责编:杨 乐
制版:高如哈
内蒙古法制报

虚拟化、智能化、集团化、国际化特点凸显

落实源头防范责任 联动打击电信网络诈骗

一通电话、一条短信，一不小心，钱可能就没了；欠费了、中奖了、退税了……骗术五花八门，你是否分得清、躲得过？

2019年，全国公安机关共立电信网络诈骗案件78.2万起，日均发案2100多起；共破获电信网络诈骗案件20万起，抓获犯罪嫌疑人16.3万。2014年至2019年，全国各地电信网络诈骗受害者年均被骗额达上百亿元，不少地区人均损失呈现逐年上升态势。

电信网络诈骗是一种远程非接触性犯罪，其作案手段频繁更新、新技术加速迭代、诈骗剧本花样百出，如同“九头蛇”，“砍掉一个头”后，又不断冒出新“头”，屡打不绝。近年更是呈现虚拟化、智能化、集团化、国际化特点，上下游形成分工明确、组织严密的黑灰产业链和犯罪利益链。

今年以来，传统刑事犯罪大幅下降，电信网络诈骗犯罪仍持续高发，发案数、被骗金额呈现较快增长态势，单笔被骗百万元以上案件多发。这对全方位提升打击治理能力，破解影响群众安全感的突出问题提出了更高要求。

“资金流”三次升级

诈骗分子通过各种理由诱骗、威胁受害者向指定账户转账，并千方百计将赃款转移取现，这一所谓“资金流”是电信网络诈骗的关键。多年来，诈骗资金流经历了ATM取款、银行卡转移，到现在的对公账户转移三次升级。

多名在一线战斗了十余年的民警表示，打击整治电信网络诈骗犯罪，很大程度是和诈骗资金流赛跑：赶在诈骗分子转移赃款之前查明资金流向，冻结涉案账户，才能挽回受害者损失。

诈骗资金流几经“进化”。

最早是ATM。闽南安溪是中国大陆最早出现电信网络诈骗犯罪的地区之一。初期，一些重点乡镇出现诈骗分子排队在ATM取钱的景象。为切断诈骗资金流，该县一度关闭了全县ATM。

随着电信网络诈骗犯罪蔓延，出现专门为诈骗团伙取款的“车手”群体，他们在ATM上将赃款取现后交给诈骗团伙，并获得抽成。直到2017年，公安部、中国人民银行等6部门出台规定，个人通过ATM向非同名账户转账，资金24小时后到账，诈骗团伙通过ATM转移资金的渠道才基本被切断。

随后，更艰巨的“战场”出现在对银行卡的管控。

福建多地公安民警介绍，网上银行、手机银行业务普及后，诈骗分子转移赃款更多挪到“线上”。他们诱骗受害者转账后，只要敲击电脑键盘或手机输入数据，就能快速实现转账。

“一旦诈骗得手，就迅速将赃款拆分到数个乃至数十上百个二级、三级账户，层层转账，逃避打击。”漳州市反诈骗中心主任陈捷忠说。

这么多账户从哪里来？记者采访了解到，有专门的开卡、收卡、售卡犯罪团伙，“初期是用收购的他人身份证去批量办理银行卡。随着银行卡实名制审核日渐严格，且个人在一个银行开卡数量有限制，又出现雇用无业人员、学生等群体持自己身份证到银行开设账户，开通网上银行后，将这些账户资料整套出售给犯罪团伙牟利现象。”多地公安民警告诉记者。

近年来，公安、银行等部门加强协作，公安部设立“电信诈骗案件侦办平台”，对全国电信诈骗涉案账户实行快速接警止付；在公安部指导下，全国建立省、市、县区三级反诈骗中心数百个，公安、银行、通信部门进驻反诈骗中心，初步形成上下联动、区域配合、内外互补的立体化打击防范新模式。

“不少诈骗资金还没来得及转走就被公安机关冻结。”福州市反诈骗中心民警饶露明说。

据公安部发布的消息，仅2019年，公安、银行就通过涉案资金紧急止付和快速冻结机制，7×24小时不间断运行，止付冻结涉案银行账户55.5万个，拦截涉案资金373.8亿元。

