银行客户“被刷脸、被转账”，人脸识别诈骗风险频发谁之责

银行引入人脸识别技术作为辅助手段，初衷在于加高金融“防火墙”；但电信诈骗分子特意针对人脸识别设计了一套诈骗话术和诈骗手段，不断试探这条防线的薄弱之处。

2022 年 9 月 1 日，郭先生在微信群中留言称，“交通银行人脸识别盗刷案”的二审时间可能要推迟。此时距离他不服一审判决并提起上诉，已经过了近两个月。

这个数十人的微信群中，还有其他类似案件的受害者，“群主”郭先

生是此前“交通银行人脸识别盗刷案”的原告代理人，他的妻子李女士于 2021 年 6 月遭受电信诈骗，损失近 43 万元。

与以往的诈骗“套路”不同的是，这起案件中的诈骗分子并未要求李女士向诈骗分子提供的银行账户转账，而是要求她前往交通银行开设一张新银行卡，并将她在其他账户中的资金转入这张新卡。

事后经查，操作李女士名下的这张借记卡，对于诈骗分子来说如同探囊取物。这张借记卡开通后 15 分钟，诈骗分子随即更改了李女士手机银行的用户名和密码；此后，又将这张借记卡原本的 5 万元转账额度提高，最终将其账户中的 40 万余元悉数转出。而这些操作，理论上均需要“本人”通过“人脸识别认证”方可完成。

重置密码、提高转账额度、大额转账等环节之所以加入人脸识别作为辅助，是作为替代“柜台认证”的一种手段，目的在于“确认本人”。然而在本案中，公安机关与法院已经确认，前述操作均非李女士本人进行。

2022 年 6 月 30 日北京市丰台区人民法院作出的一审判决认为，原告李女士“未就其案涉银行账户尽到力所能及的审慎管理义务”，银行方面无需对原告案涉借记卡内资金损失承担民事赔偿责任。7 月 10 日，郭先生作为李女士的代理人上诉，该案二审由北京金融法院

受理。

截至发稿，交行以此案正在司法程序中为由未作出回应。

银行在部分业务中引入人脸识别技术作为辅助手段，初衷在于加高金融“防火墙”，以期给客户的账户与支付安全带来更便利、可靠的保障。但在攻防的另一端，则是电信诈骗分子伺机而动，特意针对人脸识别设计了一套诈骗话术和诈骗手段，不断试探这条防线的薄弱之处，以谋不义之财。

发生类似风险案例时，个人和金融机构各应承担什么责任？对于针对人脸识别技术的新型诈骗手段，金融机构如何升级反诈技术、防控风险？

Ⅰ.”刷脸“风波

2021 年 6 月的一个上午，李女士遭遇了电信诈骗。

据李女士事后向公安机关自诉，上午 10 点 30 分，她接到一位“北京市公安局户政科陈杰警官”的电话，对方称其护照涉嫌在哈尔滨非法入境，随后又将其电话转接给一位“哈尔滨市公安局的刘姓警官”，对方又称她涉嫌一起“李燕反洗钱案”

电话中的“警官”告诉李女士，警方要“清查个人财产”，因此询问了李女士银行卡及账户余额的信息，并点名要求李女士办理一张交通银行的银行卡，并将名下其他银行卡中的钱全部转入新办理的这张卡中，还要求李女士”将可支配贷款额度贷满。也把所有贷款全部转到交通银行中"。

当天下午，她前往交通银行北京长辛店支行，于 13 点 36 分开通了一张借记卡，办理了“开通手机银行和网上银行”业务。但郭先生表示，直到当天下午 4 点半李女士前往派出所报警之前，都未对手机银行进行激活。

事后经查，在这张借记卡开通后仅 15 分钟，其手机银行的用户名和密码就被重置。开卡后的一个小时内，李女士交通银行账户中的合计 42.9 万余元，分 4 次被悉数转出，分别进入了四个不同的账号。

除了最后一笔转账金额为 3 万元，其余三次该借记卡转出的金额单笔均超过 9 万元，最高达 20 万元，超过了李女士在开卡时选择的“开通小额转账汇款，单日累计 5 万元，单笔最高 5 万元"的转账限制。

银行卡里的钱不翼而飞，李女士难以理解。她对办案民警自诉:"期间，我没有操作转钱，也没有下载过手机银行 App，没有输入银行密码

等信息，也没有收到交通银行的风险提示信息。"

根据公安机关的调查，4 笔案涉借记卡的对外转账系台湾的 IP 地址操作。一审判决书中，法院确认，案涉交易"符合他人盗取并适用持卡人银行卡网络交易身份识别信息和交易验证信息进行网络交易……的网络盗刷交易行为法律特征”。

诈骗分子为何能够冒名”转账?

