募大量的跑分人员,收取跑分人员的押金,把保证金转账至上游犯罪指定账户后,又将跑分人员的付款页面通过黑产的功能转成链接放在 “跑分”支付平台上,按交易金额收取手续费;“跑分用户”在跑分平台(网站)抢单,利用自己的银行卡、第三方支付工具为上游犯罪指定的账户进行转账,赚取一定比例的佣金;“黑产”负责技术,暴力破解购物 App 的支付渠道,改变付款人并进行链接转接;地下钱庄再将总代理、次级代理、码商等的黑色收入进行洗白。[3]

(三)虚拟货币

在公安部开展“断卡”行动背景下,大量“实名不实人”的银行卡和手机卡被冻结,但是“断卡”行动暂时还未涉及虚拟货币领域,作为新型的支付方式,虚拟货币依托其特有的匿名性、去中心化,且尚未建立有效的监控手段和法规等特性,迅速成为当前黑灰产青睐的资金转移方式。

1.虚拟货币及监管措施。虚拟货币是数字货币的一种。数字货币是以数字化形式表现其价值属性,与实物货币相对应,泛指所有以数字形式存在、可以作为支付手段的货币,是电子货币和虚拟货币的统称。电子货币是法定货币的数字化形式,与法定货币等值,例如以磁卡形式存储的电子货币、央行数字货币等。虚拟货币是非法定机构发行的数字货币,一般在特定网络虚拟空间作为支付手段使用,但不具有法定货币的地位和价值(货币分类关系见图 1)。

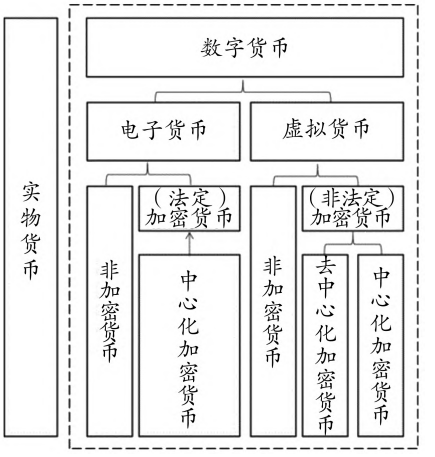

图 1 数字货币分类

目前,世界各国对诸如比特币等虚拟货币的态度因国家经济结构和监管政策不同有较大差异,我国对虚拟货币采取较为严厉的监管措施,规定虚拟货币是一种虚拟商品,不是法定货币,禁止虚拟货币交易。2013 年 12 月至今,央行、工信部等多部委联合发布了一系列公告和风险提示,防范以“虚拟货币”“区块链”名义进行交易炒作、非法集资、代币发行融资等风险。2017 年 9 月 4 日发布的《关于防范代币发行融资风险的公告》规定“任何组织和个人不得非法从事代币发行融资活动”,加强代币融资交易平台的管理。2021 年 9 月 24 日,国家发展和改革委员会、公安部、国家能源局等十部门发布《关于整治虚拟货币“挖矿”活动的通知》,将虚拟货币“挖矿”活动列为淘汰类产业,严禁以数据中心名义开展虚拟货币“挖矿”活动,一方面严禁新增虚拟货币“挖矿”项目,另一方面加快对存量“挖矿”项目的有序退出。同日,人民银行、最高人民法院、公安部等十部委发布《关于进一步防范和处置虚拟货币交易炒作风险的通知》将法定货币与虚拟货币兑换业务、虚拟货币之间

的兑换业务、境外虚拟货币交易所通过互联网向我国境内居民提供服务等虚拟货币相关业务定义为非法金融活动；明确虚拟货币投资交易活动的法律风险，任何法人、非法人组织和自然人投资虚拟货币及相关衍生品，违背公序良俗的，相关民事法律行为无效，由此引发的损失由自身承担，涉嫌破坏金融秩序、危害金融安全的依法查处。[4]2022年2月24日最高人民法院发布《关于修改〈最高人民法院关于审理非法集资刑事案件具体应用法律若干问题的解释〉的决定》将虚拟货币明确纳入非法集资案件的规制范畴。

2.使用虚拟货币进行非法网络支付。为逃避侦查，网络黑灰产的资金支付转移一般通过去中心化加密的虚拟货币进行，例如比特币、莱特币、以太币(Ether)、泰达币(USDT)等。以网络赌博为例，目前有四分之一的赌博平台可支持虚拟币的支付，最常见的有以太币(Ether)、TRON币和泰达币(USDT)。赌博平台会在支付渠道提供虚拟货币的支付接口和购买方式，指引赌客去购买和使用虚拟货币。