然而，“九头蛇”长出新“头”的实力不容小觑。去年以来，又出现通过对公账户转移赃款新动向。

今年4月，福建泉州公安机关破获一起特大跨国买卖对公账户和个人银行卡案件，抓获17名犯罪嫌疑人，查获涉案对公和个人银行账户2000多个。

在这些贩卖的账户中，“含金量”最高的是对公账户。办案民警介绍，包括营业执照、对公账户、开户手机卡、法定代表人身份证、企业公章、法定代表人私章、银行账户U盾等一整套资料，售价在1万元左右。

这并非个案。去年以来，电信网络诈骗犯罪团伙开始大量使用对公账户转移赃款，逃避打击。“几乎每一起案件都涉及对公账户。”多地办案民警告诉记者，在诈骗、网络赌博等犯罪团伙间，有一个形象的说法：谁掌握的对公账户最多，谁的资金就最安全。

电信网络诈骗犯罪团伙为何“青睐”对公账户？记者采访多地公安民警了解到，电信诈骗涉案对公账户往往分散在全国各地，查询周期长，经常是查清资金流向后，资金已被转走取现。

对此，去年以来，公安部组织部署各地公安机关，依法严厉打击买卖银行卡和企业对公账户违法犯罪活动。

“通信流”无孔不入

5月7日，在公安部统一指挥下，北京、上海等15个省市公安机关同步集中收网，捣毁为贷款类电信网络诈骗犯罪团伙提供服务的违法1069短信平台57个，抓获犯罪嫌疑人798名，扣押手机、银行卡、电脑等一大批涉案工具。

诈骗分子通过发送短信、拨打电话或网络聊天等通信手段和受害者沟通，实施诈骗，这是电信网络诈骗最鲜明的特点。记者调查发现，多年来，诈骗“通信流”花样翻新，屡禁不绝。

最初，诈骗团伙躲在闽南深山用短信群发器发送诈骗信息，用收购的手机卡拨打电话，安溪部分偏远乡镇一度成为“亚洲最繁忙的基站”。在公安机关持续严打之下，诈骗分子将窝点转移到全国各地乃至境外，利用可模拟任意号码的网络电话实施诈骗。近年来，170等虚拟运营商号段、物联卡、95号段号码等通信手段被诈骗分子广泛运用。

“这些通信手段背后的共性问题是层层转卖，实名制形同虚设，或是没有登记购买者，更多是登记的购买者和实际使用者不一致，实名不实人。”多地公安民警告诉记者。

有关部门监管缺位，为“九头蛇”长出新“头”提供了可乘之机。

以近年被诈骗分子广泛使用的95号段号码为例，该号段号码原本规划用于跨省/全国范围内统一使用的客户服务短号码、电信业务接入号码等，由工业和信息化部负责规划、分配和管理，企业实名申领后，与通信运营商签订合同，由运营商管理号段使用。

但记者调查发现，通信运营商的监管存在较大漏洞。实践中出现大量代办公司专门从事95号段申领业务，申领一个5位或6位95号段号码后，可申请拓展到8位数。这样申请一个号码后，实际可以用的号码成百上千地拓展，这些号码被层层转卖，甚至在网上公开售卖，其中一些就流入诈骗团伙。

层出不穷的通信“黑科技”为“九头蛇”不断“续命”。

例如，可以模拟任意号码的网络改号电话；将传统电话信号转化为网络信号、同时支持128个手机通话，具备远程控制、机卡分离等特点的“多卡宝”、GOIP(无线语音网关)等设备。

“诈骗分子用改号软件，模拟公检法机关办公电话，冒充办案人员，以受害者‘涉嫌洗钱’等为由，要求将存款账户资金转入办案单位‘安全账户’；有的利用‘多卡宝’设备，在境外远程遥控设立在境内窝点的通信设施进行诈骗，增加了诈骗的迷惑性，给公安机关打击带来困难。”多地公安民警说。

源头防范 联动打击

受利益驱动，围绕电信网络诈骗犯罪，一条分工明确、组织严密的黑灰产业链条已经形成。

上游，有成熟的个人信息售卖产业链。

“专门团队收集公民个人信息并提供给诈骗团伙，诈骗分子针对不同群体，精准设计骗局，迷惑性更强。”多地公安民警告诉记者。

记者调查发现，个人信息在网上公开售卖。在百度搜索“出售一手实时数据”之后，弹出近300万条结果，随机联系一卖家后，对方告知，贷款网站注册信息售价5元一条，含身份证、手机、银行等信息，其手上有上万条信息。

