

随着科技的进步，网络诈骗手段也在不断翻新。诈骗分子利用AI技术，可以惟妙惟肖地冒充某位家庭成员，向其家人张口要钱实施诈骗。这不，山东烟台的曲大爷就曾两次遇到了这样的骗局，好在曲大爷第二次成功“反杀”，并将“孙子”缉拿归案。

据媒体报道，2024年11月22日，71岁的曲大爷接到“孙子”的求救电话，说自己打伤了人，需要赔偿对方8万元，否则自己要坐牢。听说爱孙出了事，曲大爷非常着急，赶紧准备了8万元现金交给了前来取款的人，事后才知道，给自己打电话的是骗子。

一辈子的积蓄一下子被骗光，曲大爷气得病倒了。为了防止再次被骗，曲大爷随后开始学习防骗知识。让曲大爷没想到的是，这样的骗局又一次找到了自己。

2025年7月11日，曲大爷又接到“孙子”的电话，说辞和上次一样，让他赶紧准备钱。听对方说完，曲大爷气不打一处来，但随即冷静下来，决心将骗子抓住，于是耐着性子假装和对方嘘寒问暖，并答应过会儿交钱。挂了电话后，曲大爷随即报警，民警与其约定好了抓捕方案。

很快，曲大爷和民警守株待兔，将前来取款的张某抓获。在张某的配合下，民警很快将张某上线王某抓获归案。据张某交代，他是在网上看到一则兼职广告，工作内容是前往指定地点跑腿拿东西，每单可获得500元酬劳。日前，张某和王某被公安机关以涉嫌掩饰、隐瞒犯罪所得罪采取刑事强制措施。

曲大爷虽然文化程度不高，但在被骗了一次后，主动学习反诈知识，并配合民警设局，最终将假“孙子”抓获归案。可见，开展防骗宣传、提高群众的反诈意识，对于预防网络诈骗至关重要。

值得关注的是，在当前的网络诈骗中，像本案中张某这样的“工具人”大量存在。随着国家对网络诈骗的层层布控，诈骗分子线上转移资金难度越来越大，于是，他们以高薪兼职为诱惑，通过招聘“工具人”线下取现等方式获取被骗资金，然后再进行洗钱操作。

跑跑腿就能轻松获得丰厚报酬，稍微动动脑子就能想到这里面有猫腻。广大网约车、快递行业从业者以及兼职“跑腿”人员在接收运送物品订单时，务必要仔细核实包裹内容及下单人的身份信息，一旦发现可疑情况，要及时报警，别稀里糊涂地成了诈骗分子的帮凶。



本周刊投稿请
扫码加入QQ群

有人利用群众对军人的信任搭建情感纽带骗人投资，视频里的脸、军营场景全是假的，这是上游精心设计的圈套，而下线则无缝对接帮忙转移赃款——

AI换脸织就的诈骗迷网



◀2024年4月22日，检察官与公安干警研究案件。

供述，朱某彬曾专门培训他们应对检查的话术：“如果被抓，就把责任都推给匿名微信，说自己只是帮上线兑换虚拟货币，不知道钱的来源。”

公安机关调查发现，“姚建宏”的军人身份完全是伪造的。视频中的军营场景是犯罪嫌疑人从公开素材中剪辑的，“姚建宏”的面部是通过AI技术替换的真实军人影像，就连声音也是由语音合成软件生成的，能精准模仿军人的语气和常用词汇。

精准指控，深挖犯罪产业链

2024年5月25日，公安机关向检察机关提请批准逮捕蔡某忠等13人，7月22日提请批准逮捕叶某峰。检察机关分别于5月31日、7月26日作出批准逮捕决定，并向公安机关制发继续侦查提纲，建议公安机关调取虚拟货币钱包地址流水，持续追踪虚拟货币的具体走向，全力确定资金的最终去向，力求明晰资金的完整链条；依据人民币冠字码，倒查被害人的资金走向，确保每一笔资金的流动都清晰可溯；全面固定犯罪嫌疑人之间的通讯记录、聊天记录等所有可查消息，充分证实犯罪嫌疑人的共同犯罪故意，并侦查该犯罪团伙是否涉嫌其他犯罪。

