诈骗风险攀升 数据风控需多维加码

AI应用B面

本报记者 蒋牧云 何莎莎
上海 北京报道

每个硬币都有两面。随着AI技术在金融领域落地，数据安全、隐私保护等问题也日益凸显。

《中国经营报》记者了解到，近期金融领域的AI诈骗数量上升趋势明显。同时，由于违法证据收集难度较大，导致部分AI诈骗躲避了法律制裁。对此，不少金融企业也在不断升级自身风控体系，并将包括大模型等AI技术应用其中。

值得思考的是，AI诈骗攻防战背后，引出了AI技术如何保持可控与可用之间平衡的问题。对此，多位业内人士向记者表示，金融行为中包含诸多行为细节与需求、相关业务条款等，如何形成一个“法规-模型堤坝-用户需求”之间的动态平衡，将是行业内的永恒命题。为此，需要企业、行业、政府、公众等所有层面的共同努力。

诈骗门槛降低

此前，诈骗分子想要打造这样的3D模型，需要的图片素材在300张～500张。如今，只要10张甚至更少的不同角度图片，就可以生成较为真实的立体面部模型。

据了解，目前AI诈骗的形式包括AI换脸、AI拟声、虚假验证、网络钓鱼、身份窃取等。有技术人士告诉记者，AI的加持导致诈骗变得更加隐蔽和智能化。比如，通过AI更精准地模拟用户行为，分析用户数据以获得关键信息，并发起更复杂的欺骗活动，这增加了金融机构的风险识别和风控难度。

AI诈骗行为也在近期成为重点打击的对象。近日，公安部在北京召开新闻发布会，通报全国公安机关打击整治侵犯公民个人信息违法犯罪行为的举措成效。其中，针对“AI换脸”导致群众被欺诈的问题，公安机关发起专项会战，侦破相关案件79起，抓获犯罪嫌疑人515名。特别地，针对装修、贷款等骚扰电话的问题，公安机关联合工商部门也开展了专项整治。

警方发布的一例较为典型的案例显示，来自福建的郭先生是一家科技公司的法人代表。2023年4月，他的好友突然通过微信视频联系他，称自己的朋友在外地竞标，需要430万元保证金，想借用郭先生公司的账户走账。基于对好友的信任，加上已经视频聊天“核实”了身份，郭先生在10分钟内，先后分两笔把430万元转到了对方的银行账户上。事后，郭先生拨打好友电话才得知被骗，原来骗子通过AI换脸和拟声技术，佯装好友对其实施诈骗。

那么，AI换脸是否也能突破金融企业的风控体系？对此，某金融科技企业风控人士告诉记者，对于逼真的立体面部模型，实际上是可以突破金融机构面部识别这一关卡的。此前，诈骗分子想要打造这样的3D模型，需要的图片素材在300张～500张。如今，只要10张甚至更少的不同角度图片，就可以生成较为真实的立体面部模型。该人士还补充道，除了换脸之外，拟声也是AI诈骗常用的手段。通常，诈骗分子会提前通过骚扰电话等获取声音素材，随后再合成相似的声音，与脸部素材一起，生成极为逼真的视频。

不过，金融机构的防范体系有多个环节，除了脸部识别之外，往往还会有资金异动监控、异地设备登录提示等。同时，应对不断增加的诈骗案例，金融科技企业也在不断升级防范体系，其中也应用了包括大模型的最新AI技术。奇富科技相关负责人告诉记者，该公司通过独有的“山海”安全态势感知系统，能够深入业务全流程环节，有效实现了风险筛查、预警、识别、分析、决策、处置全流程AI辅助监控与响应。依靠这类系统化技术建设，奇富科技对AI诈骗乃至整个电诈行为都有完整的防范体系。

奇富科技消保工作半年报显示，其2023年上半年面向用户AI反诈提醒3.3亿次，反诈科普教育覆盖1200万人次；智能及人工反诈劝阻团队累计拦截劝阻潜在被骗者3.9万人，保护用户避免损失5.1亿元；智能风控反诈系统拦截涉赌人员超30万人，拦截疑似涉赌资产约32亿元，电信诈骗财损同比下降50%。

信也科技相关负责人也告诉记者，保障数据流通交易安全是AI反诈工作的重要基础，公司针对金融反欺诈场景进行了深入研究，成功研发了图联邦技术Fate-Graph。FateGraph的推出，不仅解决了图数据在不同单位和机构之间的孤岛问题，也扩展了隐私计算的应用范围。目前，为进一步推广该技术，信也科技正持续加强研发创新投入，控制通信成本，在计算过程中实现对数据的保护，推动隐私计算更广泛的落地。