在QQ群中，大量工商企业数据、高校在校生数据、淘宝订单数据被明码标价。一卖家称，其手上有母婴、童鞋、服装、汽车等一系列电商客户数据，一条母婴用品客户数据包含姓名、地址、电话、下单时间等信息，售价仅为1.4元。

下游，围绕诈骗“资金流”“通信流”，也存在大量黑灰产业链。

以近年来高发的“杀猪盘”(网络交友诈骗)为例，诈骗团伙通过在“珍爱网”“世纪佳缘”等婚恋交友网站注册会员，以交友为名，诱骗受害者参加网络赌博或投资推荐的股票、基金等。

而这些博彩、投资网站，均是诈骗分子找专业团伙建立的，伪装成境外知名博彩、投资网站页面，受害者能在网上搜索到这些知名网站信息，很容易被迷惑。诈骗分子在后台操控，受害者一旦投入资金，其账户本金及“收益”就只是显示在平台上的一个数字，资金早已被诈骗分子通过银行账户、第三方支付平台转走。

近年来，针对电信网络诈骗及上下游黑灰产业链，公安、银行、工信、网信等部门联手多次开展专项打击行动，查处一大批违法违规行为，起到有效震慑作用。

制度的笼子也越扎越紧。手机卡、银行卡实名开卡得到落实，此前长期存在的持他人丢失身份证也能办理等乱象得到遏制。出租、出借、出售个人银行账户或企业对公账户纳入金融信用基础数据库管理。

有关部门“见招拆招”，持续加大联动打击力度，但记者采访发现，这些措施存在一定的滞后性。不少基层办案民警坦言，在管控诈骗“资金流”“通信流”及黑灰产业链源头上存在漏洞。

以对公账户为例，出现同一人以同一个虚构的经营地址、注册数十家乃至上百家经营主体，再申领上百个对公账户出售牟利现象；有的地方出现不法分子组织大量人员到银行柜台办理对公账户，申请资料存在明显疑点，银行也一路绿灯。

又如，95号段号码、170等虚拟运营商号码、物联卡等通信手段，原本是通信部门开发、拓展的便民新业务，但因为配套安全监管没有跟上，被犯罪团伙利用用于实施犯罪、逃避打击。

因此，多地公安、通信、银行等部门工作人员提出，捏住电信网络诈骗“九头蛇”的“七寸”，除持续严打犯罪链条外，还须加强源头防范、推进联动打击、完善工作机制，实现标本兼治。

例如针对长期存在的电话卡“实名不实人”和虚拟运营商治理难题，一些地方通信运营商采取的治理措施，具有一定借鉴意义。中国联通泉州分公司信息安全部负责人艾圣宪说，“凡是营业员违规开卡涉嫌被电信网络诈骗犯罪利用的，每张罚款2000元；出现两张就扣罚全部绩效，同时追究相关人员责任，以重拳整治个别营业员与不法分子勾结售卡乱象。”

同时，中国联通泉州分公司今年4月成立专项工作组，运用大数据手段，研判涉电信诈骗犯罪电话卡特点，对诈骗号卡进行精准画像，建立反诈模型。“被系统研判为潜在诈骗号卡的，只要进入泉州就会变成废卡，将诈骗行为终止在事前。”艾圣宪表示。

“打击电信网络诈骗犯罪，关键在于各有关部门切实履行安全监管主体责任，堵住漏洞，不给诈骗分子可乘之机。”受访人员建议，完善法治手段，强化责任追究机制，落实源头防范责任。对个别部门和人员因放任、失职，履行部门责任不到位甚至内外勾结，导致所开展业务被犯罪团伙利用的，严肃追责。 (郑良 王成 吴剑锋)

广告发行部电话:(0471) 4687563 广告经营许可证:呼工商广字1501004000013 邮编:010010 本报激光照排印刷:呼和浩特日报社印刷厂 本报零售:每份1.6元