编辑 卓洋 美编 张彬 责校 池红云 电话:64101949 bbtzbs@163.com

“养虾”破财警示:银行风控面临AI新考验

一场全民“养龙虾”的AI狂欢热潮来袭。

近段时间,开源AI智能体OpenClaw(俗称“龙虾”)走红全网,以“解放双手”的便捷性吸引大量用户跟风部署,被网友亲切称为“养虾”。这款可自动完成文件处理、远程调试等功能的工具,背后却暗藏安全隐患,有用户因绑定信用卡信息、开放公网权限,遭遇信用卡盗刷,上演“养虾”变“失财”的尴尬一幕。

这一现象已为金融行业敲响警钟,3月12日,北京商报记者从多位银行信用卡中心人士处了解到,目前,部分银行已启动相关风险排查,暂未发现大规模盗刷案例,下一步将对相关案例进行研究,探索优化异常交易风控模型,提高对AI自动化操作、利用智能体安全漏洞盗刷等的识别和防范能力。

OpenClaw(龙虾)新型信用卡盗刷特点

1 利用工具高权限与普及性,远程无接触盗刷,隐蔽性强

2 小额高频、跨境虚拟消费,易绕过常规风控监测

3 AI代理模拟完整用户操作序列,传统风控规则模型难以区分

信用卡信息窃取与盗刷风险

OpenClaw的走红,源于“解放双手”的核心诉求与便捷高效的使用体验。

这款开源AI智能体,可通过整合多渠道通信能力与大语言模型,构建具备持久记忆、主动执行能力的定制化AI助手,能自动完成文件处理、脚本编写、远程调试等功能,吸引了大量用户跟风入场。

但热潮背后,隐藏着不容忽视的安全隐患,最直接的风险是信用卡信息窃取与盗刷。近日,一名开发者在社交平台分享称,他的朋友在使用AI代理工具OpenClaw编写程序时将浏览器通过VNC远程桌面开放至公网,几天后信用卡被连续盗刷。

有不少网友担忧,自己此前为了方便使用OpenClaw,已经绑定了信用卡、银行卡等支付信息,如今不知道如何彻底清除痕迹,担心信息持续泄露、遭遇盗刷;也有网友提到,原本以为“养虾”能提升效率、解放双手,没想到反而要承担财产损失的风险,直言“再也不敢跟风了”,不要为了一时便捷忽视安全。

博通咨询金融业资深分析师王蓬博指出,利用这类AI智能体实施的信用卡盗刷,更像是一种依托大众化AI工具形成的新型攻击方式。它更多是利用工具本身的高权限和普及性,来窃取支付信息并完成交易。和传统盗刷相比,这类风险可能呈现出几个比较明显的特点,比如攻击门槛更低、传播范围更广,远程操作、无接触盗刷的特征更突出,同时小额高频、跨境虚拟消费的模式,也更容易绕过一些常规风控监测,整体的隐蔽性和扩散风险相对更高一些。

在苏商银行特约研究员武泽伟看来,从安全角度看,这类AI工具被黑客利用进行信用卡盗刷属于一种新型的“智能代理滥用”攻击路径。核心在于攻击者不再直接攻击银行系统,而是通过提示注入等技术手段劫持合法的AI智能体,将其变为实施犯罪的代理工具。与传统盗刷相比,新特征体现在攻击的隐蔽性和自动化程度。黑客无需接触用户设备,而是利用AI代理在用户授权的高权限环境下,自动完成从卡片信息窃取到交易实施的全过程。

银行启动AI盗刷风险排查工作

虽然利用AI智能体实施的信用卡盗刷仍为个例,但也为金融行业敲响了警钟。

3月12日,多位银行信用卡中心人士在接受北京商报记者采访时直言,已经关注到此类新型盗刷风险,部分银行已启动AI盗刷风险排查工作。

“目前我行内部还没有部署使用OpenClaw这个AI工具,目前来看,银行业普及使用的概率不大。”一位国有大行信用卡中心相关人士提及,“排查发现我行目前也暂未出现因AI操作导致客户信用卡盗刷的事件。”

另一位股份制银行信用卡中心反欺诈部门人士也提到,“我行目前未出现利用AI智能体实施银行卡盗刷的案例,相关风险仍处于观察研究阶段,当前主流盗刷手段仍以木马病毒窃取信息为主”。

多位银行人士提到,此类智能体的技术迭代速度较快,潜在风险不容忽视。某银行风险管理部门人士坦言,此类新型盗刷行为可轻易规避银行原有基于金额、时间、交易地点等维度的规则化拦截机制,且因具备自动化、隐蔽化特征,系统难以有效识别机器操作行为。银行面临事前无法精准准入把关、事中难以实时监测预警、事后溯源追查难度大等突出问题。

