电信网络诈骗资金转移手段

及共生灰产的治理

韦 玮[[1]](#footnote-1)

**内容摘要：**电信网络诈骗犯罪作为现阶段我国发展最快的刑事犯罪，呈现出发案高、手法多、损失大、影响坏等特点，尤其是法律监管空白导致灰产泛滥、涉案赃款转移方式繁多，办案单位追赃挽损工作成效欠佳，受骗群众很难理解和满意，极大影响公安机关的执法公信力，甚至引发其他社会问题。本文结合侦查实践，围绕涉诈资金转移各个环节，归纳总结规律特点，列举涉案资金流水表现形式，分析资金转移的主要方式和共生灰产，对下一步打击治理策略进行思考。

**关键词：**电信网络诈骗 赃款 资金 转移 灰产 打击治理

“电信网络诈骗犯罪”并非我国刑法规定的一类罪名，业界普遍将其定义为一类新型的诈骗犯罪活动，其本质属于刑法第二百六十六条规定的“诈骗罪”，主要是指将传统的诈骗手段与现代通信和网络技术相互结合的一种犯罪手段或一种诈骗方式。在《人民检察院办理网络犯罪案件规定》、《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》、《电信网络新型违法犯罪案件冻结资金返还若干规定》等文件中，有关部门分别使用了“电信网络诈骗”“电信网络新型违法犯罪”等表述。2022年9月2日，在十三届全国人大常委会第三十六次会议表决通过的《中华人民共和国反电信网络诈骗法》中，将其定义为“以非法占有为目的，利用电信网络技术手段，通过远程、非接触等方式，诈骗公私财物的行为”。实践发现，无论“电信网络诈骗”、“网络盗刷”还是“裸聊敲诈”等手段，涉案赃款的转移藏匿方式和手段特点基本趋同。

因此，本文所研究的“电信网络诈骗犯罪”是指以电信网络诈骗犯罪为代表的，以非法占有受害人财产为目的，利用电话、短信、互联网等技术手段实施的各类电信网络新型违法犯罪行为的统称。

一、简述电信网络诈骗涉案账户的定义和类型

电信网络诈骗涉案账户，即与电信网络诈骗案件涉案资金有对手交易关系的资金账户，是诈骗资金转移、藏匿、洗白的工具和载体。现阶段电信网络诈骗涉案账户主要包含以下类型：

（一）个人银行账户。电信网络诈骗案件中，超过95%以上为涉案账户为个人银行账户。常见涉案个人银行账户主要是借记卡账户。但2019年开始，各地普遍出现个人信用卡（贷记卡账户）涉案情况，以2020年“断卡行动”后更为突出。随着“断卡行动”纵深推进，借记卡买卖行情“水涨船高”，犯罪团伙逐渐盯上个人贷记卡。因个人贷记卡账户开办不受账户开户和限额管理措施限制，涉案资金通过贷记卡账户转移，公安机关仅能对溢缴款部分进行止付、冻结，极大制约了涉案资金追缴效能。如G省E市韦××被诈骗案中，涉案资金23万元被分拆后进入5张三级账户，全部为个人贷记卡账户，犯罪分子通过提前刷POS机消费套现，再转入涉案资金“还款”的方式来规避公安机关资金查控措施。

(二）个人支付账户。支付账户是指获得互联网支付业务许可的支付机构，根据客户的真实意愿为其开立的，用于记录预付交易资金余额、客户凭以发起支付指令、反映交易明细信息的电子簿记。现阶段，支付账户仍存在实名制落实不到位、存在非属地化管理、账户管理制度不够完善、消费者对支付账户实名制认知不足等问题导致支付账户涉案情况普遍存在。

（三）单位账户/对公账户。涉案单位账户（也称涉案对公账户）主要是银行对公账户和企业支付账户。此类账户转账限额远高于个人账户，在“冒充公检法”、“冒充企业老板”等单笔涉案金额巨大的案件较为常见。在“放、管、服”背景下，市场主体登记程序放宽导致商业银行尽职调查时限被极大压缩，账户买卖问题很难完全杜绝；同时，非银行支付机构为满足自身发展利益，也存在单位支付账户实名审核不到位、使用不规范等问题，尤其是随着互联网经济发展，出现“××电子商务”“××科技”“××贸易”之类的电商企业支付账户大量涉案的情况。

