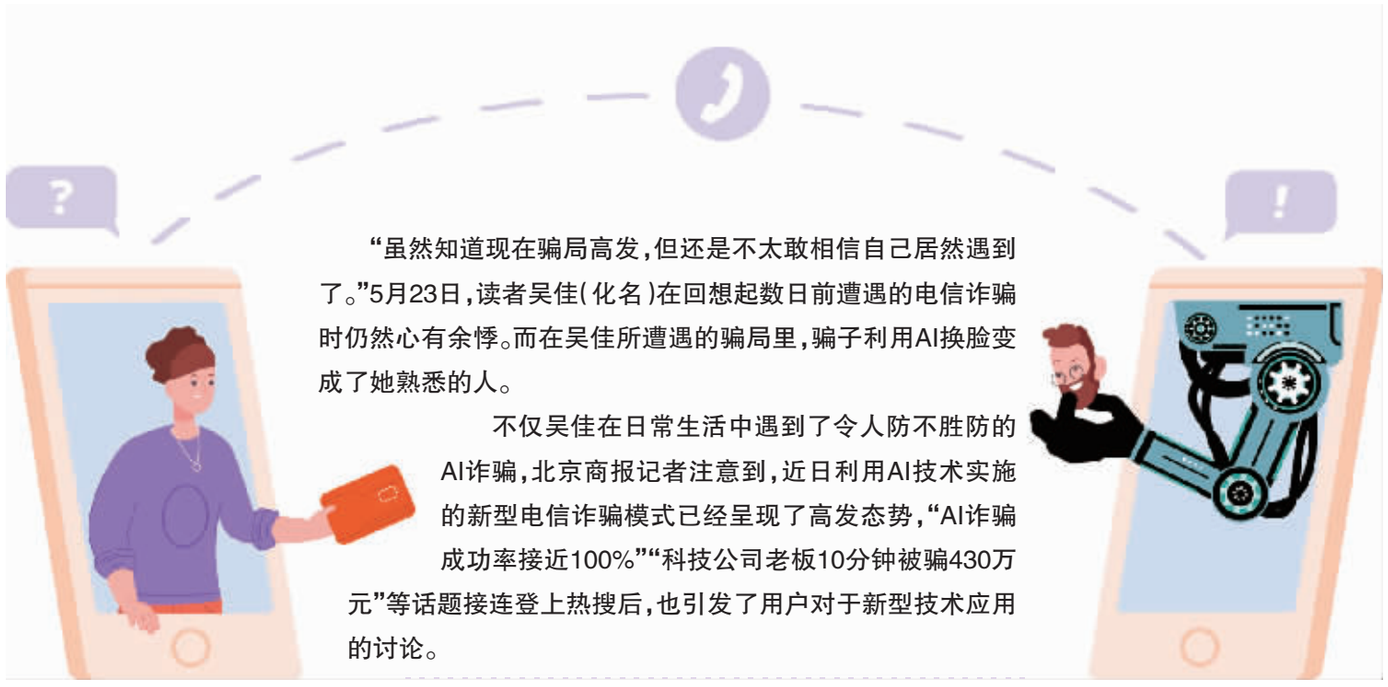
编辑 和岳 美编 白杨 责校 杨志强 电话:64101949 bbtzbs@163.com

当AI遇上诈骗



“虽然知道现在骗局高发,但还是不太敢相信自己居然遇到了。”5月23日,读者吴佳(化名)在回想起数日前遭遇的电信诈骗时仍然心有余悸。而在吴佳所遭遇的骗局里,骗子利用AI换脸变成了她熟悉的人。

不仅吴佳在日常生活中遇到了令人防不胜防的AI诈骗,北京商报记者注意到,近日利用AI技术实施的新型电信诈骗模式已经呈现了高发态势,“AI诈骗成功率接近100%”“科技公司老板10分钟被骗430万元”等话题接连登上热搜后,也引发了用户对于新型技术应用的讨论。