公安机关经全面补充侦查查明，被骗资金兑换成虚拟货币U币后被分多笔转入境外电诈高发地区账户，梁某等被害人的转账及现金资金流向均与犯罪嫌疑人账户、银行记录精准匹配。公安机关还发现朱某彬曾组织诈骗平台等其他犯罪线索，新增47份证据材料，并冻结了蔡某忠、朱某彬的15万U币。

公安机关侦查发现梁某案并非个案，该犯罪团伙在多地参与多起类似诈骗案件。辽宁的吴某被“刘建成军官”骗走57.8万元，甘肃的唐某被“陈刚军官”诱导投入1108.9万元血本无归。经证实，共有13名被害人被骗数十万元至上千万元，该犯罪团伙转移资金达1300多万元，获利17万余元。2024年7月31日，公安机关以蔡某忠等14人涉嫌掩饰、隐瞒犯罪所得罪移送审查起诉。

检察机关经审查认为，蔡某忠、

朱某彬作为组织者与上线形成较为稳定的配合关系，直接对接境外电诈集团，安排取现和U币兑换，在犯罪活动中起主要作用，构成诈骗罪；谢某林等12人明知资金来源可疑，仍提供银行卡、运输现金等帮助，构成掩饰、隐瞒犯罪所得罪。2024年11月29日，检察机关以蔡某忠、朱某彬涉嫌诈骗罪，谢某林等12人涉嫌掩饰、隐瞒犯罪所得罪对该案提起公诉。2025年7月4日，该案开庭审理，法院将择日宣判。

案件办理后，检察机关并未就此止步，而是深挖犯罪产业链条。根据朱某彬的供述，成功抓获上游“U商”2人，扩破案件2起，进一步扩大了打击成果。

打好“打防管治”组合拳

2025年4月23日，针对利用AI换脸等“深度合成”技术实施网络诈骗犯罪活动问题，检察机关与公安机关联合发布《新型诈骗防范指南》，通过老年大学、社区讲座等多种渠道，向群众揭露“虚拟身份+高回报”的诈骗套路，提高公众的防范意识。在老年大学的讲座上，检察官用通俗易懂的语言讲解了AI换脸的原理和诈骗分子的常用手段，现场演示了如何识别AI换脸视频的破绽。老人们纷纷感慨，这种高科技诈骗手段确实不易识破，均表示受益匪浅。

5月9日，针对虚拟货币监管漏洞，该院向金融监管部门制发检察建议，推动建立USDT交易异常监测机制，对大额兑换、频繁跨平台转账、非正常时间频繁转账等行为实施预警。6月18日，该院还与公安机关、法院座谈，对虚拟货币的处置达成共识，并会签相关文件，为今后处置涉虚拟货币案件的财产提供参考。

在案件办理过程中，检察机关结合该案特点，开发出网络犯罪资金链溯源模型。目前，该模型在莱西市检察院办理网络犯罪案件中广泛应用，通过分析银行流水等数据，筛查犯罪团伙线索，推动公安机关立案侦查，为打击新型网络犯罪提供了技术支持。

□邵明岩 李笑东

2024年春，在山东省莱西市光阳医院(化名)门口，3名戴着口罩的男子正低声交谈，见梁某走过来后，其中一人从梁某手中接过一个黑色双肩包。这一幕看似寻常的街头交接，实则是跨境电信网络诈骗犯罪链条的关键一环——诈骗赃款的秘密转移，而此刻，这场交易已被公安机关纳入布控视野，成为抓捕行动的重要突破口。

随着3人的落网，一个涉嫌诈骗罪，掩饰、隐瞒犯罪所得罪的14人犯罪团伙彻底暴露。经查，该犯罪团伙为上游诈骗分子转移赃款1300余万元，并利用虚拟货币将资金转至境外完成洗白。值得注意的是，此次他们参与的诈骗犯罪暗藏新型手段——上游诈骗分子全程利用AI换脸技术实施诈骗，这也让该案的犯罪手法更具隐蔽性。