二、涉案资金交易流水的表现形式

本文所研究的涉案资金交易流水，主要指办案民警视角下的涉案账户资金交易记录。当前电信网络诈骗案件涉案资金流水主要以三种表现形式存在：

（一）转账支付。转帐支付是通过银行(支付机构)把款项从付款人帐户划转到收款人帐户而完成的货币支付行为，分为三种情形：1.银行账户互转。即交易流水中交易双方均为银行账户，交易流水中常见备注为“转账”、“他行汇入”等。银行账户之间转账，包含同行和跨行两种情况，清算方式和过程比较简单，不再赘述。2.支付账户互转。即交易流水中交易双方均为第三方支付账户。根据相关监管条例规定，不同支付机构之间不能直接通过银行备付金收付户、存管户发生直接的资金往来。因此支付账户互转仅限于同一机构账户之间。3.银行和支付账户互转。一是银行账户转支付账户，即个人/企业账户转入备付金账户，支付机构予以“记账”的过程。二是支付账户转银行账户，即向支付机构“提现”，由备付金账户转入个人/企业账户的过程。

（二）特约商户消费。特约商户，是指银行卡收单业务中，与收单机构签订银行卡受理协议、按约定受理银行卡并委托收单机构为其完成交易资金结算的单位、商户或其他组织。特约商户通过收单机构POS机，可以实现非现金结算，即俗称“POS机消费”。目前，我国收单业务已发展成247家商业银行+70家农商银行+119家村镇银行+61家持牌支付机构和数量庞大的收单外包服务机构组成的线上线下全覆盖业务体系，但由于野蛮生展和监管滞后，现阶段POS收单市场存在非法套现、非法移机、切机等问题，是违法资金转移活动的天然温床。

（三）现金取款。涉案资金交易明细中，一般第五级卡以后开始出现现金取款，但自“断卡行动”以来，诈骗团伙获“卡”成本提高，在第二、三级卡就组织“车手”冒险取款的情况呈上升趋势。涉案资金通过现金取款方式转移，在银行交易流水中一般备注为“现金取款”、“ATM取款”等标识，并附终端设备号码供查溯。

三、当前电信网络诈骗犯罪资金转移的规律特点

（一）涉案账户“伪实名”现象普遍

涉案“一级卡”绝大多数为“伪实名卡”，即：犯罪嫌疑人通过各种渠道购买已经由他人实名认证开户的银行账户用于作案，案发后公安机关往往只能追查到卡主本人（即“卡农”）和组织收贩卡的“卡头”，较难发现幕后犯罪嫌疑人（实践中，对“卡头”组织“卡农”本人到场“刷脸”转账的方式一般也作为“伪实名卡”进行侦查研判）。笔者收集G省近年来100起电信网络诈骗案件中一到五级共4216个涉案账户信息发现，涉案一级卡“伪实名”比例最高，达到98.4%，随着涉案资金逐级转移，涉案账户的“伪实名”比例逐渐下降，至五级涉案账户时已有23.4%为真实卡主使用。之所以出现这种情况，是诈骗团伙利用“跑分平台”、虚拟货币交易、地下钱庄等进行涉案资金转移，具体在后文详述。

（二）涉案账户存在“试卡”行为，资金快进快出特征明显

随着我国移动支付技术的发展，各类移动支付产品加速了资金流转，在提高用户体验的同时，也方便了各类违法犯罪资金的转移。在对G省100起电信网络诈骗案件中4216个涉案账户信息发现，87.5%的账户在涉案资金进入后5分钟之内被转走；5-30分钟内转走的占9.3%；超过30分钟才转走涉案资金的占比不足3.2%，涉案资金账户总体呈现快进快出特点。约40%的涉案账户，在作案当天有小额转账的“试卡”行为，如：通过手机网银转账0.1元至红十字会等公益账户或其他个人和对公账户。