正如武泽伟所言,目前银行信用卡风控体系主要基于预设的专家规则和机器学习的统计模型,通过对交易金额、频率、地理位置等结构化数据的实时分析来识别风险。然而面对AI智能体驱动的新型盗刷,现有体系存在显著的不适应性。在识别层面,由于AI代理的行为模式高度模仿人类操作,甚至能模拟完整的用户行为序列,导致传统基于单一特征点的规则模型难以将其与正常交易区分开。预警层面,传统模型多依赖事后标签进行训练,对AI攻击这种无历史样本的全新欺诈模式反应滞后,缺乏前瞻预判能力。在拦截层面,AI攻击的跨境、小额高频特征恰好能绕过许多基于额度和地域的基础风控规则,导致系统在交易发生时无法做出实时有效的阻断决策。

从四大维度升级信用卡风控体系

随着AI技术的快速普及,尤其是OpenClaw这类可实现自动化操作的AI智能体出现,信用卡盗刷场景迎来了新的变化,也对银行风控体系、权限管理与责任认定机制提出了更高要求。

上述国有大行信用卡中心相关人士进一步指出,“后续我行风控部门会对相关案例积极研究,探索优化异常交易风控模型,提高对AI自动化操作、利用智能体安全漏洞盗刷等的识别和防范能力”。

前述银行风险管理部门人士亦强调,针对此类新型盗刷风险,后续银行风控体系将实现迭代升级,不再局限于传统交易要素的单一监测,重点转向对操作行为是否为AI自动执行的深度识别。通过完善风险特征画像、构建智能化识别模型,加快推进具备实时拦截能力的风控系统建设。

素喜智研高级研究员苏筱芮表示,从安全角度看,这类AI工具被黑客利用进行信用卡盗刷,属于面向AI代理的自动金融欺诈,其攻击的本质,是不再直接攻击银行或用户设备,而是操控用户授权的高度自动化AI代理,利用其合法权限和行动能力,以符合业务逻辑的方式实施欺诈。与传统盗刷相比,被劫持的AI代理能模仿人类行为,自主决策并执行多步骤任务,具有较高的身份迷惑性。在此背景下,传统风控模型依赖的“异常行为”信号消失,攻击行为顺利融入正常流量,会使得金融机构的监测处于盲区。

银行的防御体系需要从“被动、静态、单点”向“主动、动态、全局”进化,在完善动态自适应的同时,推动多模型融合与大小模型协同。苏筱芮补充分析指出,从长期看,AI技术与金融安全的博弈将是一种常态,在风险与创新的不断迭代中共生共存,在这样的技术发展环境之下,一方面需以标准和责任划定红线,加快制定AI金融应用的国家标准和安全规范;另一方面行业也需从单点防御走向协同共治,推动建立金融行业风险信息的联防联控体系,打破数据孤岛,共同应对跨机构、跨区域的系统性风险。

“针对AI智能体引发的新型盗刷,银行应从规则、模型、数据和系统四个维度全面升级信用卡风控体系。”武泽伟建议,在规则与模型上,需引入具备因果推理能力的复杂模型,构建能够理解交易上下文和行为意图的智能决策引擎,以识别AI代理的自动化行为链。在数据层面,应打破数据孤岛,整合设备指纹、行为序列等非结构化数据,构建动态的客户风险全景画像。在系统层面,需建设具备实时监控和自适应学习能力的智能风控平台,实现对新型攻击模式的快速迭代响应。从长期看,平衡AI技术发展与金融安全底线的关键在于确立“可信人工智能”的治理框架,将安全设计内嵌于技术应用的整个生命周期,而非事后补救。这意味着金融机构既要积极拥抱AI提升效率,又要坚守审慎经营原则,通过建立行业级的风险情报共享机制和严格的算法审计标准,确保金融创新始终在安全可控的轨道上运行。

北京商报记者 宋亦桐

湖北消金转让4.39亿元不良资产

北京商报讯(记者 廖蒙)消费金融行业不良资产转让持续进行中。3月12日,北京商报记者注意到,3月11日湖北消费金融股份有限公司连续发布四期个人不良贷款(个人消费贷款)转让项目转让公告,规模共计4.39亿元。按照公告,相关不良资产将于3月25日进行线上公开竞价。

具体来看,湖北消金本次发布的转让公告,分别为2026年第3期、4期、5期、6期,对应不良资产的未偿本息总额分别为1.16亿元、9977万元、1.02亿元以及1.21亿元,其中未偿本金总额合计接近4亿元。逾期账龄方面,本次批量转让的不良贷款加权平均逾期天数最长为179.47天,最短为140.66天,资产类型均为个人消费贷款。

同时,相关不良资产均为未诉资产,即认定为不良资产后,湖北消金公司未对逾期借款人进行司法诉讼,便直接挂牌转让。

此前,2月6日,湖北消金发布了2026年第1期、2期不良贷款转让的相关公告,转让规模为1.48亿元,资产类型同样为个人消费贷款,且是未诉资产,加权平均逾期天数分别为145.37天、156.6天。由此计算,湖北消金年内已经挂牌的不良资产规模达到5.87亿元。

根据银登中心官网披露,2025年湖北消金累计23次对外转让个人消费贷款业务产生的不良资产。在2025年第1期贷款中,湖北消金所转让的不良贷款未偿本息总额为2.4亿元,起拍价低至694.7万元。总体来看,与2025年相比,湖北消金在2026年所转让的不良资产,逾期周期有所缩短,未诉资产的比重明显提升。

