阻断涉诈“资金链” 金融机构反诈攻防战再升级

随着监管对诈骗资金链治理持续走向常态化，金融机构面临的主体责任也在升级。

近期，中共中央办公厅、国务院办公厅印发《关于加强打击治理电信网络诈骗违法犯罪工作的意见》，特别提出：坚持全链条纵深打击，依法打击电信网络诈骗以及上下游关联违法犯罪，加强金融行业监管，及时发现、管控新型洗钱通道。

“资金链”治理一直是打击电信网络诈骗犯罪的重要一环。央行支付结算司司长温信祥在近期的国新办发布会上指出，当前我国电信网络诈骗的“资金链”治理已步入“深水区”。同时其也再次重申了进一步压实主体责任的态度——商业银行、支付机构按照“谁的账户谁负责”“谁的商户谁负责”“谁的钱包谁负责”，持续落实风险防控责任，断开涉诈资金链条。

监管力度持续升级，犯罪分子资金转移的手法、工具不断翻新，新型洗钱通道不断冒头，金融机构反诈反洗钱的压力激增，新的攻防战也分外焦灼。

资金通道压力激增

“我们的反诈客服团队已经从2020年的14人扩充到目前的30人，还是感觉压力比较大。除了AI客服的拦截，真人客服每人每天平均拨打约100通电话，拦截诈骗电话的比例差不多是十分之一。”一位互联网平台反欺诈中心人士向《中国经营报》记者透露。

机构反诈部门扩容的背后，是诈骗从购物平台、社交网络，再到短视频平台的渠道迁移和手段翻新的复杂现状：裸聊威胁、商品退款、兼职刷单、注销账号、冒充公检法、投资理财、充值返现、杀猪盘等骗术屡见不鲜。

公安部刑事侦查局局长刘忠义在前述国新办发布会上披露：目前公安机关发现的诈骗类型已经超过50种，其中网络刷单返利、虚假投资理财、虚假网络贷款、冒充客服、冒充公检法是最主要的诈骗类型。诈骗集团利用区块链、虚拟货币、AI智能、GOIP、远程操控、共享屏幕等新技术新业态，不断更新升级犯罪工具。

诈骗的最终目的是获取资金。随着近年来反诈资金链治理不断加压，金融系统在拦截涉诈资金上取得了较明显效果。根据温信祥披露：2021年商业银

行、支付机构根据公安部门指令，查询、止付、冻结涉诈资金 1.5 亿笔，紧急拦截涉诈资金 3291 亿元。月均涉诈单位银行账户数量降幅 92%，个人银行账户户均涉诈金额下降了 21.7%。

与此同时，机构也付出了真金白银的成本。由于电信网络诈骗的最后一步就是资金的转移，因此对于金融机构，反诈和反洗钱往往结合在一起。根据《中国金融机构反洗钱合规实践白皮书 2021》统计，在过去三年里，银行、支付机构反洗钱相关的行政处罚记录超过 2600 条，近千家责任单位及 1600 多名相关责任人遭到处罚。

一家收单机构内部人士向记者透露：监管近年来的现场检查很多，因为涉及反洗钱通常都是“双罚”（罚机构+罚责任人），机构高管对此异常重视。“针对诈骗赌博和洗钱，不仅要配合监管加强宣讲教育，人力投入和技术投入都在加码。我们去年外部采购了相应反洗钱的监测系统。除了合规部门设立专门的反洗钱岗位之外，每个业务线也会配备反洗钱兼职人员负责配合落实。”该人士表示。

不过，面对新型通道和模式的激增，金融机构的应对仍然存在较大挑战。

电信网络诈骗犯罪从涉案资金转移手法看，主要分为三个环节——收款、转移和变现。根据央行披露的模式，在收款环节，犯罪分子常常通过买卖、租借银行卡收取诈骗资金；转移环节，当前则存在由“传统洗钱团伙通过洗钱产业链洗白”向“跑分平台拆分交易”以及“虚拟货币转移赃款”扩展变化的趋势。而在变现环节，包括出境刷卡取现、构造虚假交易、以及地下钱庄的跨境“对敲”等最终实现账款在境外转移。

仅仅从第一个环节看，账户买卖这个老问题被打击多年却仍未得到完全解决。2021 年 11 月，人民银行曾公布一组数据，在断卡行动中，已对 130 余家商业银行和支付机构开展专项检查，暂停了 620 家银行网点 1 至 6 个月开户业务。而根据前述发布会公安部披露的数据：2021 年因反诈惩处的营业网点、机构达到 4.1 万个。