银行提供的交易信息显示，在李女士分次向交通银行借记卡转入 30 万元后不到 5 分钟，这张借记卡就通过“人脸识别”的方式提高了转账限额。根据李女士诉交通银行长辛店支行的一审判决书，双方均认可这张借记卡曾“通过人脸识别重置登录密码及提高转账限额"。银行方面也表示，案涉交易采用交易密码、动态密码以及辅助人脸识别的客户鉴别模式。

一审判决书显示，案发当日，李女士的交通银行借记卡共进行了 6 次需要"人脸识别活检”的操作，包括 1 次登录密码重置和 5 次大额转账，活检结果均为“成功”，并显示“人脸识别成功通过”。

这说明，本应用于“确认本人身份”的人脸识别系统，却由“非本人”通过了。

“2020 年 10 月至 2021 年 10 月期间，发生了多起这样的案件。仅是我知道的就有 7 个受害者，都是被诈骗分子要求去交通银行开卡。"郭先生认为这是电信诈骗分子有计划地瞄准了交通银行在人脸识别方面存在的漏洞。

就在李女士将交通银行长辛店分行告上法庭时，另一位北京的买女士也遭遇了类似的电信诈骗。2021 年 8 月，买女士接到了'北京市出入境管理局的警察”打来的电话，同样为买女士转接了“哈尔滨公安局”。

“他们怀疑我把银行卡提供给犯罪人员进行非法洗钱，说现在给我一个'复讯机会。"买女士自诉，"一个自称黄警官的人要求我提供我所持有的银行卡卡号，以供他们调查我近期的银行卡流水。"

随后，买女士也被该名“警官”要求，前往交通银行办理一张新的银行卡作为“安全账户”，甚至以买女士当前为“警方监控对象”为由，要求买女士向这张卡里存入“取保候审保证金"。最终，心神不宁的买女士不得不借款以凑齐这笔钱，在新办理的交通银行卡中存入 40 万元。当天，买女士这张交通银行借记卡中的近 40 万元资金被冒名转走。

此外，买女士另一张此前办理的中国工商银行借记卡的账户信息被诈

骗分子骗得后，卡上资金亦被转走。最终，买女士总计 58.76 万元被先后分 8 笔转出，单笔转账最低 5 万元、最高 13.5 万元。

买女士提供的资料显示，2022 年 2 月，北京银保监局对买女士的举报作出回复。北京银保监局的调查意见书显示，在买女士受骗当日，其工商银行借记卡确实曾“经人脸识别验证通过”，将转账限额调高至单笔/日限额 20 万元”，即开通“一键大额转账”:其交通银行借记卡所办理的调高转账限额(由单笔 5 万元调高至单笔 20 万元)和 4 笔对外大额转账，也均“经人脸识别验证通过”。

II. 拆解“盗脸”过程

“确认本人”是银行账户安全和支付安全的重中之重。通常来说，银行常用的身份认证工具包括 U 盾(USBKeys)、电子密码器、短信验证码、密码，以及包括指纹、“刷脸”在内的生物信息识别等。其中，人脸识别技术被不少技术人士和银行业人士认为，是一项成熟且便利的身份验证手段。

中国信息通信研究院安全研究所 2020 年发布的《人脸识别技术在 App 应用中的隐私安全研究报告》介绍，人脸识别的主要环节包括人脸图像采集及检测，人脸特征关键点提取、人脸规整和图像处理、以及人脸识别对比。当 App 扫描用户人像时，经活体检测、人脸质

量检测、人脸图像等处理后与先前获取的用户人像照片进行人脸对比，完成身份验证的过程。

那么诈骗分子又是如何骗过了银行的人脸识别系统?据各方了解，多位受害者都曾与诈骗分子进行视频连线、或向诈骗分子发送视频，这或许是人脸信息被盗取的关键。

李女士对警方表示，诈骗分子曾要求她在手机上下载一款在线会议软件“瞩目 Apd”，开启会议模式以核实身份信息等。买女士也自诉，诈骗分子要求她下载“瞩目 App”与她核实身份，还要求她“用手机录制多段点头、摇头、眨眼的视频，通过 QQ 发送给他们"。

可以看出，受害者的人脸信息在诈骗分子的引导下“泄露”，引发了“盗脸"风险。不过一个关键问题是，既然人脸识别系统设有“活体检测”环节，为何还会错将视频中的人脸当作了真人?