（三）涉案账户形式多样、数量庞大

在一起电信网络诈骗案件中，侦查员通常要追查超过十级以上的涉案账户，调取账户数量在几十个到几百个不等。以G省A市咸××被诈骗案为例，办案单位调取了涉案一级卡7张、二级卡14张、三级卡29张、四级卡57张，几乎涵盖个人借记卡、个人贷记卡、个人支付账户、企业银行账户、企业支付账户、POS特约商户等所有账户类型。



（四）涉案资金流水复杂、追查难度大

以G省B市刘××被诈骗案为例，涉案资金进入一级账户后被分拆成6笔进入3个二级账户，随后再次分拆成18笔进入5个三级账户。三级账户的资金流开始出现A地开户、B地转账、C地取现、D地消费、E地购买理财产品等跨空间、跨区域特征，并存在多次分拆汇聚。侦查员要对交易时间、对手账号、交易金额等多项数据进行分析处理，对办案经验和耐心是一项挑战。

（五）普遍存在“一卡多案、一卡多级”现象

通过对G省C市赵××被诈骗案涉案一级账户资金查询，办案民警发现该账户还分别接受了9个账户汇入资金，经查均来自9名不同受害人，同时该一级卡还作为另外3起案件的二级卡帮助转移资金。笔者将G省4216个涉案账户进行全国比对，共串出6219起案件，其中作为一级卡涉案1618个、作为二级卡涉案2035个、作为三级卡涉案1936个、作为四级卡涉案1860个、作为五级卡涉案2324个。单卡涉案最多40起、最少1起，平均2.3起，超过96的卡涉案数量在5起以内。超过92的涉案账户为多层级涉案关系，以2-3个层级涉案情况最普遍，仅有335个账户只作为单一层级涉案存在。

（六）涉案账户由大银行向小银行转移趋势明显

据统计，2021年1月-2022年4月全国涉案银行账户中，国有商业银行和全国性股份制银行涉案账户占比逐渐下降，而农村信用社/农商行涉案账户占比由2021年初提高近5个百分点，增速超过300%，涉案账户由大银行向小银行转移趋势十分明显。一些地方性村镇银行账户在开户审查和资金查冻等工作方面重视不足、投入不够，各项监管措施触达滞后，备受犯罪分子青睐。

|  |
| --- |
| 2021年1月-2022年4月全国涉案银行账户比例(单位：%) |
| 银行类型 | 1月 | 2月 | 3月 | 4月 | 5月 | 6月 | 7月 | 8月 | 9月 | 10月 | 11月 | 12月 | 2022年 1月 | 2月 | 3月 | 4月 |
| 国有商业银行 | 81.3 | 82.8 | 79.4 | 79.8 | 78.5 | 76.4 | 72.8 | 70.8 | 75.2 | 70.7 | 72.9 | 69.6 | 71.8 | 74.5 | 75.9 | 77.4 |
| 全国性股份制银行 | 12.7 | 10.9 | 12.9 | 13.0 | 14.2 | 15.2 | 17.8 | 20.4 | 16.9 | 17.7 | 16.3 | 17.2 | 15.9 | 13.6 | 12.7 | 11.4 |
| 城市商业银行 | 3.7 | 4.1 | 5.1 | 4.5 | 4.6 | 5.2 | 4.9 | 4.3 | 3.6 | 5.3 | 4.6 | 5.5 | 4.6 | 4.1 | 3.9 | 4.0 |
| 农商行/农信社 | 2.2 | 2.2 | 2.5 | 2.6 | 2.6 | 3.2 | 4.4 | 4.4 | 4.2 | 6.2 | 6.1 | 7.6 | 7.5 | 7.6 | 7.3 | 7.1 |
| 民营银行 | 0.1 | 0.1 | 0.0 | 0.0 | 0.1 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.1 | 0.0 | 0.1 | 0.1 | 0.1 | 0.0 |
| 村镇银行 | 0.0 | 0.0 | 0.1 | 0.1 | 0.1 | 0.1 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.1 | 0.1 | 0.1 | 0.1 | 0.1 |
| 外资银行 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |

（七）赃款善意取得无法追缴的情况凸显

被追查冻结的涉案资金，经查实符合善意取得无法追缴的情况愈加突出，尤其2020年疫情爆发以后，涉案资金以代付货款的形式流入外贸商户的现象猛增。如：G省D市王×被诈骗案中，涉案资金96万元分拆至3张三级卡后，分别流入广州市白云区某外贸服装商城7家正规商户，经查系境外“客户”购买服装“货款”，资金实际已经地下钱庄“对敲”出境，办案单位无从追查。2021年4月，一份义乌公安的内部文件在网上流传，义乌外贸商户资金账户冻结问题、第三方代付货款问题等再次摆至公众面前，进一步凸显了涉案资金追缴形势的复杂和严峻。此外，在虚假投资理财/刷单返利类案件甚至网络赌博案件中，A受害人的“返利”资金来自B受害人被骗资金的情况也比较常见。

四、当前涉案资金的转移手段与共生灰产

近年来，电信网络诈骗犯罪产业化趋势十分明显，诈骗资金转移作为下游犯罪产业，与司法部门在技术、法律等层面的对抗不断升级，电诈犯罪资金转移生态与专业“洗钱”生态已经高度融合，且与我国互联网和金融市场的灰色产业存在共生关系。主要存在几种类型：

（一）资金分拆。犯罪嫌疑人利用银行、支付机构之间的数据壁垒和公安机关查证手续的繁琐特点，通过操作多个“伪实名”账户，将涉案资金分拆成多笔转移，人为制造多笔资金流水，意图通过模糊资金去向来干扰办案侦查视线，金流可归纳为“高频率、小额度，先散后聚”特点。

此类转移方式的共生灰产主要是“两卡”非法买卖（出借、出租）产业。截至2021年底，全国“断卡”行动共查处“两卡”违法犯罪嫌疑人45万名，打掉犯罪团伙2.7万个，惩戒“两卡”失信人员10.8万余名。虽然打击惩戒力度不断加强，但仍有不少人员尤其是农民、学生等群体面对高额诱惑，出卖出租自己名下“两卡”，甚至演变成当面“供卡”“刷脸”，为涉案资金分拆转移提供便利。

（二）虚假交易。犯罪嫌疑人利用POS机、电商店铺，将涉案资金伪造成购买商品、刷卡消费等方式进行转移，通过虚构交易来干扰资金查控手段。利用POS机虚构消费：嫌疑人通过收单机构结算资金，人为制造资金隔离，继续将涉案资金转移。利用电商店铺虚假交易：嫌疑人通过在店铺中上架特殊商品，扮演买家和卖家操作“购买”，通过“寄空包”方式完成整个“网购”闭环，利用电商平台结算，实现涉案资金的隔离和转移。

此类转移方式涉及四类共生灰产：一是虚假商户。虚假商户，又称空壳公司，即不以实际贸易活动为目的登记的企业。据统计，我国自2014年开始对企业开立实行“宽准入，严监管”简化政策，截至2020年底全国在营企业数量从1200万家猛增至4000万家，疑似空壳企业超过500万家。空壳公司在洗钱、避税、骗贷、虚开发票等方面独特的隐蔽性特点，市场需求很大。这些空壳企业还可以在不同的电商平台多头开户入驻创办多个网店，因此实际流入市场的虚假商户/空壳企业数字难以估计。二是电商刷单。刷单，是指电商为吸引消费者的注意力、获取更多交易机会，以雇“刷手”刷单、虚构交易、虚构关注度、虚构好评等手段，用不正当方式提高商品销量、用户好评度和店铺信誉，从而吸引消费提高销售额的违法行为。由于“刷单”只追求客单量和成交额，极易成为违法犯罪活动资金转移的工具。三是收单业务外包市场混乱。收单业务（即POS机销售推广）是支付机构线下市场的主要业务，大多数支付机构主要采取外包模式开展业务。因为外包服务机构良莠不齐，出现“劣币驱逐良币”现象，如：对特约商户准入审核“形式化”、特约商户日常管理“空心化”、违规手段“隐蔽化”等问题。四是POS套现。POS套现是收单市场的“顽疴”，不法套现者利用信用卡56天的免息政策，通过多张信用卡、多个POS机针对性“刷卡交易”并提取结算资金，以“卡养卡”的形式可以轻松获取数百万的流动现金，融资成本远小于银行贷款。从套现者所属公司账务和银行交易记录看，均表现为正常的经营所得，但在一刷一支之间，已达到隐瞒或掩饰资金来源与去向的目的。