“AI换脸”搞诈骗

人工智能又火了,这次是围绕电信诈骗。吴佳告诉北京商报记者,此前自己久未使用的一社交账号突然收到了一位多年未联系的高中“好友”的问候,起初自己并未起疑心。但简单寒暄过后,对方提出了借款2000元应急的需求。尽管略感困惑,但基于过往亲厚关系,吴佳没有在第一时间内拒绝,而是提出要通过语音和视频进行核验身份。

“先是给我发了几句语音,听起来也很正常,也比较像她的声音。紧接着我拨通视频电话,她很快接通了,确实是她的脸。”吴佳表示。据吴佳回忆,由于频繁出现网络卡顿情况,视频电话接通后两人对话并不流畅,对方只推脱说网络不好,还提出“我的脸你都不认识了”等话术。

并没有详细解释需要借钱的原因,而是在确认“脸”后急于挂断电话,对方的反常举动引起了吴佳的警惕。随后,吴佳在电话中询问了对方两人共同的高中老师的姓氏,对方未正面回答,并重复提出“就是我本人”。在意识到可能遇到骗局后,吴佳挂断视频电话,并进一步使用其他渠道向该同学进行了求证,得到了借钱者并非本人的回复。

对于这起骗局,吴佳心有戚戚。吴佳称:“知道电信诈骗招数很多,但万万没想到视频验证的方式也可能行不通了。后来我提醒了一下家中的长辈,如果遇到同样的情况很容易被骗,于是再度跟他们强调不要随意通过网络渠道交易资金。”

综合吴佳反馈的信息来看,她遇到的正是近日受到广泛关注的AI诈骗。5月22日,“科技公司老板10分钟被骗430万元”“AI诈骗成功率接近100%”“AI诈骗在全国多地爆发”等话题接连登上热搜,也有不少警方发布了AI技术相关的电信诈骗案例。

温州市公安局反诈中心在5月22日发布的信息显示,“我想你应该不会亏待我,在你收到短信图片之后速与我联系”。温州市民陈先生收到一条来自“私家侦探”的勒索短信,并附上一张所谓的陈先生与一名女子的不雅视频截图,但相关视频却是AI合成而来。陈先生报警向警方求助,此案目前正在调查中。

无独有偶,平安包头官方微信号5月20日披露,包头市公安局电信网络犯罪侦查局日前侦破一起使用智能AI技术进行电信诈骗的案件,福州市某科技公司法人代表郭先生接到好友微信视频电话,在通过视频确认了好友面貌与声音后,郭先生在10分钟内将430万元转至对方账户。直至转款后再与好友联系,郭先生这才意识到被骗。最终在包头警方协助下将诈骗账户内的336.84万元被骗资金拦截,但仍有93.16万元被转移。

易观分析金融行业高级咨询顾问苏筱芮表示,伴随着AI技术应用的逐步成熟以及应用门槛的降低,通过AI以假乱真来实施诈骗成为了不法分子作案的新趋势。

个人隐私过度泄露

事实上,近年来打击电信诈骗工作已经成为监管方的一项重点工作,通过民警、银行、社区、媒体等线上线下多方渠道,对于各类电信诈骗手段进行详细的预警披露,但花样百出的电信诈骗仍然令人防不胜防。

不过,在多方警示之下,用户对于电信诈骗的警惕程度在不断提高。在本次关于AI诈骗话题的讨论中,也有不少用户提出了保护个人隐私信息、对于任何涉及到钱的事都不能掉以轻心等观点。

博通咨询首席分析师王蓬博同样认为,科技的进步让防范电信诈骗的难度在提升,但电信诈骗频出的原因还是在于信息时代用户个人隐私信息过度泄露。北京商报记者也向多位读者进行了解,一位曾经遭遇电商平台退货骗局的用户指出,骗子在电话中清晰地提供了自己的账户名、所购买的产品以及收货地址,最终造成了自己的大额损失。