经山东省莱西市检察院提起公诉，7月4日，法院开庭审理该案，将择日宣判。

“现役军官”的甜蜜陷阱

2024年3月初，莱西市民梁某在刷短视频时，被一条婚恋弹窗广告吸引，点开广告链接，在页面上填写了个人信息，独居多年的她希望能在此找到晚年伴侣。没过多久，一个自称是“婚恋顾问”的人主动联系她，并将她推荐给了一个名叫“姚建宏”的人，对方自称是“驻湖南部队军官”。

“姚建宏”每天准时发来嘘寒问暖的信息，偶尔还会发来他身穿军装训练的视频，视频背景中有清晰的军营标语和嘹亮的军号声。更让梁某放下戒心的是，两人视频通话时，“姚建宏”还实时展示军营环境，有时视频中还有其他“军人”走动。

一段时间后，“姚建宏”开始向梁

某透露“好消息”：“我有内部渠道，能在‘某委买’平台上投资稳赚不赔，这是部队内部的福利，一般人根本接触不到。”他边说边发来自己的盈利截图，数字十分诱人。梁某起初有些犹豫，但在“姚建宏”的持续诱导和对高额回报的渴望下，决定尝试一下。

她按照“姚建宏”的指引，通过网银转账了197万元到指定账户，第二天登录平台时发现账户余额显示为412万元。“姚建宏”在微信里发来庆祝的表情包，并劝她：“机会难得，我托战友多争取了额度，不过这个额度需要通过承兑商线下操作，这样更安全，也是部队的规定。”

梁某完全相信了“姚建宏”的说辞。在接下来的10天里，她分四次将534万元现金在莱西市不同的茶馆、停车场交给了3个戴口罩的陌生男子。每次交接时，对方都显得十分谨慎，拿到钱后便迅速离开。

直到2024年4月中旬，平台突然无法登录，页面一直显示“系统维护”，梁某急忙联系“姚建宏”，却发现他的微信、电话全部失联，这时她才意识到自己被骗了。

2024年4月22日，梁某拿着一沓银行流水和聊天记录走进莱西市公安局报案。公安机关立案侦查后发现，犯罪嫌疑人一直与梁某沟通，疑似再次作案，于是要求其稳住犯罪嫌疑人，同时调取前几次犯罪嫌疑人取现的监控视频，研判目标，加强布控，为抓捕做好准备。25日上午10时，当骆某聪、黄某志、陈某甲3人准备取钱时，民警当场将3人抓获，在现场查获的手机里发现上线朱某彬发来的叮嘱：“口罩戴好，钱到就走，别多说话。”

用AI技术替换真实军人影像

2024年4月26日，公安机关邀请

身份证照片被AI生成了动态视频

湖北南漳：查办利用“换脸”视频骗过人脸检验系统的新型犯罪

□本报记者 戴小巍
通讯员 邱天 尹周航

“当心！假亲人、假领导可能正盯着你的钱包！”7月17日、18日，湖北省南漳县检察院干警与县公安局民警连续两天深入社区、走进养老院、来到快递站，轮番播放反诈微视频，揭露“AI换脸”这一新型诈骗的作案手法与防范要点。

“00后”自学AI换脸技术

2024年5月，南漳县公安局接到广州市公安机关移交的一条侵犯公民个人信息线索。根据线索，南漳县公安局找到了涉嫌利用AI技术合成人脸动态视频的陈某。

陈某是一名“00后”，原本靠打游戏、做代练谋生，因对AI换脸技术感兴趣，自学相关技能并在网上发布作品。很快，肖某联系他制作用于电话卡实名认证的AI合成人脸动态视频。在利益诱惑下，明知可能违法的陈某接下了“订单”。