一位人脸识别领域资深人士分析，诈骗分子有可能采取了“底层注入”的手段。"这种手法是指诈骗分子在他们自己手中的手机上，下载木马程序，通过一段代码'劫持'手机摄像头。这样，他们就可以将录像'注入’，让这台手机上的摄像头以为这段录像来自于实时影像。"

“正常来说，这种手法只有在很巧合的情况下才能成功，因为银行对

于实时的人脸验证有很多环境条件的要求。"不过前述人脸识别领域资深人士也坦言，由于这种风险本身并不在银行系统中，防控起来确实有难度，“因为他们攻击的不是银行系统，而是自己的手机。"

他介绍，目前银行业的应对方法包括将高风险的、容易被木马程序劫持和篡改代码的手机型号列入高风险手机名单，并考虑到当前的风控模型中。

除了这种针对终端的攻击模式，仅从算法的角度来看，直接进攻人脸识别算法的途径主要还有三种:面具、屏幕(即视频)和 3D 头模。

其中，最简单的就是直接将照片打印出来，做成面具。"有的银行要求眨眼、张嘴，那我就把眼球和嘴巴那里给抠出来。"一名互联网公司人脸识别技术负责人解释，过去这种面罩可能就是简单的纸张，未来还可能会有更多材质。

第二种是通过屏慕播放提前录制的视频。“这屏幕也会分很多，比如现在有(分辨率)4K、8K 的屏幕，有视网膜屏等。"第三种攻击手段则是利用 3D 头模。“这个攻击成本就非常高了，材料有树脂、硅胶、玻璃钢等，甚至这个头模里面还有可能加一些机械，可以动。”前述互联网公司人脸识别技术负责人解释道。

从人脸识别系统本身，行业内针对以上攻击手段已经发展出了对策。"我们会在摄像头上打出一些主动的'炫彩’，这种光打在屏幕上时的反射和打在正常人脸上的反射是很不一样的，这样就可以防御一部分攻击。"该负责人介绍，"再比如说 3D 头模，它可能就没有下半身，或者它是没有微小移动的，而一般真人在验证过程中，脸部区域不可能一动不动。"

“也就是说，人脸识别系统的防御，一定是软硬件有一些主动的或者被动的交互配合，再加上一些静态模型，再加上一整套风控系统。"他续指。

以李女士的这起交通银行纠纷为例，这位互联网公司人脸识别团队负责人指出，"比如当时登录网银的 P 地址在台湾，而客户又很显然不可能在台湾，那么(系统)是不是可以把当时的操作认定为高危操作?”

Ⅲ. 为何多道风险防线失效

2019 年 9 月，人民银行科技司司长李伟在金融网络安全论坛上指出，不要简单地将人脸特征作为唯一的交易验证因素，粉享据风险等级结合用户口令等其他因素进行多因素认证。

另一位人脸识别服务技术提供商负责人对财新坦言:“线上的人脸识

别活体验证，只是防欺诈或风控体系中的一环，还是要配合很多其他手段，包括密码、短信验证码，多因子验证来提高安全等级。"

遗憾的是，在前述李女士、买女士以及其他几起类似的人脸识别盗刷案中，银行所提供的其余风控手段均被诈骗分子攻破。

在诈骗分子的诱导下，李女士下载了"公安防护 App"这个手机软件程序。在李女士第一次向公安机关报案时，她提及诈骗分子曾通过“瞩目 App”的屏幕共享功能，指示她“将手机的拦截电话、短信等功能开启"。不过，她随后在庭上否认了该说法，但李女士的否认未被一审法院采纳。

据一审判决书，在李女士遭盗刷期间，第二笔转账发生后，交通银行曾给李女士扶出三次电话。前两次未能接通，第三次银行电话被接起，"过程中客服询问了是否(李女士)本人、是否本人操作转账 10 万元、是否知道收款人名字、与(收款人)的关系、转账的用途、是否接到过自称公安局或其他陌生电话等，对方均认可系(李女士)本人操作，并称和(收款人)是朋友关系，转账 10 万元是业务往来，没有接到过陌生电话。"

此外，一审判决书中写道，交通银行还在交易过程中向李女士预留的手机发送 22 条短信密码。但郭先生表示:“犯罪分子试图用短信验证

码登录失败以及重置密码时的短信提醒，四次转账的验证码，还有调整额度的短信验证码，我爱人都没有收到。”

买女士的情况与此类似。据北京银保监局的调查，交通银行除了向买女士发送短信验证码，还两次拨打了买女士的签约手机号，“对方回答流畅，表示未曾接到自称公安机关的电话，认识转账对象，是本人正常交易。"工商银行则在当日向买女士发出至少 24 条短信。