当赌客要进行充值时，将赌资(如人民币)在虚拟货币交易所兑换成虚拟货币，然后将虚拟货币作为赌资进行注册充值或结算。此外，虚拟货币还被用于互联网金融创新，比较典型的有质押挖矿模式、合约交易所模式、理财钱包模式、量化机器人交易模式、DeFi模式等，但这些模式无一例外都被不法分子利用，进行电信网络诈骗、网络传销、非法集资等犯罪。

除了上述三种比较典型的方式，网络犯罪非法资金支付转移手段还包括利用“卡密”转账、利用第三方支付的信用卡还款漏洞等各种方式，其目的都是逃避监管和风险控制。

三、网络犯罪资金支付逃避监管的方式

针对黑灰产资金链，各大银行和各大第三方支付公司都在加大监管和打击力度。为了逃避监管，非法网络资金的支付平台(如赌博平台)会采取各种措施对抗大数据风控，非法网络资金支付平台对抗监管和风险控制的方法有以下一些。

(一)限制资金交易时间

有些非法网络资金支付平台逐渐摸清了银行在时间上的监管规则，因此会相应地限制资金转账的时间，目的是为了在某些时间绕过银行的风控。比如发布提示信息，提示夜间21:30之后不可跑分的银行卡列表有**银行、**信用社等；或者通过程序设计，系统设置晚上22点开始禁止某些银行卡转账、凌晨0点之后限制交易金额、凌晨3点之后又逐渐开启等。

(二)交易金额的化整为零

有些非法网络资金支付平台将充值的整数自动变成小数结尾的金额，以规避风控，比如赌客充值500元，该收款界面显示的是499.75元。有些赌博平台接收在赌客充值的时候，会要求充值金额不能为整数，或充值金额结尾是8、9。比如，有些平台的收款界面会跳出提示文字“请使用1028,1238,1528等类似金额，成功率较高”或提示“请转账时务必增加小数点(如1000.68),以便财务查款”。

很多情况下，参与网络赌博的赌客在充值时，会进行大额资金的支付，但频繁的大额资金支付，会引起银行和支付机构的监测预警，因此，赌博平台会要求赌客在充值时把大额拆分成小额。比如规定一张银行卡单日流水不要超过20万，每笔资金不要超过1万，有些甚至要求将一笔大额支付变成300—5000元不等的多笔进行交易。

(三)在支付方式上避开监管风头

由于近两年第三方支付平台的风控系统做得比较完备，使用银行卡方式进行充值，更易于隐藏资金流水，所以，有些非法网络资金支付平台会重点推荐使用某某银行卡(特别是农村信用社)进行支付。比如，为了鼓励赌客使用银行卡支付，一些赌博平台会给予一些优惠政策，对使用银行卡进行充值的赌客，每笔加赠5%的优惠。

由于很多非法网络资金支付平台在收付款直接跳转到支付宝、财付通等第三方平台进行充值时，会被拦截和记录，于是平台会采取先通过第四方支付App，之后再跳转到支付宝等第三方支付工具进行转账充值的方式。[5]

而当借记卡和第三方支付被严厉监控时，非法网络支付平台又利用微信、美团、京东等平台的“信用卡还款”功能进行支付转账。相较直接使用借记卡转账，信用卡资金流水限制相对宽松，且这些平台都支持“为他人信用卡还款”功能，用户还款操作很方便，所以“信用卡还款充值”的形式在一段时间被大多数非法网络支付平台使用。

四、网络犯罪资金非法支付的治理对策

(一)根据各类非法网络支付手段,完善资金查控与预警

目前,公安机关可以通过“网联”接口查询第三方支付交易信息。针对非法第四方支付,由于其支付手段依赖第三方支付平台,因此,对于此类支付转移手段的调查取证,可以通过具体案件中聚合支付收款码的制作公司,联系该公司的法务部查询、调取收款码注册商户信息、注册资料、绑定的银行卡以及该收款码产生的交易记录。

