编者按

> 中国人民银行支付结算司对美国一起虚拟货币“杀猪盘”电信网络诈骗的典型案例进行了分析，梳理总结了当前全球电信网络诈骗案件屡禁不止的底层逻辑，并在此基础上提出持续研究关注国际电信网络诈骗犯罪形势及特征，不断升级我国综合治理体系，防范虚拟货币成为涉诈资金转移新通道，加大涉诈人员打击惩处和管控力度，加大关联犯罪打击力度，精准开展反诈防诈宣教等建议，为全方位筑牢技术反诈防护网，全领域铲除电信网络诈骗犯罪滋生土壤，全维度强力挤压涉诈犯罪生存空间，坚决打赢反诈人民战争提供了有益的参考。

随着现代网络科技的发展进步，电信网络诈骗犯罪也呈现多发高发态势，除在我国已成为发案最多、上升最快、涉及面最广、人民群众反映最强烈的犯罪类型外，国外的电信网络诈骗犯罪也在不断增加，社会危害巨大，但国外对此类犯罪的打击治理力度与我国相比仍有很大差距。以习近平同志为核心的党中央对打击治理电信网络诈骗违法犯罪工作高度重视，近期中办、国办印发了《关于加强打击治理电信网络诈骗违法犯罪工作的意见》，对加强打击治理电信网络诈骗违法犯罪工作作出安排部署，为进一步提升打击电信网络诈骗犯罪的力度与效能提供了重要依据。在党中央的正确领导下，我国打击治理电信网络诈骗犯罪工作已取得显著成效，充分体现了以人民为中心、为群众办实事的人民立场和为民情怀，充分彰显了中国共产党领导和我国社会主义制度的显著优势。电信网络诈骗犯罪具有虚拟性、跨国性、非接触等特点，打击治理客观上存在相当的难度。 面对当前这一世界性犯罪难题，为把握国内外电信网络诈骗犯罪趋势、进一步提升打击治理效能，本文从一起美国虚拟货币 “杀猪盘”的典型电信网络诈骗案例入手进行分析，并在此基础上探讨相关启示建议。

美国虚拟货币“杀猪盘”电信网络诈骗案例

2022年4月4日，《华盛顿邮报》报道了一起虚拟货币“杀猪盘”电信网络诈骗案例。该案例受害人“詹金斯”是一名57岁的美国退休警察，曾在纽约皇后区赌场担任安保主管，擅长发现藏匿在赌场中的各种骗局，然而这样一位经验丰富的警察，也被诈骗团伙利用虚拟货币骗取资金1.5万美元。犯罪分子诱导受害人在虚拟货币交易所Coinbase购买虚拟货币“泰达币”，在虚假“流动性挖矿”网站CB-ETH上投资，并利用木马程序洗劫受害人虚拟货币账户。受害人经与执法部门、虚拟货币公司及虚拟货币交易所等多方沟通协商，仍无法就此案立案并追踪被骗资金。

通过对本案例的梳理分析，可以发现
“杀猪盘”式的电信网络诈骗犯罪的基本“剧本情节”及危害。

初期建立情感连接

获取受害人信任

为寻找诈骗目标，诈骗分子初期利用“爱丽丝”这一虚构身份在约会软件结交好友并发现潜在受害人“詹金斯”，而后便使用通讯软件与受害人取得联系，采用各种手段施展魅力吸引受害人，并通过每天交流关于生活、家庭等方面话题，甚至视频聊天获取“詹金斯”信任，受害人按照诈骗团伙的计划一步步走入其事先准备的“恋爱”陷阱。

抛出虚拟货币“诱饵”

诱导受害人入坑

在熟识一个多月后，“爱丽丝”向“詹金斯”推荐了虚拟货币和“流动性挖矿”投资，称只需花费26美元在专门处理“流动性挖矿”的网站CB-ETH购买一张“采矿证书”，便可开始投资虚拟货币并赚取回报。“詹金斯”被高额收益吸引，便在“爱丽丝”引导下在虚拟货币交易所Coinbase购入4000美元的泰达币，并全部投资到CB-ETH网站。为确认钱包内的泰达币由自己控制，“詹金斯”将存入的资金从钱包提取，并再次存入。“爱丽丝”而后抛出投资达1.5万美元可享每月15%回报的诱饵，“詹金斯”笃定钱包内的资金安全，便逐渐将投资增加到1.5万美元。随着持有时间增长，网站显示收益在稳步上升。为此，“詹金斯”甚至鼓励亲戚朋友共同参与投资。