某国内顶级律师事务所的反洗钱业务合伙人向记者表示：银行在打击可疑交易方面目前承担着比较大压力，从源头看，电信诈骗主要难点是实名制，当前黑电话卡问题还比较突出。此外一个突出难点可疑交易的判定目前还缺乏统一标准。在识别“可疑”并进一步判断是否与诈骗相关时，不同银行之间不仅

技术能力不一致，标准也并不统一，银行比较难从同业处罚中得到有针对性的借鉴。

记者注意到，央行曾于2020年向机构下发《涉赌涉诈可疑资金特征及账户线索核查要点》（以下简称《核查要点》）。上述未公开发布的《核查要点》从账户端与商户端两个维度提出四大类共32条核查要点，列出了如大额现金异常存取、单笔贴近整额交易、交易时间集中等异常特征。一定程度上给予了机构一些参照标准。

“但相关标准的描述到转化成技术参数，还有比较大的距离。”前述反洗钱业务合伙人认为。

通过海外卡等方式“死灰复燃”

面对不断加压的反诈反洗钱压力，机构与黑灰产的攻防战也持续焦灼，可谓道高一尺、魔高一丈。

刘忠义在前述发布会上就指出：从通讯网络通道看，利用虚假APP实施诈骗已占全部发案的60%，并开始大量利用秒拨、VPN、云语音呼叫以及国外运营商的电话卡、短信平台、通讯线路实施诈骗。

黑灰产情报和反诈技术服务商永安在线的最新报告显示，2021年“断卡行动”虽然对网络诈骗等问题造成了有效的打击，但黑灰产正在通过海外卡/拦截卡/私接等方式“死灰复燃”；此外IP伪装——使用秒拨和代理平台“灵活”绕过各平台的风险检测。

支付宝相关人士向记者坦言：应对目前反诈业务攻防对抗的难度在于诈骗团伙也在不断“进化”，单个平台难以获取完整的风险情报。必须协同司法、政务、甚至其他市场化机构的多元数据，此外，需要把风险防控前置到更细微的场景，比如更多深入“事前”的投教环节，而不是仅仅只着眼资金链一环。

而在“事中”，更多是机构与诈骗分子技术实力上的角力。事实上，在前述发布会上，温信祥也提出：商业银行、支付机构要充分发挥大数据、人工智能等技术手段，提升风险识别、拦截精准性。加强对虚拟货币等新型领域风险防范，全方位堵截犯罪资金。

据前述支付宝人士透露：2021年，支付宝平台内AI系统已能自动识别50余种诈骗手法，逐步形成信息泄露防治、异常操作捕捉、风险预警、交易阻

拦、线下打击的全链路风控体系。比如，当识别到青少年被诱导用长辈手机给骗子转账时，平台会第一时间进行人脸等身份核验中断交易。

这种与诈骗分子的赛跑，必须依靠技术攻关。比如在去年以来非常突出的“注销校园贷骗局”中，支付宝方面透露：平台就需要对 5.9 万个网站及 APP 不间断巡检，在风险发生前先行锁定高度可疑的欺诈账户；一旦发现用户被骗子诱导转账，AI 机器人能以 0.1 秒的速度，通过弹窗、问答、延时到账、电话劝阻、交易拦截等方式主动发出预警。目前此类骗局的资损已下降 85%。

面对复杂紧急的诈骗，很多时候也不能完全依靠 AI 完全阻断。美团反欺诈中心人士透露：在风控模型判断某用户存在潜在被骗可能时，系统会从 600 多种维度综合评估，给用户打出“电诈模型分”，分数越高，则被骗概率越大。“目前，由于平台 AI 客服还在起步阶段，更多承担电诈模型分较低的部分用户提示工作；分数较高的，需要全部使用人工客服进行劝阻以增加成功率。”

甚至话术也需要不断调整。“比如以前我们会询问用户是否遇到‘刷单返现骗局’。现在我们会更多地使用骗子曾对用户说过的话，如‘是否有人让你在某平台点赞，之后给你返钱’，会更多增加用户认同。”该反期诈中心人士表示。

而在事后环节，支付机构则面临着如何协助诈骗赃款如何返还的一些问题。值得注意的是，近年来，通过第三方支付渠道进行诈骗的犯罪活动屡见不鲜，但现行法律尚未对诈骗赃款返还受害者做出明确规定。

“《关于印发电信网络新型违法犯罪案件冻结资金返还若干规定的通知》主要面向银行业金融机构拟定，鉴于支付机构和银行业金融机构在实际业务上存在差异，建议后续进一步出台针对支付机构的相关指引标准。”前述收单机构内部人士表示。

（来源：中国经营网。转引自：复旦大学中国反洗钱研究中心。网址：http://www.ccamls.org/newsdetail.php?did=42021。时间：2022 年 5 月 1 日。访问时间：2022 年 5 月 10 日 15:43。）