回归AI诈骗这一新型模式,全面推进数字化的当下,各类平台收集个人信息成为常态。当诈骗遇上了AI,行骗成功率接近100%。苏筱芮指出,包括AI在内的新型技术,本身应该是中性的,在能够为生产、生活带来便利的同时,也需要警惕其中暗藏的各类风险。

对刷脸、刷掌支付影响几何

根据警方通报的内容,利用AI技术实施诈骗的方式主要包括声音合成、AI换脸,以及盗取微信号后,提取语音文件或安装非官方版本(插件),向微信好友转发此前的语音记录获取信任。还有一种方式,则是通过AI技术筛选受骗人群,在精细筛选后找到目标对象。

由此看来,与传统诈骗方式相比,AI诈骗还涉及到了人脸、声纹等生物信息。数字化时代,指纹、声纹、人脸甚至是虹膜等生物信息都成为能开启资金账户的“钥匙”,这也意味着,除了常规的验证码、身份证号信息外,当前用户要保护的隐私信息也逐渐包括个人生物信息。

另根据过往北京商报记者的实际调查情况,尤其是在金融领域,新技术与新事物的出现往往极易成为骗子利用的砝码,以此向不知情的用户实施诈骗。AI“换脸”诈骗的方式出炉后,也有不少用户对人脸识别等方式的安全性表达了担忧,提出骗子是否有可能通过AI技术盗用个人资金账户。

不仅如此,就在AI诈骗引起广泛讨论的同期,微信正式对外发布刷掌支付这一全新的支付方式。关于刷掌支付的讨论中,也有用户提到了掌纹信息采集和支付安全的问题。根据介绍,区别于指纹识别读取指腹的表皮纹路,掌纹识别读取的是掌心血管纹路。

新技术带来便利的同时,如何规避新技术带来的诈骗等问题,也成为机构方应该考虑的问题。谈及新技术在金融领域的应用,王蓬博指出,如果有机构要推行新技术,一定要在如何保护个人隐私、反诈骗和便于用户使用之间实现平衡,起码要提前预备好防范和应对机制。

“以刷掌支付为例,个人信息的规模化采集和应用实际上都缺乏法律支撑,如何避免信息被过度采集,如何避免个人专属的且应该是绝密的生物识别信息不被泄露,如何做好数据储存,要想调用必须经过何种方式确保个人信息安全……这些问题目前都没有很好的解释。”王蓬博直言,在个人隐私保护逐渐被广大用户接受的今天,新技术要想面向个人用户普及难度就比较高。

转账前交叉验证

对于消费者而言,更为重要的是,要守好自己的“钱袋子”。对此,王蓬博表示,消费者首先要提高警惕,涉及到转账的需要认真核实信息的真实性,及时通过正规渠道联系相关信源,进行交叉验证。

苏筱芮则指出,需要从三个层面进行看待:一是监管侧,需及时向社会公众发布风险提示和预警,在执法队伍中进一步强化科技人才引进,总结提炼新型电诈的新特征、新模式,通过树立一批大案、要案以震慑市场;二是平台侧,例如骗子常驻、常利用的购物平台、社交平台、支付平台等,需加强风控管理,合理采取拦截措施,在账户异常或者聊天内容异常时及时向用户发布提醒;三是用户侧,不轻信陌生来电和短信,在转账、付款前通过官方等渠道核实好对方的身份信息。

北京商报记者 廖蒙

收单机构“断臂求生”

合作机构数量众多、资质良莠不齐的收单外包市场再迎进一步整改规范。

5月22日,中国支付清算协会(以下简称“协会”)一纸《关于加强收单外包服务市场规范管理的意见》(以下简称《意见》)引发行业高度关注。而自查的第一个重要时间节点,定在了一个月后的6月底。把好准入、强化登记、推进备案、加强风险控制……显然,留给收单机构们自查整改的时间不多了。

有机构开启“断臂式整改”

接下来的一个月,“自查整改”将是大部分收单机构要重点推进的一个任务项。

正如中国支付清算协会发布的《意见》中强调,收单机构要把好外包机构准入标准,选择符合监管规定和自律规范要求的外包机构开展合作,不得采取“注册即合作”等不加审核的自助合作模式;合作外包机构不超过1000家的,收单机构应在2023年6月30日前将全量合作外包机构信息登记至协会系统。

且收单机构应通过监控检查等手段强化对外包机构推荐商户的风险管控,不得将商户资质审核、收单结算账户设置与变更等服务委托外包机构办理;不得支持外包机构代特约商户向收单机构发起提现或资金结算的交易指令。

自查整改时间也已敲定:2023年6月底前,外包机构完成自查整改,收单机构完成自查并制定整改方案。那么,最后通牒已下,机构准备如何?