植入木马程序

悄然转移受害人资金

“詹金斯”在投入1.5万美元后不久，发现其钱包内的资金不翼而飞，亲戚朋友钱包内的资金也同样消失。事实证明，CB-ETH网站上显示的收益并不存在，只是向受害人制造不断获得收益的假象，以此诱骗受害人持续加大投资，且受害人在网站购买的“采矿证书”并非“证书”，而是一段区块链语言编写的木马程序，授权犯罪分子远程操纵被害人虚拟货币账户洗劫资金。

大量受害人遭遇虚拟货币“陷阱”

追赃挽损难

实际上，遭遇相同虚拟货币诈骗的受害人不在少数，《华盛顿邮报》相关人员通过寻找“詹金斯”被骗资金转入的账户，共定位到其他5046个账户具有与“詹金斯”账户相似的交易特征，这些账户平均损失超过1.3万美元。由于区块链的匿名性，被盗的虚拟货币被转移的账户地址只是字母和数字的组合，无法找到持有人真实姓名、联系信息甚至是所在的国家或地区，导致追回资金的难度较大。相关虚拟货币公司“Tether公司”、虚拟货币钱包的运营公司“Coinbase”均对“詹金斯”追回损失的请求表示无能为力。且由于美国现有监管框架尚未明确虚拟货币诈骗相关监管职责，当“詹金斯”向警察局报案或联系联邦调查局和证券交易委员会时，未收到执法部门的任何回应。这也充分证明，美国对电信网络诈骗犯罪仍未足够重视，更未完善反电信网络诈骗治理体系。

当前电信网络诈骗案件

高发的底层逻辑

通过分析上述美国诈骗案例不难发现，任何形式、国家的电信网络诈骗案件普遍存在相似的犯罪逻辑。为取得受害人信任，犯罪分子会想方设法抓住受害人贪财、恐惧、规避风险等心理，利用获取的受害人信息及完善的诈骗链条量身制定诈骗“剧本”，使受害人深信不疑后骗取钱财。目前国内电信网络诈骗案例大致具有以下几种特征。

利用受害人心理弱点

进行“剧本”设计

为引诱更多受害人上钩，诈骗团伙会对受害人的心理进行较深入的研究，利用高超的话术技巧，编造针对不同心理特点的虚假信息，以实现犯罪目的。

1.利用贪财心理的利诱型诈骗。
诈骗团伙以丰厚的奖金、投资回报等利益为诱饵，并以需要交纳保证金、邮费、投入初始投资成本等理由让受害人先行支付一笔费用。利用受害人贪图钱财，试图付出小额成本获取高额收益的心理弱点，使其“自愿”交纳财物。常见诈骗方式包括虚假中奖信息、高收益投资理财、无息或低息贷款等。

典型案例：
国内某高校学生张某某日收到一条中奖短信，称其在某平台购买了商品，平台为回馈用户举办了抽奖活动，其购物单号被抽中，奖品是电脑一台，可以折现2万元。

张某便添加对方微信联系，对方称折现需要交手续费、认证费和税费，折现成功后所交费用全额退还。张某信以为真便向对方提供的账户转账1.5万元，后发现被骗，遂报警。

2.利用恐惧心理的恐吓型诈骗。
目前最常见的恐吓型诈骗主要是诈骗团伙冒充公安、法官或检察官等办案，利用受害人对公权力威严的敬畏和恐惧，并施以威胁手段使受害人不敢报警或向他人求助，进而让其转移资金到“安全账户”。

典型案例：
郑女士某日接到一自称“北京公安”的电话，对方称郑女士涉及一起“洗黑钱”案件，要求其将银行卡的钱转到“安全账户”。对方期间身着警服与郑某视频通话，表示其可向附近派出所了解详情，同时威胁若进派出所可能会被抓。郑女士十分害怕，在派出所门口左右徘徊，直到被民警发现才识破骗局。

3.利用规避风险心理的诈骗。
诈骗团伙根据掌握的受害人信息虚构情境，如受害人的网购商品出问题需退款、航班退改签、境外大额消费记录等，受害人在难以辨别真伪时，为减少损失、规避风险，点开虚假钓鱼链接被转走资金，或通过诈骗团伙提供的其他方式支付手续费。

典型案例：
杨女士在某网购平台购物之后，接到自称“官方客服”的来电，对方称其购买的商品质量有问题，可以申请退款，对方能准确报出其购物的订单号。杨女士信以为真，在引导下点击对方提供的网址链接并将银行卡号、密码以及验证码发送给“客服”，银行卡内的5万余元即刻被转走。

4.利用特殊心理需求的诈骗。
部分诈骗团伙根据单身人群情感空虚、渴望关怀等心理需求，设下“杀猪盘”逐渐取得受害人的信任，后通过向受害人借钱、引导投资、高额消费等方式骗取钱财。