根据公开信息也可以看到，近期包括腾讯云、度小满、京东等在内的多家企业均将大模型技术应用到了金融风控。比如，2023世界人工智能大会期间，腾讯云宣布升级MaaS平台，将行业大模型能力应用到金融风控。据悉，采用行业大模型的金融风控解决方案，相比之前有了10倍的效率提升，整体反欺诈效果比传统模式有20%左右的提升。

寻求可用与可控的平衡

从具体的合规操作来看，将AIGC产品保持一个可控可用的平衡，将是一个长久的命题。

在业内人士看来，AI诈骗频发的背后，反映出面对AI等较新的技术，数据保护等行业规范还有待跟进。对于金融科技企业而言，除了需要警惕自身信息泄漏、技术漏洞之外，也对企业自身的合规管理提出了更高的要求。

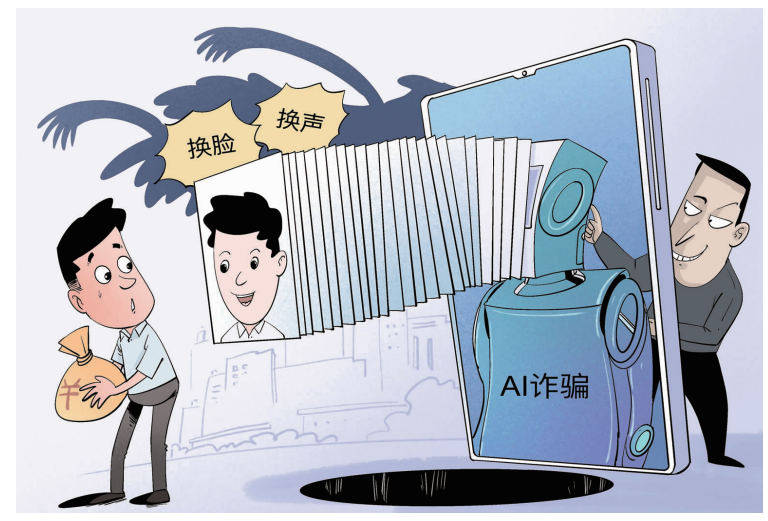
恒生电子AI技术专家向记者表示，目前AI技术进步飞快，而原有的政策法规和伦理规范并不能快速跟上技术发展。在极具变化的科技和市场环境下，AI技术公司和研究人员专注于技术本身和商业效益，可能会在社会影响方面形成一定的忽视，因此更加需要对新技术制定相关监管政策和法律法规。

近期，相关的监管办法也在逐渐跟进。国家网信办出台的《互联网信息服务深度合成管理规定》于今年1月10日正式施行，主要针对深度合成服务者的义务进行了规定。其中要求，深度合成服务提供者提供智能对话、合成人声、人脸生成、沉浸式拟真场景等生成或者显著改变信息内容功能服务的，应当进行显著标识，避免公众混淆或者误认。

在AIGC（生成式人工智能）方面，国家网信办等七部门联合发布《生成式人工智能服务管理暂行办法》，于8月15日起施行。其中要求，生成式人工智能服务提供者开展训练数据处理活动时，要使用具有合法来源的数据和基础模型，涉及个人信息的，应当取得个人同意或者符合法律、行政法规规定的其他情形等。

那么，金融科技企业在进行AI技术应用时，具体如何保护数据安全？

恒生电子AI技术专家表示，针对数据安全和隐私保护，恒生电子采取了一系列的措施来确保数据的脱敏、合规、授权和追溯，包括：去除数据中所有敏感的个人以及机构数据；对收集的所有数据进行匿名化和加密处理；制定严格的数据使用规范和访问控制，只允许授权人员在控制环境下使用数据；记录所有操作行为保证数据来源可追溯；与用户签订数据保密协议，明确数据所有权和使用期限等。同时，恒生电子还通过建立可靠的网络安全系统、定期开展安全评估等方式，识别和消除数据安全隐患。



目前AI诈骗的形式包括AI换脸、AI拟声、虚假验证、网络钓鱼、身份窃取等。 视觉中国/图

奇富科技相关负责人也告诉记者，基于公司在金融科技领域的持续积累，形成了金融安全的顶层系统性设计思路。在设计金融行业专属的大模型时，奇富科技充分考虑到了敏感数据收集和处理问题，如在不牺牲实用价值的同时，预先设置信息过滤壁垒和敏感数据围栏，依照用户需求判别行业特性后，将用户数据或敏感数据预先封装阻隔，只进行单次处理，只针对脱敏部分完善训练。与此同时，通过产品与规则设计，将金融行业政策规范文档与条款产品化，通过预处理，让大模型处于安全可控的笼子里。