北京商报记者5月23日采访了十余家收单机构,尽管部分对此三缄其口,但仍有半数机构告诉记者已在按照《意见》要求开启整改;有机构在谨慎选择外包服务机构,收紧了准入把控;甚至有机构称采取了更为彻底的自查,凡是涉及到虚假商户和违规操作的外包商,一律归入“一刀切”的剔除模式。

例如,包括支付宝、新国都、银盛支付等多家机构回复北京商报记者,将在人民银行及协会的指导下,积极、持续落实服务商的登记、备案及相关管理工作。

另外,一华南地区支付公司也表态,“已经在针对性地制定相应的奖惩制度,对检查发现的违规收单外包服务机构实行惩戒,规范化管理收单外包机构开展业务”。

一上市系收单机构也称,正在从事前准入、动态管理、企业内控三个主要方面构建和完善外包机构管理体系。首先对外包机构采用严格的准入限制,强化对合作机构的资质审核,同时建立多部门联动的全面审查机制,严格执行备案要求,加强对业务人员的培训与考核;其次对合作外包机构实行动态管理,按日监控服务商展业风险,按月落实服务商检查及续约工作,按季开展服务商业务评级,及时处罚及清退不合规的外包机构。

“公司确实已经在抓紧自查了,求稳是第一位,首先要保证能活下去,该清理的清理,该整改的整改。”一华东地区支付机构人员同样说道,该公司的工作方向是,确保商户信息的真实性,加强商户资质审核等。另外,他向北京商报记者透露,目前有收单机构通过外包服务商拓展的虚假商户占比高至90%,而经过这一自查整改,无疑是“断臂求生”。

外包服务管控难在哪

断臂,只为谋生,而这只是众多收单机构中的一个缩影。

线下收单市场中,支付机构和外包服务商一直被业内称为“利益共生体”。一方面,外包商卖力为支付机构推销产品,为后者业务发展“献力献策”;另一方面,也有外包商为追求利润剑走偏锋,让不少支付机构“连吃罚单”。

“不想再给‘监管罚单’打工了!”一收单机构资深人士戏谑道,所以整改势在必行。

但整改并非易事。首先要打破的一大难题就是,随着收单市场迅猛扩张,收单外包服务机构行业快速发展,由于一般情况下外包机构合作的模式相对简单,准入门槛较低,大量收单外包机构入局,导致一些收单外包机构服务质量参差不齐。

正如一支付公司从业人员透露,目前业内大部分收单机构都依靠外包公司展业,收单费率低成为了困扰部分企业盈利的重要因素,继而导致套码、虚假外包等现象愈发猖狂。然而,对于外包服务商的监管难度尤其大,有时其提交的信息很难验证真伪。在对外包公司高度依赖的背景下,庞大的数量为管理、查证增添了巨大难度。

“例如部分外包机构在商户回佣的刺激下不惜铤而走险,误入歧途,为套码套现等违规交易接入收单网络牵线搭桥,个别外包机构甚至为诈骗平台、网络赌博等黑灰产业提供便利,这一系列急功近利的行为,也将自己陷入到风险之中。”前述支付公司从业人员直言。