典型案例：
陈女士在刷短视频时收到一名男子私信，称想和其交朋友，并以交流方便为由诱骗她下载某学习APP，两人通过APP频繁聊天后发展成为“恋人”关系。对方告诉陈女士自己在北京某证券交易所工作，并称近期购买新股即可大赚一笔，陈女士便听信建议投资2.8万元。后陈女士发现资金无法提现，联系该男子也失去音讯。

利用信息不对称

对受害人精准“攻击”

电信网络诈骗的实施需要精准掌握受害人信息，诈骗团伙通过收集、分析和传递个人信息，获得信息优势，然后利用各种手段将信息效益最大化，以达到犯罪目的。

1.利用非法获取的受害人信息实施精
准诈骗。
诈骗团伙利用从社交平台或其他非法渠道获取的公民个人信息，对诈骗对象进行“画像”，实施精准诈骗，如利用网购信息进行网购退款类诈骗、利用学校信息进行网贷注销类诈骗、利用财务人员职业信息进行冒充老板类诈骗等。由于诈骗团伙能精准描述出诈骗对象的基本情况和个人敏感信息，符合理应掌握这类信息的工作人员特征，因此容易取得受害人的信任。特别是疫情暴发以来，各类防疫信息呈爆炸式增长，犯罪分子借机大范围利用非法获取的用户行程信息、快递信息等实施精准诈骗。

典型案例：
张某在社交平台发布信息后，某诈骗团伙通过张某动态对其精准定位并发现张某附近出现疫情，遂致电告知他与一位密接有行程交叉，诱导受害人点击链接填写个人信息，随后再以近期大数据行程卡访问量过大，存在系统故障为由，索取短信验证码确认行程轨迹，最终张某被骗4.3万元。此外，王某接到声称购物平台客服的电话，称快递包裹因为核酸检测阳性无法配送，可申请退款理赔，当王某按照提示下载软件，填写银行卡、验证码等信息后，被骗4.9万元。

2.利用受害人缺乏专业领域相关知
识实施诈骗。
近几年，区块链、虚拟货币等技术概念兴起，诈骗团伙利用受害人对这些新兴、专业、热点领域的了解不足，引诱受害人进行新兴领域投资，使受害人在虚假投资网站、APP投入大量资金。其中，老年人由于教育背景较为薄弱，且获取信息渠道单一，成为利用“专业知识”诈骗的重点对象。2022年北京商报总结的老年人金融骗局中，大部分是利用老年人金融知识薄弱进行诈骗。

典型案例：
某诈骗团伙虚构“理财神器”，通过虚构国企背景、承诺保本保息获取老年人信任，再通过虚构项目、高收益诱导老年人充值投资，以复杂的“理财产品”骗取老年人信任，最后平台以各种理由表示无法提现甚至失联，最终导致受害人超百万元投资款血本无归。

通过成熟黑灰产和专业分工

提供“技术支撑”

电信网络诈骗已经发展出一条成熟的黑灰产业链，且犯罪团伙成员经过专门培训，有固定的作案流程，其中不乏精通网络技术的“黑客”和熟知被害人心理的“话务员”等。作案工具方面，常利用智能群呼网关、GOIP等设备，通过远程操控、机卡分离实现诈骗呼叫，隐藏自身网络、通话特征，规避公安机关侦查打击和通信行业技术防范。专业分工方面，犯罪产业链上下游分工明确，“菜商”负责获取、买卖公民个人信息，“话务员”负责使用电话或社交软件联系被害人，“卡农”负责批量租借购买用于转移资金的银行卡，“车手”负责取款，“水房”负责洗钱、拆分资金流等。

典型案例：
2021年，江苏扬州警方在一起电信网络诈骗案件缴获的U盘中发现各类公民个人信息两千多万条，警方认为犯罪嫌疑人屡屡得手，主要是由于其充分掌握被害人的基本情况。2021年底，湖南警方打掉一个专门从事收购贩卖银行卡、帮助实施信息网络犯罪的团伙，该团伙高价收购银行卡和配套的电话卡为诈骗犯罪提供帮助。2021年3月，福建警方捣毁一个为赌博、诈骗集团提供资金服务的跑分窝点，犯罪团伙线上搭建“跑分”平台为上游赌博、诈骗集团取款转账；线下则用金钱利诱，招募大量持卡人员用于“人肉跑分”。

全球电信网络诈骗形势严峻

我国在打击电诈方面已位于前列

当前，电信网络诈骗已成为全球性问题。数据显示，2021年以来，美国、英国电信网络诈骗犯罪高发、多发，诈骗团伙利用虚拟货币进行涉诈款项支付增长趋势明显。有英国媒体指出，政府打击和预防诈骗犯罪的力度不足，导致诈骗犯罪案件数量居高不下。与之相比，我国坚持以人民为中心，建立“打、防、管、控、宣”五位一体打击治理体系，电信网络诈骗犯罪上升态势得到有效遏制。2021年6月至今实现电信网络诈骗立案数连续9个月同比下降。

