

电信诈骗的“罪”与“罚”

——从识别骗局到紧急维权，这份指南带你吃透防诈攻防战

本报记者 马文青 魏鑫 高虎

电信网络诈骗犹如潜伏在数字时代的“隐形陷阱”，从冒充客服的温情骗局到虚假投资的暴富诱饵，从兼职刷单的小利诱惑到社保异常的恐慌操控，骗子的套路不断翻新，给公众财产安全带来威胁。

为揭开电信网络诈骗的真面目，帮助大家认清法律边界、掌握防范技巧，本报记者特别专访相关人士，从司法实践、法律制裁、侦查细节到维权方法，全方位拆解骗局，为公众送上一份实用的防诈“护身手册”。

法治访谈

嘉宾：

马云（陕西省高院刑事审判第二庭副庭长）

王萍（陕西省检察院第四检察部副主任）

孙静（西安市公安局莲湖分局经侦大队教导员）

电信诈骗无“小案” 3000元即达追责标准

记者：生活中，很多人觉得“小金额诈骗不算事”。从您办理的案件来看，参与几千元的电信诈骗，犯罪分子会受到怎样的法律制裁？

马云：这种“小金额诈骗不算事”的想法是完全错误的。我国法律对电信网络诈骗的打击力度是明确且严格的。根据《最高人民法院、最高人民检察院关于办理诈骗刑事案件具体应用法律若干问题的解释》第一条规定，利用电信网络技术手段实施诈骗，诈骗公私财物价值三千元以上的，就达到了刑法第二百六十六条规定的“数额较大”标准，要以诈骗罪定罪处罚，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金。

近期，我们审理了一个案件，小张是一名大学生，在网上看到兼职刷单信息，想着赚点外快。一开始，他刷了几单都收到了小额返利，便放松了警惕。后来对方说有个大额任务，完成后返利很高，小张就投了5000元，结果提现时被拉黑了。报警后，警方很快抓获了犯罪嫌疑人。最终，这名嫌疑人因诈骗金额达到“数额较大”标准，被判处有期徒刑八个月，并处罚金2000元。

除了判刑和罚金，诈骗者还要退还违法所得、退赔受害人损失，一旦有犯罪记录，还会影响信用、贷款、求职等。即便金额没达到刑事立案标准，根据《治安管理处罚法》，也会面临拘留和罚款。所以，任何诈骗行为都必然受到法律制裁，千万别抱侥幸心理。

记者：冒充客服退款、虚假购物这些行为，它们在法律上算电信网络诈骗吗？如果有人不小心帮骗子转账，会有什么法律后果？

王萍：这些行为在法律上都属于电信网络诈骗。根据“两高一部”的相关意见，电信网络诈骗是指利用电信网络技术手段，虚构事实或隐瞒真相，骗取公私财物的行为。冒充客服退款，是骗子伪装成电商客服，以“退货退款”为由诱骗转账；虚假购物则是通过虚假网站销售不存在的商品骗钱。它们都借助了手机、互联网等工具，具有隐蔽性、跨地域性特点，符合电信网络诈骗的特征。2024年公安部发布的十大高发电信诈骗类型中，这两类都在列。

如果有人不小心帮骗子转账，法律后果要根据具体情况判断，主要有三种可能：

第一种是构成诈骗罪共犯。如果和诈骗团伙共谋，或参与编写话术、搭建虚假平台等关键环节，哪怕只负责一环，也会被认定为共犯。根据刑法，诈骗数额较大的，处三年以下有期徒刑等；数额巨大的，处三年以上十年以下有期徒刑；数额特别巨大的，处十年以上有期徒刑或无期徒刑。

第二种是构成掩饰、隐瞒犯罪所得罪。如果诈骗已经完成，明知是赃款还帮忙转账、套现、转移，就可能定这个罪，核心是“事后明知”。2023年西安有个案例，无业人员杨某明知资金来路不正，还多次用银行卡刷POS机买黄金，帮骗子套现61万余元。尽管他说“不知情”，但聊天记录、转移银行卡等行为证明他主观故意，最终被判处有期徒刑二年，罚金20000元。