随着侦查深入，一条“技术+物流”的新型犯罪链浮出水面：陈某和肖某等人从网络黑市非法获取大量公民高清身份证照片，利用AI换脸工具制成包含眨眼、张嘴等活体动作的动态视频，辅以无人直播插件骗过电信运营商人脸检验系统，非法激活电话卡；负责快递转运的李某、华某(已另案判决)通过电商平台批量购买电话卡，利用快递中途改址或专人转寄等方式“洗白”运输痕迹；秦某则当起“中间商”，把激活的电话卡以450元到550元一张的价格卖给卡商，最终流入诈骗团伙手中。

检警联手锁定关键证据

在南漳县公安局物证室内，10余台电脑主机、20余部手机和成捆的电话卡静默陈列着。面对犯罪团伙使用境外加密聊天软件联络、虚拟货币交易结算等反侦查手段，2024年7月，南漳县检察院依法介入该案，在电子证据固定方面引导公安机关对查封的电子设备展开三重勘验，提取加密聊天记录、复原AI操作痕迹，追踪虚拟货币流向，构建起完整证据闭环。

为证实技术帮助与诈骗结果的关联性，检察官列出23项补充侦查提纲。公安机关通过国家反诈平台对涉案电话卡逐张比对，锁定54张卡直接用于实施诈骗，将上游技术帮助行为与下游诈骗造成的巨额损失紧密关联。同时，检察机关在审查中发现李某、华某等涉案漏犯线索后，依法监督公安机关追诉，力求彻底摧毁犯罪网络。

守好数字时代群众“脸面”安全

今年4月，这起由南漳县检察院

提起公诉的帮助信息网络犯罪活动案宣判，陈某被判处有期徒刑二年二个月，并处罚金5000元；肖某被判处有期徒刑一年，并处罚金5000元；秦某被判处有期徒刑一年八个月，并处罚金1万元，涉案工具和违法所得被依法处理。

该案查获的1183张居民身份证照片大多源于网络泄露。“这些身份证照片一旦被用于AI技术激活电话卡，就成了诈骗工具。”办案检察官解释，诈骗分子用这些“实名”电话卡冒充客服、公检法人员，实施精准诈骗。

检察官提醒广大市民，要保护好个人身份信息，切勿随意上传手持身份证照片或视频；定期通过运营商官方渠道查询自己名下的电话卡，若发现信息被冒用或遭遇可疑诈骗，要及时保留证据并报警。



违法滥用AI换脸技术面临哪些刑事法律风险？

在使用AI换脸技术时，非法收集、使用或泄露他人的人脸信息等敏感个人信息，可能会构成侵犯公民个人信息罪；

制作嘲讽或丑化他人的换脸视频，实施网络欺凌或者发布侮辱性内容的，可能构成侮辱罪；

利用AI换脸技术制作、传播含有淫秽内容的视频或图片的，可能构成制作、传播淫秽物品牟利罪或传播淫秽物品罪；

利用AI换脸技术伪造他人身份，通过视频通话等方式实施诈骗，骗取他人财物的，可能构成诈骗罪；

利用AI换脸技术，帮助网约车司机绕开平台的人脸验证机制，实现随意注册新账号或者使用他人账号接单的非法目的，可能构成提供侵入、非法控制计算机信息系统程序、工具罪。

AI伪造风险识别与防范

动作验证法：当视频中对方(尤其是涉及转账、借钱等敏感要求时)显得有点“怪”，则急着答应。请对方做一个连贯的转头动作，或者用手掌完全遮住脸再快速移开。目前的AI技术在模拟这些复杂的面部遮挡和光影变化时，容易出现卡顿、模糊或扭曲。

声音细节辨真伪：仔细听语音细节。AI生成的语音有时会缺乏自然的呼吸停顿、情感起伏，或者带有轻微的机械感、背景杂音异常。

多渠道核实身份：涉及金钱交易或敏感信息时，务必通过其他可靠途径二次确认。比如，问一些只有对方知道的问题，挂断视频后直接拨打对方常用且你熟悉的电话号码(不要回拨可疑来电号码)，或者通过共同认识的第三人进行侧面核实。这是最核心的一招！

◀2023年4月26日，检察官在月湖广场开展反诈宣传。

▼2024年2月17日，检察官在老年大学开展反诈宣传。