美国电信网络诈骗

高发趋势明显

1.电信网络诈骗案件数量显著增长。
根据美国联邦贸易委员会公布的数据，美国电信网络诈骗案件从2017年一季度的29.7万件上升至2021年四季度的52万件，2021年诈骗金额约为2017年的5.4倍。特别是2020年新冠肺炎疫情暴发后，诈骗案件数量增长较快，在2021年一季度达到最高值82.4万起（见图1）。

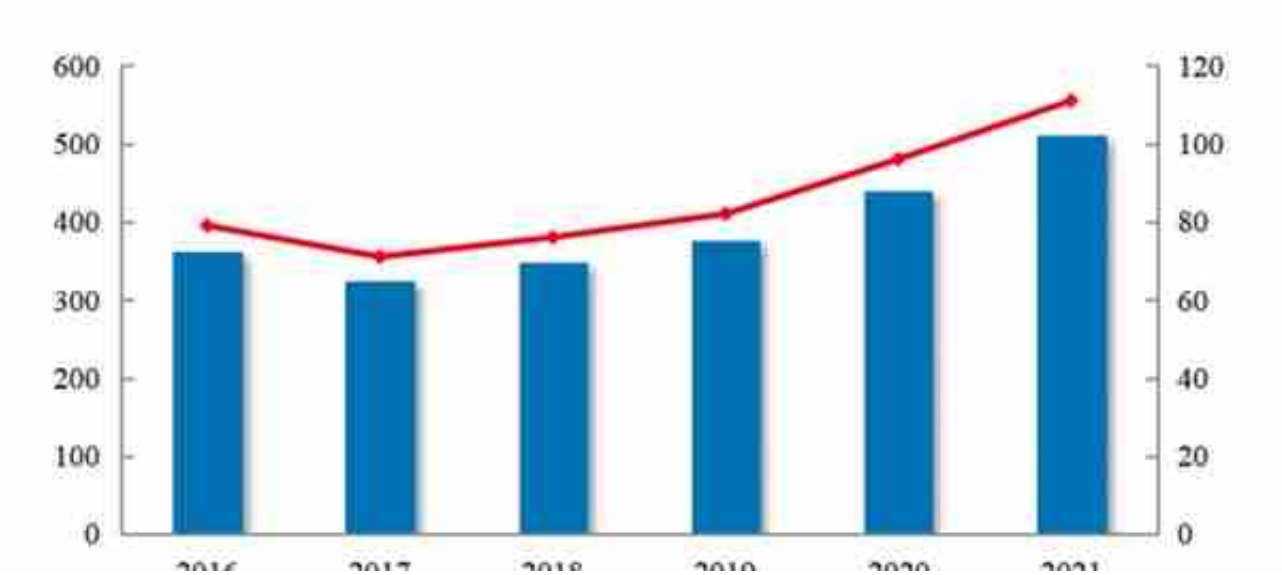

图2 2016-2021年英国电信网络诈骗犯罪趋势图

2.政府
打击和预防诈
骗犯罪的力度不足，导致诈
骗犯罪案件数量居高不下。
英国内政部数据显示，2021年英国警方结案的诈骗案件数量仅5.2万起，有2.2万起被停止侦查，只有不到5000起案件的嫌疑人被起诉。英国《泰晤士报》调查显示，因人手短缺，执法部门无力应对激增的诈骗犯罪。受害人拨打警方举报专线时，平均需要28分钟才能接通。英国智库社会市场基金会指出，英国反诈骗体系和机制一团糟，记录在案的诈骗案件，每1000起只有2.1名警员侦办。

我国电信网络诈骗犯罪上升态势

得到有效遏制

1.严打高压，打击治理工作取得突破
性进展。
2021年，全国公安机关大力开展打击治理电信网络诈骗犯罪工作，坚持源头治理，出重拳，下狠手，强预防，克服疫情带来的不利影响，破获电信网络诈骗案件44.1万余起，抓获违法犯罪嫌疑人69万余名，近三年同比显著增长（见表1）。打掉涉“两卡”违法犯罪团伙3.9万个，追缴返还人民群众被骗资金120亿元。2021年6月至今实现电信网络诈骗立案数连续9个月同比下降。相关工作推进过程中，公安部门勇于担当作为，对银行网点提供的异常开户等线索快速响应，坚决斩断买卖银行卡黑灰产业链。