第三种是构成帮助信息网络犯罪活动罪，也就是“帮信罪”。如果没直接参与诈骗，但出借银行卡、支付账号，或代为转账（俗称“跑分”），且未尽合理注意义务，就可能构成此罪。法律上的“明知”包括“应当知道”，比如对方要求夜间操作、给远高于市场的佣金，频繁换账户等。根据刑法，要处三年以下有期徒刑或拘役，并处或单处罚金。

我们办案时会严格区分主观故意，对初犯或情节轻微的，优先适用认罪认罚从宽制度，督促退赃退赔；但对明知故犯、恶意参与诈骗核心环节的，会坚决严惩。

涉诈行为分情形 维权方法要牢记

记者：我们常说“陌生链接别点、陌生转账别信”，但还是有人上当。您在处理警情时，发现大家最容易在哪些生活场景陷入诈骗？骗子是怎么设套的？

孙静：确实有很多常见场景容易让人掉进陷阱。先说网购退款，骗子会先通过非法手段获取你的网购信息，然后冒充电商客服联系你，说商品有质量问题要退款。他们能准确说出你的购买信息，很多人就信了。接着发个退款链接，让你填信息，其实是钓鱼网站，你一输银行卡号、密码、验证码，钱就被转走了。

还有社保通知类诈骗，骗子自称是社保部门工作人员，说你的社保账户异常，被冻结或要补缴费用，还能说出你的姓名和身份证号，让你觉得事情严重。然后引导你点击链接、下载APP操作，其实就是套你的钱。另外，兼职刷单、虚假投资理财、冒充熟人借钱也是高发场景。比如虚假投资理财，骗子会先在你小额投入时给点返利，等你加大投入后，平台就登录不上了；冒充熟人借钱的，会先打“感情牌”，说自己遇到急事，让你赶紧转账，很多人碍于情面就没核实，结果被骗了。

记者：如果不小心被骗，我们应该怎么做才能更好维权？

马云：一旦被骗，第一时间要做这几件事：一是立刻拨打全国反诈专线96110，说清转了多少钱、对方账号、转账方式，反诈中心能迅速采取行动，阻止资金外流。二是如果错过了最佳时机，赶紧冻结自己的相关账户，银行卡打银行客服，支付宝、微信支付分别打95188、95017冻结支付功能，防止骗子进一步利用你的账户。三是拨打110报警，说清转账时间、金额、对方账户等关键信息，提供骗子的联系方式、聊天记录等证据，告诉警方你已经采取的措施，方便警方展开调查。

在收集证据方面容易犯错的情形包括：随意删除聊天记录，觉得没用或占内存，但这些记录能直观展现骗子的话术、承诺和诱导过程，是证明诈骗行为的关键证据；还有就是不注意留存转账凭证，它能明确资金流向和金额，是证明财产损失的直接证据。有些受害者觉得“银行有记录就行”，等到需要时再去银行打印，就耽



田耀辉 作

防诈需辨“不合理” 不做电诈“工具人”

记者：帮信罪的核心要素是什么？识别帮信罪可以从哪些方面入手？

王萍：帮信罪是指明知他人利用信息网络实施犯罪，而为其提供技术支持或广告推广、支付结算等帮助的行为。其核心在于“主观明知”和“客观帮助”两个要素。

识别帮信罪可从三方面入手。从行为模式看，多是“低门槛、高回报”的非法活动，像以“兼职刷单”“代转账”招募人员，要求提供银行卡、支付宝账号转移资金；帮注册空壳公司、开办对公账户帮诈骗团伙转账；出租微信、QQ等社交账号发布诈骗信息。这些行为看似简单，但若涉及不明资金，就可能涉嫌支付结算帮助，多数帮信案源于此类“灰色兼职”。

从主观认知看，“明知”包括直接知道或应当知道。若对方要求保密、用暗语，或转账涉及“赌博”“投资”等敏感词，需警惕涉罪。识别标准很简单，涉及资金操作时，问自己这笔钱来源合法吗？不确定就立即停止并报警。

在案件办理中，检察机关通过多种途径助力识别预防。一方面强化法律监督，审查案件时重点核查电子证据，建立“帮信罪风险预警模型”，识别短时间内多账户频繁交易等可疑行为；另一方面推动社会共治，联合公安、银行开展“断卡行动”，管控异常账户，通过官网等发布指南，提醒公众不轻信“轻松赚钱”广告、不出借个人证件。