（三）错位匹配。主要有两种形态：1.订单劫持。犯罪嫌疑人非法获取话费、燃气、电费等充值平台的订单，通过互联网技术将赃款匹配成正常充值订单，而真实充值用户在不知情的情况下将钱“充”入嫌疑人指定账户，因此侦查员追查赃款充值记录只能追查到真实的充值客户。2.跑分平台。犯罪嫌疑人通过控制大量商户/个人收款码，搭建非法第四方支付通道，批量接收“跑分客”资金，再将赃款与“跑分客”进行匹配，完成“跑分”(即物理隔离和结算)过程。

“跑分平台”的用户端常见于PC和手机端，主要依附于大量非法出售出租的个人和商家收款码，搭建非法聚合支付通道（方便跑分客“一码通扫”提高跑分效率）完成资金转移。

（四）等价物买卖。涉诈资金转移过程中，犯罪嫌疑人往往将资金在不同类型的“等价物”之间转卖以干扰办案人员追查。主要有四种类型：1.不记名预付卡。如充值卡、超市礼品卡、游戏点卡。2.网络虚拟道具。如网游装备、Q币。3.虚拟货币。如比特币BTC、以太坊ETH、泰达币USDT。4.贵重商品。如黄金、珠宝。涉诈资金会在“伪实名”交易平台上（或“场外交易”的方式），以“高买低卖”等价物的方式进行转移。

（五）地下钱庄。地下钱庄，也被称为“地下银行”，是一种服务型犯罪，是金融监管部门和公安机关的“老对手”。地下钱庄通常为经济犯罪、电信网络诈骗、走私、贩毒、网络赌博、恐怖活动等提供资金划转和支付结算服务，严重扰乱国家正常的金融管理秩序，同时也危害国际经济安全。当前涉诈资金通过地下钱庄转移主要是非法汇兑型地下钱庄的“贸易对敲”手段。前文提到的广州、义乌等地外贸商户账户被冻结，大部分是通过地下钱庄接收了境外客户货款，而地下钱庄所接收的资金属于涉诈资金，导致账户被办案单位查控。诈骗资金通过非法汇兑型地下钱庄转移步骤一般为：①首先对诈骗资金进行一轮简单的分拆。②与非法汇兑型地下钱庄勾连，掌握外贸商户汇兑结算需求。③境外商户将外币打入水房境外账户。④诈骗团伙操作涉案资金（人民币）分拆成等价数额，通过境内水房账户打入境内商户账户。⑤境内商户确认收到“货款”后，安排发货。⑥地下钱庄在扣除洗钱费用后，将外币打入诈骗团伙安全账户。

**涉案资金（人民币）**

**诈骗资金通过地下钱庄转移示意图**

作案账户

**安全资金（外币）**

境内商户

境外商户

安全账户

受害人

境外账房

境内账房

定期对账

发货

外贸订单需求

支付货款（人民币）

支付货款（外币）

非法汇兑型地下钱庄的“对敲”模式资金未发生物理跨境转移，但实际已达到为客户跨境转移资金的目的。我国外汇管制十分严格，通过地下钱庄“对敲”结算，不仅帮助转移涉案资金，并且时常伴随骗取出口退税、非法买卖外汇、虚开增值税发票等违法犯罪活动，一直以来都是相关部门打击重点。