不过，该负责人也指出，从具体的合规操作来看，将AIGC产品保持一个可控可用的平衡，将是一个长久的命题。“具体来说，人类自然语言、AIGC技术的发展、各个行业的法条规范三者之间有动态的变化关系，人类自然语言变化与AIGC技术可能是正相关的，二者相互促进。而相关行业规范与法条则是必不可少的抑制力量，以我们的经验而言，法条可以产品化、预设化加入到大模型训练，相当于为人脑预设类似于‘道德’的堤坝。以金融行业来说，金融行为中无数的行为细节与需求，无数的相关业务条款，如何将法条产品化、规则化预设，形成一个‘法规-模型堤坝-用户需求’之间的动态平衡，将是行业内的永恒命题。”该负责人谈道。

对此，恒生电子AI技术专家也表示，要解决前述问题，还有诸多可以努力的方向。具体而言，企业层面需要不断优化算法和技术，建立内部安全审查制度，主动接受外部监管，以规避人工智能可能带来的数据安全与社会伦理问题；行业层面则需要建立AI指引规范，开展行业认证，形成行业自律；政府层面也有待加快出台AI监管法规和政策，推动行业合规发展，鼓励公众监督参与，加强国际合作。此外，公众也需要逐步提高对AI的理解，理性看待AI的进步。

深入触达小微企业 大数据破解融资风控难题

本报记者 张漫游 北京报道

在助力国民经济持续恢复的呼声下，小微企业近期再迎利好，其中多是为小微企业融资“亮绿灯”的政策。

除政策方面的扶持外，金融机构的支持也十分重要。业内人士认为，小微企业融资难、融资贵，其根源在于银行和小微企业之间信息不对等。随着先进技术深入到金融业务当中，银行为小微企业提供融资的全流程线上化程度、对小微企业融资需求的响应度均得以提升，小微企业融资的贷后管理更加智能化。

在采访中，《中国经营报》记者了解到，对小微企业的风控问题依然是制约企业融资的一大难题，也是下一步金融科技发力的重点。

应对“数字鸿沟”

2023年上半年，小微企业获得的融资规模持续提升。

国家金融监督管理总局有关部门负责人介绍称，截至6月末，全国普惠型小微企业贷款余额27.37万亿元，有贷款余额客户数4115.12万户，两项指标过去五年平均增速已超25%；普惠型小微企业贷款平均利率同比下降0.49个百分点，民营企业贷款平均利率同比下降0.25个百分点。

与此同时，近期助力小微企业融资的政策络绎不绝。

例如，财政部、国家税务总局日前发布《关于支持小微企业融资有关税收政策的公告》；工业和信息化部、中国人民银行等五部门联合印发《关于开展“一链一策一批”中小微企业融资促进行动的通知》；中华全国工商业联合会、中国银行业协会向各金融机构发布2023年“助微计划”倡议书，提出共同推动经济运行持续好转，共助小微加速回暖复苏。

谈及金融机构不敢放心大胆地给小微企业贷款的原因，国家金融与发展实验室金融法律与金融监管研究基地秘书长尹振涛分析称：一是小微企业由于缺乏抵押担保品及其他资产增信手段，很难通过银行的风控要求；二是由于贷款金额小，利息无法覆盖银行的资金、风控及人力等成本；三是担忧小微企业经营变化太快，增加银行的贷后管理工作和难度。

随着数字技术的迅猛进步和在金融领域广泛运用，金融科技在小微企业融资方面的支持作用越来越明显。数字化赋能已经成为打破传统信贷模式、解决小微融资难题的关键因素。近年来，银行也加大了科技赋能，助力小微企业融资。

如中国工商银行聚焦“场景+”生态共建，依托“网贷通、经营快贷、数字供应链”三大线上核心业务，培育和打造了一批贴近市场、贴近客户、贴近需求的线上融资产品，全方位满足小微客户多样化的融资需求。该行副行长段红涛透露道，2023年将全面提升小微金融服务的数字化水平，持续推动普惠业务下沉。

再如近期兴业银行与中国电子口岸数据中心、中国出口信用保险公司开展合作推出了跨境融资产品——小微企业跨境融资-信保贷，该产品通过大数据模型构建客户“画像”，全方位满足小微企业“短、急、快、频”的融资需求，助力缓解出口型小微企业融资难、融资贵问题。