素喜智研高级研究员苏筱芮表示,湖北消金持续的不良资产转让行为,是近年来持牌消金公司加大不良资产处置的典型缩影,一方面可顺应监管导向,在“甩包袱”的同时加速业务风险出清;另一方面也可优化财务报表,将精力聚焦于更为核心的主营业务上。

对于不良资产在逾期周期、诉讼情况方面呈现的新特征,苏筱芮认为,这些变化主要是基于时间、费用等成本考量。相较而言,诉讼和清收是资产管理公司的专业领域,将不良资产包在早期阶段出给这些专业机构,能够助力持牌消金避免风险累积、降低管理成本,推动实现快速出表。但也可能会削弱消金公司自身对复杂逾期案件的自主催收、法务处置等能力。

“这个变化对贷后管理影响还是挺大的,会倒逼消费金融公司将重心往前移,更看重前端风控和贷中管理。”博通咨询首席分析师王蓬博补充道。

2022年末,持牌消费金融机构被纳入不良贷款转让试点机构范围,2025年底试点到期后,又获监管部门批准延期一年至2026年末。这一过程中,持牌消金公司逐步成为不良贷款批量转让市场的主力军,整体呈现“量多价低”的特征。

不仅仅是湖北消金,2026年以来,消费金融机构延续此前的处理方式,对不良贷款进行密集挂牌转让。据北京商报记者不完全统计,年内已有招联、中银、蚂蚁、小米等多家消费金融机构挂牌转让不良个人消费贷,规模超过120亿元。

苏筱芮指出,随着不良资产转让试点平稳延期至2026年底,持牌机构在稳定的政策预期之下,出包策略正转向更具计划性的常态化运营。关于资产质量,持牌消金需从源头切入,摒弃过度下沉的客群定位,转向聚焦特定优质群体,同时将金融服务深度嵌入真实、透明的消费场景,运用AI大模型、机器学习等技术,构建全流程智能风控体系以提升资产质量。

王蓬博指出,消金机构还是得从源头抓起,严格审核客户资质,将授信额度把控好,再加强贷中的风险监控,才能真正压降不良率。

聚焦 Focus

长护险将走向全面覆盖

北京商报讯(记者 李秀梅)作为应对人口老龄化的重要举措,长护险这一被称作社保“第六险”的制度,自2016年启动试点至今已走过十年历程,十年间,长护险制度从无到有、从试点到扩面,取得了阶段性成效,如今正从试点探索迈向全国建制的关键阶段。根据规划,“十五五”时期,国家医保局将加快推动具有中国特色的长护险制度从试点转向全面建立,逐步覆盖全民,并在制度建设上实现新突破。

今年作为“十五五”的开局之年,无疑是长护险制度全面建制的关键时期。“长期护理保险制度覆盖3亿人”“推行长期护理保险制度”,在今年的政府工作报告中,长护险两次被提及。该制度也是全国两会热议的焦点话题之一,多位人大代表、政协委员就发展长护险建言献策,比如建议建立完善的长护险制度,统一全国各省市长护险规范标准,尽快制定长期护理保险法,构建完善的长护险法律体系等。

在制度走向广覆盖、政策持续完善的背景下,市场参与主体的服务创新,正成为决定长护险能否“行稳致远”的关键一环。北京商报记者注意到,在这一重大民生工程的推进过程中,商业保险机构作为重要的经办服务力量和产品供给方,正持续探索服务能力升级路径。越来越多的保险机构开始参与长护险经办管理,承担基金核算、服务稽核、失能评估等核心职能。

苏商银行特约研究员付一夫告诉北京商报记者,保险机构参与长护险主要体现在四个维度:一是经办管理服务,包括基金核算、失能评估、服务稽核等具体工作;二是产品供给,开发商业长护险产品作为基本保障的补充;三是服务网络整合,利用自身资源对接护理机构、医疗资源等;四是数据与系统支持,协助政府进行信息化平台建设和运营管理。

除了政策性长护险,商业长护险在市场需求迸发、政策窗口红利显现的背景下,也将迎来广阔的发展前景。去年9月发布的《关于推动健康保险高质量发展的指导意见》提到,加快商业长护险与失能收入损失保险发展,支持商业长期护理保险为被保险人退休后提供满期保障。国务院印发的《关于促进服务消费高质量发展的意见》也提出,推动商业健康保险与健康管理深度融合,丰富商业长期护理保险供给。

在长护险扩面过程中,商业保险公司该如何抓住新机遇?付一夫表示,产品创新方面,开发差异化商业长护险,如针对特定人群、与健康管理服务结合的产品;服务整合方面,构建“评估—护理—康复”闭环,整合居家护理、社区照护、机构护理资源;生态构建方面,联合医疗、康复、养老机构打造服务网络,探索“保险+服务+科技”模式,例如通过智能设备监测预防失能风险,形成覆盖预防、补偿、支持的长期护理服务体系。