前述收单机构资深人士同样验证了这一情况,“确实会有部分外包机构涉嫌推荐虚假商户或违法违规商户,或为商户提供结算账户设置和修改服务甚至提现服务的情况”。

近年来,套码套现仍是盘踞在收单行业的一大痼疾。部分第三方支付机构利用不同类别商户手续费率不同,通过后台技术变造,从商户处以标准费率收取费用,在向清算机构报送时,则享受某些优惠费率以从中赚取差价。日前,拉卡拉、翠微股份相继自曝支付收单业务“跳码”问题,收单行业“合规风暴”再度升级。

对此,《意见》同样对外包服务机构提出要求,强调“业务真实合法,严禁从事套码套现等违法违规行为”;应“维护客户资金安全,不得向商户提供收单结算账户设置修改、向收单机构发起提现或资金结算的交易指令等涉及资金的服务,防范业务风险”。

在中南财经政法大学数字经济研究院高级研究员金天看来,这充分体现着对于此类违规行为监管力度的再一次加强。

金天表示,打击套码套现需要两方面共同发力,一是加大对商户资质的审核,二是加大对异常交易的识别和阻断。就前一方面来说,有赖于市场各方、特别是收单机构和外包机构的共同努力。相对而言,外包机构短期激励高、风控水平低,是最有动机也最有可能将不合规商户拓展进入的,因此打击套码套现需要首先要求外包机构做好自查整改、约束不合规的商户拓展行为。

《意见》披露,截至2023年3月,在协会完成备案并公示的外包机构已超过1.6万家。在如此庞大的数量背景下,对于收单外包的整改难度仍然不小,部分支付机构也“心有余而力不足”。王蓬博说道,“整改难点在于服务商掌握着大量的真实商户,从利润的角度来看,很多收单机构无法做到真正严格要求对方,所以会出现很多行业乱象”。

金天同样称,收单外包服务市场集中度不高,从业人员鱼龙混杂,在业务竞争中以免费、低费率等营销噱头引导商户、特别是不符合资质的商户入网,入网后不能满足前期承诺,以及诱导或纵容套码套现、涉黄赌毒等地下经济等“骚操作”层出不穷,对市场整顿带来了一定难度。

自查整改将更加常态化

《意见》中明确提出,2023年6月底前,各外包机构按照意见完成自查整改,并将自查整改报告发送全体合作收单机构;2023年6月底前,各收单机构应按照意见完成自查,制定整改方案确保按期落实意见要求,并形成自查整改报告存档备查。

仅剩一个月的时间,留给机构们自查的时间不多了。

基于长期存在的“盈利与安全”考量,收单外包乱象的整顿绝非一日之功。“收单外包服务整顿是行业合规的必经之路,在肃清乱象的同时,给予合规机构以更大的成长空间,也有助于收单机构进一步提升合规水平,减少因外包机构等影响而收到的监管罚单。”易观分析金融行业高级咨询顾问苏筱芮说道。

可以预见的是,在此次《意见》规范和整顿下,大部分收单机构也加速了自查动作,正如前述收单机构资深从业人员表态,在《意见》指导下,企业自查动作将更加彻底,以可持续为发展理念,坚持合规经营,将虚假商户剔除。“虽然可能会使业务量受到一定影响,但仍要在自身完全合规合法的前提之下开展业务,将安全阈值拉到100%。”

上述上市系收单机构同样提出,为构建收单行业健康生态,公司会积极推动行业自律与互助,一方面积极配合协会开展外包服务机构共享机制的搭建工作;另一方面,主动开展收单外包方从业人员实名制展业、素质考核,从收单基础知识、收单外包规范、行业监管、法律法规等方面进行考核,同时建立从业人员黑名单库,与收单机构及收单外包服务机构共享。

金天指出,“预计市场上各从业机构的自查整改将更加常态化,此外在收单机构加强内控管理和风险监测方面,也可能出现与数字化技术应用相关的新的市场机会”。

此次《意见》也提到,除了自查整改阶段,2023年7月也将开始自律检查阶段,检查工作结束后还将进入持续巩固阶段。协会将通过明确后续工作安排,引导收单机构和外包机构等市场主体的预期,压实《意见》的主体责任,促进有效落实。

北京商报记者 刘四红 实习记者 董晗萱