“跑分”这种移花接木的非法支付手段利用资金支付者和转移账户的错位,为上游犯罪的违法资金提供了转移通道,扩大了洗钱的链条,增加了公安机关资金查控、追踪的难度。无论“跑分”的形式如何变化,其本质都是利用网络上不特定的用户账户,为违法犯罪资金进行支付和转移。由于“跑分”也依赖银行卡和第三方支付工具,要对“跑分”平台进行查控,应加强对于银行卡、第三方支付账户的开户使用等事前、事中和事后各个环节的监管,挖掘“跑分”资金流的规律,建立监测预警模型,有力提升对于黑灰产业资金结算全链条的动态查控能力。[6]

虚拟货币是资金电子数据的一种,侦查取证中应适用《公安机关办理刑事案件电子数据取证规则》和《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》的细则。由于虚拟货币在交易、存储和支付等环节一般使用密码技术进行算法加密,存在匿名性,资金流追踪难度较大。目前,虚拟货币的侦查取证一般采取钱包地址标注、嫌疑账户关联、资金路径追踪、交易平台调证等步骤方法。实践中,要根据侦查的需求进行交易路径追踪,精准定位嫌疑人的虚拟货币流出/流入了哪个交易所或平台,再通过合法的调证手续,对交易所或平台进行调证、取证。[7]

针对虚拟货币的查控,除了积极与科技公司合作,笔者认为,主管部门应出台虚拟货币的取证规则,对虚拟货币交易记录的电子提取、冻结、检查、认定,及其证据形式的固定、封存、移送等程序进一步明确;对虚拟货币取证、鉴定、展示、质证等方式方法做出规范;公安机关应完善虚拟货币预警监测平台,深挖线索;加强资金流研判,穿透虚拟货币的匿名性,锁定嫌疑人钱包地址。

(二)严厉打击窃取、出售公民个人信息等侵犯公民个人信息犯罪

非法支付结算是互联网犯罪核心的利益链条,根据非法支付结算的特征,无论是上游的“黄”“赌”“骗”等涉网犯罪,还是DDOS攻击、木马病毒、外挂等计算机犯罪和网络犯罪的实施,均得到了网络黑产供给链的全环节支撑。而恶意注册账号仍然是非法支付结算的源头。黑产团伙利用买来的“四件套”“八件套”等信息,恶意注册电商平台、发卡平台等账号,为网络犯罪黑产洗钱铺路。因此,侵犯公民个人信息作为网络犯罪的上游犯罪,应予以严厉打击。

要对侵犯公民个人信息犯罪的非法收集、提供窃取、交易、交换等整个利益链条进行全覆盖打击,深挖各类犯罪的相关利益链条。目前,对数据的窃取变成了黑灰产的重要部分。2021年被窃取的数据中,数据类型主要集中在各类平台的用户信息、公民个人信息、数据库账号、后台源码信息等。被窃取的数据,通常会被犯罪分子用Telegram或暗网交易,而购买这些数据的下游又将这些用户信息用于网络电信诈骗、广告推广和恶意商业竞争等。

同时,要进一步落实网站平台、网络服务商的网络安全防护责任,切实贯彻收集、使用个人信息的合法、正当、必要原则,对于未按法律要求、未落实相关义务,而导致公民个人信息泄露的,要予以严厉制裁。API(应用程序接口)作为承载数据流转和业务功能实现的核心,在2021年成为黑灰产攻击的焦点,也是致使数据被窃取事件频发的重要原因。很多平台对API管控不当,成为引发数据资产泄露的最大原因。这主要是企业数据流转节点的不断增多,导致大量无法感知到的API暴露在外,被黑产利用并进行攻击。公民个人信息泄露的另外两个主要原因是运营商/短信通道泄露和内部人员泄露导致,这也是行业对数据资产管理失范的后果。此外,应严厉打击平台企业超范围收集个人信息、超权限调用个人信息等违法行为,从严管控非必要采集数据行为,依法依规打击黑市数据交易行为。

(三)推动协同治理,加强防范和监控

目前,非法支付结算团伙正是利用了银行业金融机构、电商平台、互联网金融创新政策等各方

面漏洞,绕开支付机构的风控策略,为网络犯罪提供资金结算通道。非法支付手法模式快速迭代发展,呈现出专业化、团伙化、智能化、国际化趋势,与安全风控策略对抗愈加激烈。因此,对非法网络支付结算的治理应多方协同。