（六）其他转移方式。1.取现。取款“车手”通过遮挡面部等方式在ATM机取款再转存其他账户的方式对涉案资金物理隔离。2.购买基金理财产品后赎回。嫌疑人通过操作涉诈资金购买基金后立即赎回，利用基金/保险等理财产品入金账户和出金账户不一致的特点，实现对涉诈资金的“软隔离”，干扰资金追查工作。3.赌博或购买彩票。常见于稳定赔率/胜率的即开型博彩模式中。如G省F市办理的卢X被诈骗案中，涉案资金被以“网上下注”的形式，通过全国多地彩票投注站定期投注购彩，犯罪嫌疑人让彩票商户将中奖彩金转至指定账户完成转移。

五、打击治理策略

2021年4月6日，习近平总书记对打击治理电信网络诈骗犯罪工作作出重要指示，强调要坚持以人民为中心，全面落实打防管控措施，坚决遏制电信网络诈骗犯罪多发高发态势。针对电信网络诈骗资金追查追缴的现状和共生灰产问题，可从以下方面重点推进：

（一）加强法律研究。当前，电信诈骗资金转移产业已与专业洗钱产业高度融合，但限于刑法“洗钱罪”上游犯罪规定，大量为电信网络诈骗犯罪的“洗钱”行为被掩饰、隐瞒犯罪所得、犯罪所得收益罪、帮助信息网络犯罪活动罪、非法经营罪等“轻罪”所吸收。电信网络诈骗已上升为我国社会主流犯罪，诈骗资金的藏匿、转移、漂白也成为我国金融体系的主要洗钱危险之一。参与洗钱犯罪人员数量不断扩充，甚至大量的白领、学生也为他人周转洗钱资金，但受到洗钱罪上游犯罪的限制，打击上述洗钱犯罪的效能并未得到提升。因此，应加强对洗钱罪上游犯罪行为的扩容研究，考虑将电信网络诈骗等产生巨大收益的犯罪行为纳入洗钱的上游犯罪，同时可根据洗钱人员参与环节的不同、洗钱数额的不同、角色分工的不同，设置不同处罚档次。对洗钱罪进行细化和扩容，有利于打击为电信网络诈骗提供“洗钱服务”的产业链条，进一步斩断资金转移通道。

在即将颁布实施的《反电信网络诈骗法》中，也专门规定了对参与或为电信网络诈骗活动提供帮助的人员，除依法承担刑事、行政责任以外，还应按照《民法典》有关规定承担民事赔偿责任。相关部门要加快出台司法解释，迅速指导实际案例落地，进一步提高电信网络诈骗和协助资金转移行为的违法成本，有效震慑此类犯罪。

（二）坚持严打整治。公安部连续多年部署开展严厉打击电信网络诈骗犯罪专项行动，2021年共抓获各类涉诈犯罪嫌疑人69万名、破获案件44.1万起，同比分别上升90.6%、37.1%。针对电信网络诈骗犯罪突出问题，应持续严打整治、以“打”开路，尤其是对“追赃难”问题，除了关注诈骗主案，还应紧盯为诈骗资金转移、藏匿、洗白提供帮助的下游犯罪生态，加压打击。当前，大批诈骗窝点向境外转移，非法交易手机卡、信用卡愈加猖獗，跑分平台、聚合支付等新洗钱手段加速迭代，公、检、法、司各门部应主动研究诈骗资金转移、藏匿、洗白的手段特点，尤其是办案人员应加强业务技能培训，用好法律武器，不断加大资金追查和打击下游犯罪的力度，做到破案追赃“两不误”，确保尽最大力量挽回受骗群众的经济损失，切实维护人民群众合法权益。

（三）提升技术应对。一是推进数字人民币技术研发和落地。数字人民币掌握全量用户信息、交易记录和货币流通全过程，在反洗钱领域具备天然优势。随着数字人民币试点的持续推进，其支付场景深入拓展、支付方式日益健全、支付媒介不断丰富。数字人民币这场货币革新，势必对货币政策、支付生态、金融业态、普惠金融等方面产生重要影响。二是提高对潜在受骗转账操作的技术识别和阻断能力。银行和支付机构应结合自身和外部数据，不断提高对潜在受骗转账操作的技术识别和阻断能力，构筑保护群众“钱袋子”的最后一道屏障。如某第三方支付机构在高考期间，推出了“防范高考欺诈”防火墙风控业务。通过对用户年龄和交易记录等进行画像，再结合对手账户信息的智能分析，能判断该用户疑似被诈骗，进而自动阻断该笔交易，并向用户发送提醒消息。