总之，请大家牢记，“低门槛、高回报”兼职多有问题，涉及资金操作先确认为来源合法性。

记者：普通人该怎么分辨哪些是机会、哪些是骗局呢？

孙静：可以从三个角度判断。第一看“钱的流向”是否合理。正常兼职或投资，要么是你付出劳动后对方给你钱，要么投资项目、风险提示、资金用途都很透明。但如果对方总让你先交钱，比如“入职交押金”“投资垫资”“刷到一定金额才返现”，而且钱收了不返还，或让你继续追加才能“解锁”，就可能是骗局。

第二看“承诺的回报”是否脱离常识。如果说“兼职一天赚几百上千，不用花多少时间”“投资门槛低，稳赚不赔，收益远超银行理财”，就要警惕。天上不会掉馅饼，正常收益和付出是成正比的，把回报说得太高，大多是勾住人的贪心。

第三看“对方是否回避关键信息”。正规合作方会告诉你公司信息、项目详情、联系方式等。但骗子会回避，问公司地址，说“线上运营，没实体”；问具体项目，说“保密”；联系方式只用微信、QQ，不给固定电话或真实姓名。这种躲躲藏藏的行径，很可能是违法的。

给大家分享一个简单好记的防诈口诀：“陌生电话要警惕，可疑短信需注意；中奖退税送便宜，哄你汇钱是目的；公检法司来联系，安全账户纯瞎扯；不听不信不转账，多方核实没坏处。”牢记这个口诀，能帮大家有效防范很多诈骗。

此外，保护好个人信息是防诈的基础。不要随意透露身份证号、银行卡号、密码、验证码等重要信息，不点击来历不明的链接，不下载非官方渠道的APP。遇到可疑情况，要及时向公安机关或相关部门咨询核实，别盲目听陌生人的指令。

记者手记

合上采访本时，桌上的反诈宣传册被风掀起一角，“隐形陷阱”四个字格外刺眼。几天的采访里，法官、检察官、民警讲述的案例像拼图，一点点还原出电信网络诈骗的真实面貌——它从不是影视剧里的离奇剧情，而是藏在手机弹窗、陌生来电、兼职广告里的日常危机。

法官提及的大学生小张案让人唏嘘。5000元，对学生而言不是小数目，却成了骗子精心设计的诱饵。更值得警惕的是，庭审记录显示，诈骗者起初只骗几十元“试水”，正是“小金额诈骗不算事”的心理作祟。这让我想起法官反复强调的话：“法律的标尺从不含糊，每一份诈骗所得都要付出代价。”那些觉得“骗点小钱没事”的侥幸，最终都会撞上法律的铜墙铁壁。

检察官拆解的帮信罪链条更触目惊心。杨某用银行卡刷POS机买黄金时，或许没想过61万元流水会换来两年刑期。“看似帮忙转账，实则成了骗子的‘工具人’”，这句话在采访中被反复提起。当“兼职刷单”“代收账赚佣金”的广告弹出时，很少有人意识到，出借的银行卡可能正在流转赃款，点击的链接或许已将个人信息卖给犯罪团伙。法律对“明知”的界定早已超越“直接知情”，那些“应当知道”却选择忽视的瞬间，就是踩向犯罪深渊的第一步。

民警总结的“防诈三问”至今清晰：钱往哪去？回报合理吗？关键信息敢说清吗？这三个问题像照妖镜，能让多数骗局现形。网购退款时，真客服从不会要银行卡验证码；社保异常会有官方渠道核实，绝不会让你下载陌生APP；“稳赚不赔”的投资，本质上都是冲着你的本金来的。可惜太多人在“高回报”的诱惑中忘了常识，在“熟人求助”的急切里放弃了核实。

采访结束时，电子屏正滚动播放反诈标语：“守住验证码，就守住了钱袋子”。突然明白，这场人与骗术的较量里，技术攻防固然重要，但更关键的是每个人心中的防线。当我们学会对“轻松赚钱”说不，对“紧急操作”慢半拍，对“私密转账”多核实，那些潜伏在数字世界的陷阱，自然就失去了生存的土壤。

防诈从来不是某个人的事，而是需要每个人都成为清醒的守护者。毕竟，最好的“护身手册”，永远是存于心底的理智与警惕。

警惕陷阱，多问几个为什么

高虎