主管部门应从顶层设计上强化数字化监管支撑,建立非法网络支付违法线索线上发现、流转、调查处理等非接触式监管机制,提升监测预警、线上执法、信息公示等监管能力。2021 年 12 月,国家发改委、人民银行等九部委联合印发了《关于推动平台经济规范健康持续发展的若干意见》,明确指出要强化支付领域监管,断开支付工具与其他金融产品的不当连接,依法治理支付过程中的排他或“二选一”行为,对滥用非银行支付服务相关市场支配地位的行为加强监管,研究出台非银行支付机构条例。规范平台数据使用,从严监管征信业务,确保依法持牌合规经营。发挥行业协会作用,推动平台企业对网络经营者违法行为实施联防联控。加强和改进信用监管,强化平台经济领域严重违法失信名单管理。推动平台企业深入落实网络安全等级保护制度,探索开展数据安全风险态势监测通报,建立应急处置机制。[8]

公安机关要深挖打击为网络犯罪提供资金结算的非法网络支付机构及从业人员,紧盯“资金链”背后的黑产团伙,深入研判资金异常交易比较活跃的地区,部署开展专项整治,依法查办一批协助上游犯罪进行资金支付结算的非法团伙。还要会同主管部门建立常态通报机制,对每一起重大涉网案件所勾连出来的非法资金结算的线索及时通报,严肃倒查,进行全链条打击,同时也加大对地下钱庄、电信诈骗等各类上下游犯罪的并案的打击力度,切断黑灰产资金转移通道。商家平台和支付平台要跟踪和剖析黑产手法的演变过程,在治理和应对监管、法律风险方面要进一步升级打击策略,不断加强防范和分析,建立常态化审查机制,实现事先预警、事中阻断,事后修补漏洞;要借助大数据、人工智能等新技术完善安全风控体系,实现跨行业、跨政企联防联控,打破信息孤岛,履行好企业主体责任。

(四)加强网络犯罪危害的宣传,提高群众防范意识。

利用各类手段进行资金支付转移中涉及的账号,除非法获取大量公民个人信息外,网络犯罪团伙还通过招募各级代理,再由层层代理以兼职为名义,发展网上大量不特定的用户提供支付宝、财付通等第三方支付账号进行非法结算。如前所述,“跑分”平台这种使用普通用户的收款二维码为赌博网站提供非法结算服务,手法更加隐蔽,查控愈发困难。尽管刑法第 287 条之二规定了帮助信息网络犯罪活动罪(简称帮信罪)但现实生活中这些普通用户贪图小利,在不知不觉中成为网络犯罪活动的参与者。因此,要加强普法宣传,围绕各类非法网络支付的动向和特点,充分利用网络、电视、报纸、公众号、短视频等平台开展针对性宣传,提高宣传的受众面、及时性和精准度。同时还要建立快速发布机制,及时发现归纳网络犯罪的新手法、新伎俩,多种渠道发布预警提醒。要重点针对老年人、青年学生等群体,采取喜闻乐见的形式,有的放矢开展宣传。[9]同时,积极倡导广大群众积极检举揭发涉及网络犯罪的平台、商家,建立有奖举报机制,实现全民参与、全民防范,才能有效遏制网络犯罪的高发态势。

参考文献:

[1] 郑旭江,刘仁文.非法第四方支付的刑法规制[J].社会科学研究,2021,(2):126-129.

[2] 周喜庆.支付机构二维码收单业务洗钱风险管理初探[J].北方金融,2021,(11):35-37.

[3] 刘梦.“跑分平台”的刑法定性误区及其匡正[J].江西警察学院学报,2021,(4):5-7.

[4] 陈纯柱,李昭霖.数字货币犯罪风险的防范与应对[J].政治与法治研究,2019,(10):37-39.

[5] 赌博平台充值支付方式行为研究 [DB/OL].(2021-10-29)[2022-03-07]. 永安在线情报平台 https://www.163.com/dy/media/T1516788585342.html.

[6] 唐淑臣,刘英才,于龙.第三方支付洗钱犯罪侦查研究[J].江西警察学院学报,2021,(2):13-17.

[7] 谢玲.电信网络诈骗犯罪资金流查控研究[J].中国人民公安大学学报(自然科学版),2021,(2): 49-51.

[8] 牛超群.非法第四方支付平台及其数据治理对策[J].网络空间安全,2021,(3):29-31.

[9] 徐鹏.非法第四方支付平台的金融风险及治理对策[J].北京警察学院学报,2021,(2): 92-93.

责任编辑:张　艳