（四）强化行业监管。一是健全完善行业实名机制。要按照“断卡”行动总体部署，加强对“两卡”开办环节“实名”核验，加强企业注册源头管理和尽职调查，对可疑“两卡”采取“二次实名认证”等风控措施。对“洗钱”生态中的点卡交易平台、黄金市场、网络游戏、电商平台等重点行业领域，要建立健全实名认证机制，及时封堵非法交易风险漏洞。二是全面规范行业管理。有关机构对收单业务外包服务要履行审慎义务，核心业务禁止外包，对线下实体特约商户要履行现场核实和年审职责。要严控POS电销网销，严格执行线下收单业务的属地化管理规定，健全完善线上收单业务的非属地管理机制。监管部门应尽快出台符合实际的个人/企业支付账户的开立、使用、变更、撤销等全过程管理要求。要建立健全行业黑名单制度，加大违规处罚力度，在洗钱风险问题上坚持“零容忍”。要构建并完善第四方支付监管制度，加强合规建设，发挥大数据和AI技术监管优势，引导聚合支付市场的良性发展。要建立网娱行业大额交易和可疑交易报告制度，强化对第三方支付机构参与网娱行业的监管。要探索建立虚拟货币监管机制，提升金融科技的监管水平，切实解决虚拟货币“堵而不疏”的困境，将虚拟货币纳入严格有序、规范合理的监管视野。三是加强交易监测和日常巡检。要加强账户交易活动监测，对多头开户、异常休眠账户纳入关注，对试探性交易、快进快出、夜间集中转账、ATM遮脸取款等异常情况实时预警。要在日常巡检中全面落实“了解你的客户”原则规定，提高电话、视频回访质量，有条件的要上门见面回访。

（五）密切部门联动。一是健全完善涉案资金“查、止、冻、返”联动机制。要打通公安与银行、支付机构特别是对一些村镇银行和小型支付机构的资金查控数据链路，实现系统对接，提高响应时效，避免出现资金查控盲区，延误追赃挽损战机。要完善侦查阶段资金返还操作程序，规范手续文书，统一公安机关、银行、支付机构资金返还程序和业务标准，提高返还效率。二是探索建立跨行业部门数据交叉核验的账户风控机制。要发挥打击治理电信网络诈骗犯罪工作联席制度优势，打破数据壁垒，探索建立基于市场监管、税务、文旅、公安等政府部门和金融、通信、互联网行业的大数据账户风险管控机制，利用区块链、人工智能等技术，强化数据联合建模，全方位多维度分析涉案账户行为特征，对潜在作案账户提前发现、精准风控、及时挽损。三是建立健全误封账户快速核验解封救济机制。针对账户错封误停情况，公安机关与银行要建立误封账户快速核验解封机制，对群众的解封申诉要及时核对反馈；确属误封的，要出具解封意见快速解封并做好解释工作，争取群众理解，避免产生负面舆情；对恶意投诉、滋事闹事的，公安机关要依法迅速处置，维护银行网点治安秩序。

（六）依法惩戒曝光。实施惩戒、公开惩戒曝光是破解“两卡”难题的有效途径，是从源头上管控电信网络诈骗资金转移、藏匿、洗白活动的有力抓手。要按照银发[2019]85号文件有关规定，对出租、出售、出借、购买银行账户或支付账户的单位和个人及相关组织者实施5年内暂停银行账户非柜面业务和支付账户所有业务的惩戒措施。通信管理部门要按照《关于依法清理整治涉诈电话卡、物联网卡以及关联互联网账号的通告》要求，尽快出台对非法办理、出租、出售、购买和囤积电话卡、物联网卡以及关联互联网账号等行为的惩戒措施。对行业“内鬼”、主体责任履行不到位的代理商、合作商等要深入公开曝光，强化舆论监督，形成强力震慑。