值得一提的是，小微企业数字化和信息化程度普遍不高，大多采取单一化经营，抗风险能力较弱。为解决小微企业“小额、短融、高频”金融需求特点带来的“风险识别难”和“作业成本高”难题，具体到操作层面，新网银行风控科学部总经理刘嵩告诉记者：“新网银行通过数字技术从业务模式、技术手段、风险方法等方面搭建起了一套以BC联动为核心理念，把C端业务锻造出的风控能力迁移至B端小微企业的数字普惠业务，在策略、模型、系统多个方面迭代升级，应用迁移学习技术以BC联动的方式升级模型体系，使用人企组合评估的方式迭代风险策略体系，利用自研外部数据平台和模型计算平台为策略和模型提供基础技术能力，打造了完整、有效、可持续的风控体系。”

谈及先进技术主要解决了小微企业融资面临的哪些问题，江苏苏宁银行金融科技高级研究员孙扬梳理道：一是通过精准营销，解决了小微企业在融资中难以匹配合适金融产品、金融机构难以触达小微企业的问题；二是通过大数据，丰富了小微企业画像，解决了金融机构对小微企业了解不够深入的问题；三是通过图像识别、智能客服等技术，解决了金融机构服务海量小微企业效率低、成本高等问题；四是通过区块链、联邦学习、隐私计算等技术，解决了金融机构如何在安全合规的前提下和平台合作服务小微企业的问题。

尹振涛补充道，科技赋能可以增强小微金融专业化服务能力，运用金融科技手段和平台化思维，探索形成批量化、规模化、标准化、智能化的小微金融服务模式，这一模式就是所谓的小微企业信贷工厂。例如，“310”（即3分钟申贷、1秒钟放款、全程0人工介入）全流程线上贷款模式，可以最大程度降低贷款成本、提高服务效率，解决小微企业的短期流动性资金问题。同时，借助金融科技的力量，金融机构还可以为符合授信条件但未办理登记注册的个体经营者提供融资支持，激发创业动能。

风控水平待提升

中国人民银行党委书记、行长潘功胜曾强调，针对普惠金融发展面临的服务门槛高、覆盖面不足、“数字鸿沟”等难题，坚持问题导向和目标导向，充分运用移动物联网、智能终端等现代信息技术拓展金融服务渠道、扩大服务半径、降低边际成本，推动网络化、智能化金融业务与生产生活场景深度融合，打造产品丰富、交互智能、流程高效的数字普惠金融服务体系，不断提升普惠金融的下沉深度、覆盖广度。

在当下，即使利用金融科技，小微企业融资还有哪些问题待解决？

孙扬认为，金融机构开展小微企业融资业务的数据还比较匮乏，价格还比较高。同时，为小微企业提供融资的金融机构人才比较匮乏，尤其是懂行业、懂小微企业需求的专才还比较少。另外，小微企业融资的科技系统还不够发达，行业里面专做小微企业客户管理、风控管理、业务支撑的科技公司还比较少。

刘嵩表示，接下来应利用人工智能技术开创新型金融服务模式。一方面，在金融作业过程中应用人工智能技术增效降本，满足小微企业金融需求；另一方面，在风险控制中应用人工智能技术迁移已有技术积累，可以提升风险识别能力。

在采访中，风控问题被业内人士认为仍然是制约小微企业融资的一大难题。

刘嵩坦言，我国小微企业地域分布广泛，企业类型多样，小微企业的经营方式、业务范围、盈利模式都有很大的差异，过大的差异会增加风险策略和指标需求匹配难度，对于数字化风控体系的自动化将是一个较大的挑战。

孙扬认为，在一些通用的领域，比如客服、客户关系管理、贷后管理等领域，金融科技在小微企业的应用是可以复制的。但是，在精准营销、风控模型等方面，还是要根据不同行业、不同地区进行差异化的安排。

“过往小微金融服务过程中需要业务人员上门尽调访谈，以人工审核的方式完成小微企业风险评估和信贷审批。而数字化风控则以算法模型为基础，依托全场景、全方位的互联网应用所沉淀的‘高维、高频、高可信’的行为数据构建客户画像，有效识别风险，大大降低小微企业融资的时间成本和融资难度。”刘嵩举例道，新网银行就是通过迁移学习对企业信用评估模型在风控指标和用户特征信息方面进行补全，风控要素实现从财务数据到颗粒度很细的行为数据，风控模型从基于财务数据的简单现金流模型拓展至高维变量决策模型，迁移学习技术进一步丰富了新网银行小微企业风险评价维度。

在尹振涛看来，金融机构应加强小微企业信贷风险管理和内控机制建设，提升小微企业贷款风险识别、预警、处置能力。同时，积极打造智能化贷后管理系统，通过大数据分析、多维度监测等手段，及时掌握可疑贷款主体、资金异常流动等企业风险点和信贷资产质量情况，有效识别管控业务风险。小微企业的智能贷后管理系统可以从客户登记信息、行政处罚信息、司法案件信息、纳税经营信息等方面以低成本、无触感、勿打扰的方式做好贷后管理工作。