虽然买女士并未明确表示自己设置了短信和电话的拦截功能，但她父亲表示，女儿并未收到过银行的来电和短信。

据了解，像买女士当日在工行“被交易"的情况，需要经历三个部分的操作流程。第一部分是登录手机银行，由于该设备并非买女士的常用设备，除了输入手机银行登录密码，还需要输入接收的短信验证码，并输入银行卡的密码。

第二部分是调高转账额度，需要短信验证码、支付密码和人脸识别“三道坎”全部通过，才能开通“一键大额转账”。

第三部分是具体的三笔转账，其每一笔都需要经过三重认证:支付密码、短信验证码和上行短信。所谓的上行短信，是指银行方面向用户发送短信、并需要用户向适定号码转发该条短信，方可成功操作。

买女士提供的包含 24 条短信的详单，勾勒出了当日 12 点 30 分至 13 点 20 分之间，她工商银行借记卡上发生的共计八次转账尝试。其中，有六次交易尝试触发了上行短信，提示“确认汇款请将本短信转发至 95588，5 分钟内有效”，其中的三笔交易通过了转账的“三重认证”。

一位银行网络金融业务人士对财新表示，一般触发了"上行短信”这种防控措施，说明后台的人工智能模型已经检测到了异常交易，并对相关交易开启了增强型验证。例如短时间内发生多笔大额交易、与过去历史交易情况不符，同一 MAC 地址发生多台设备登录，或者账户涉及公安部门提供的黑名单以及与之关联的灰名单等，这些都是风险的特征。"

对于银行来说，人脸识别只是风控体系中的一个辅助手段，不会是独立的、惟一的手段。在这个案例中，必须得是以上所有步骤都发生了信息泄露，才会让诈骗分子得逞。”前述银行网络金融业务人士无奈道。

IV. 谁来担责?

从技术上来说，人脸识别技术和绝大部分风控手段一样，难以确保

“万无一失”;而且人脸识别只是多道风控防线中的其中一道。风险发生后，究竟该由谁来承担"被刷脸”的责任?

一审法院认为，李女士按诈骗分子的指令下载相关 App 并且开启会议模式等行为，导致了身份识别和交易验证信息泄露的风险，“成为导致其案涉银行卡内款项被划去的关键原因”“可以认定李女士在案涉 42.9 万元被盗刷的过程中过错明显".“(交行长辛店支行)已通过多个登录密码、验证码、人脸识别的合理方式识别使用人身份，未见存在明显的错误或过失。”

北京银保监局 2022 年 2 月对买女士回复的调查意见书称，"未发现上述过程中，工行北京市分行存在违反银行业监督管理法律法规的情形":以及“未发现充分证据证明交通银行北京市分行在上述过程中存在违反银行业监督管理法规的情形”。

银保监会在 2022 年 5 月 10 日对买女士的回复中则写道:"在银行开户、转账时，客户需使用短信验证码、支付密码等多重认证手段，认证通过后可进行交易，人脸识别是辅助技术手段，不是交易成功的决定性因素，也不是实施交易的必备手段。"

其实这个(案件中)没有真正意义上地突破人脸识别技术，主要还是因为被骗了。"一位国有大行金融科技相关人士认为。

前述互联网公司人脸识别技术负责人也无奈表示:“如果用户连短信都提供了，那别说是再加一道人脸识别，加什么都会攻破的——这本质上就是诈骗，不是刷不刷脸的问题。"

但负责李女士二审上诉的代理律师却不同意这种说法。他认为，一审判决混淆了泄露的账号信息的过错和人脸识别导致损失的过错。

“用户显然不是没有任何过错，但是人脸识别系统的问题，用户确实是完全不知情，而且也是用户完全无法控制的。"李女士上诉代理律师强调。

他指出:"哪怕堂握了交易密码和验证码，那么传统验证方法所能够导致的转账金额本身其实也是有限的。现在法院认为用户有泄露验证码的过错，哪怕有过错，是不是也应当限定在特定范围?"

李女士上诉代理律师认为，李女士泄露验证码只能导致一定限额内的盗刷损失，即开卡时李女士与银行约定的“5 万元以下小额转账”；之所以最终损失被放大为 40 余万元，是由于有人冒用了李女士的人脸信息。“那么在短信验证码范围之外的损失，即只有通过了人脸识别才能实现转账’的这部分，应该由银行来承担责任。"

买女士的律师也主张，其工行卡中的损失系由最高转账限额被修改所

致，而工行对虚假的人脸识别予以验证通过，应对限额提高范围内的损失承担赔偿责任:而交行的交易规则本就要求“密码+验证码+人脸识别"完成，因此将要求交行赔偿全部损失。

目前，郭先生和李女士仍等待二审开庭的时间，其他类似受害者和他们的家属也在密切关注着此案的动向。