（七）强化宣传教育。一是普及全民反诈防骗意识。通过电视、广播、网络和自媒体等多渠道宣传普及反诈防骗意识，及时揭露新手段新骗术，筑牢群众心理防线，特别是要提高群众对买卖“两卡”行为的危害性认识，远离“租号”“刷单”“跑分”等违法行为。二是做好行业内部宣传。针对教育、金融、通信、医疗等行业系统，开展个性化的反诈宣传，加强从业人员法制教育和管理培训工作。三是强化教育挽救。对正在从事电信网络诈骗和提供洗钱服务的犯罪人员，可发布《敦促自首公告》等，落实认罪认罚政策。同时应准确把握宽严相济政策，对未成年人、在校学生、老年人等敏感群体帮助、参与涉诈洗钱活动的，要甄别涉案程度，强化教育挽救力度，慎拘慎捕，防止打击扩大化。

（八）加强国际合作。一是加强国际执法合作。应充分利用、完善既有条约，不断扩展《打击跨国犯罪公约》、《刑事司法协助条约》、《执法备忘录》等条约签订主体，以合作文件为基础，开展联合侦查、追赃、引渡等执法合作。要密切追踪电信网络诈骗犯罪人员的跨境犯罪轨迹，并增强适度预见性，与没有和我国建立刑事司法合作关系的相关国家签署多种形式的刑事司法合作文件，为开展包括电信网络诈骗犯罪在内的跨境追赃刑事司法合作奠定法律基础。二是加强国际反洗钱监管合作。应根据我国电信网络诈骗犯罪规律特点，与部分重点国家反洗钱机构建立合作机制，利用国际金融情报交流平台，与国外反洗钱机构无缝对接，不断拓展反洗钱情报来源渠道。要探索区块链技术等前沿科学技术在跨国反洗钱领域的普遍应用，实现跨境资金流动境内外追查的顺畅、迅速衔接，让赃款洗白、资金藏匿无处遁形。

参考文献

1. 苏芳.浅析电商企业账户监管难点及对策[J].审计与理财. 2021,(04):51-52.
2. 马剑.诈骗分子的“锅”不能让守法商户背[N].新华每日电讯,2021,4月16日第七版.
3. 陈一良.义乌外贸“冻卡”冲击波 被冻卡的义乌商户或达80%[J]，部分商户陷入经营困境.中国经济周刊. 2021,(08):34-35.
4. 田野,陈宏微.中国空壳公司问题研究报告——空壳公司的成因、来源和目的探究[J].山西农经,2020,(09):3-8.
5. 万静.“刷单炒信”形成黑灰产业链诱骗消费者[N].法制日报,2021,8月4日第六版.
6. 任丽丽.支付机构收单业务风险与监管研究[J].金融会计, 2020,(03):69-75.
7. 秦晓霞.网络“跑分”行为暗藏的洗钱风险及监管对策[J].北方金融. 2019,(04):57-59.
8. 孙天宏.义乌外贸商户信用卡被冻结说明什么[N].第一财经日报,2021年4月27日A11版.
9. 孙洋洋.自洗钱独立入罪的意义[J].法制博览,2021,(19):68-69.
10. 蔡宁伟,李姣.洗钱罪认定与上游犯罪领域拓展研究[J].金融监管研究, 2021,(02):103-114.
11. 武颖,刘振.数字人民币与反洗钱：机遇、挑战和应对[J].海南金融,2021,(06):77-82.
12. 郑楠.金融科技发展背景下强化支付账户监管的路径研究[J].北方金融, 2021,(02):82-84.
13. 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,(02):89-94.
14. 冯静生,刘春华.网络游戏行业洗钱风险及监管对策[J].当代金融家,2021,(01):130-132.
15. 李兰英.虚拟货币洗钱犯罪的风险剖析及治理策略[J].贵州省党校学报, 2021,(02):78-91.
16. 郝家英.电信网络诈骗犯罪跨境追赃与国际刑事司法合作[J].北京警察学院学报, 2021,(02):1-9.
1. 韦 玮：广西壮族自治区公安厅刑事侦查总队二级警长。 [↑](#footnote-ref-1)