中国支付清算协会文件

中支协发〔2026〕128号

关于印发《智能体支付应用自律公约》的通知

各会员单位:

为推动人工智能技术在支付清算行业安全规范发展，防范技术应用安全风险，保障消费者合法权益，中国支付清算协会（以下简称协会）组织制定了《智能体支付应用自律公约》（见附件），并广泛征求了会员单位意见，经协会第五届常务理事会第二次会议审议通过，现予以发布实施。

附件：智能体支付应用自律公约

中国支付清算协会

2026年8月21日

附件

智能体支付应用自律公约

第一章 总 则

第一条 为落实《国务院关于深入实施“人工智能+”行动的意见》等要求，促进智能体支付应用安全、合规、可持续发展，有序推进人工智能与支付业务融合，保障会员单位合法权益及公众利益，防范技术应用安全风险，经中国支付清算协会会员单位协商，制定本公约。

第二条 本公约所称智能体支付应用是指会员单位利用大模型等人工智能技术，在用户授权的前提下，根据用户真实意思表示，使用智能体与电子商务等数字服务进行交互，发起和执行支付指令。智能体是指感知环境，并主动采取行动以实现特定目标的软件系统。

第三条 本公约适用于开展智能体支付应用的各会员单位，包括在智能体支付应用中提供账户管理、交易处理、收单、转接清算等服务的会员单位。

第二章 基本原则

第四条 会员单位开展智能体支付应用应严格遵循国家及金融行业的有关法律法规、技术规范，自觉遵守各项自律规范。严格落实网络安全、数据安全、个人隐私保护等规定，将依法合规

理念贯穿智能体支付应用全流程。

第五条 智能体支付应用涉及账户管理、交易处理、资金清结算等支付业务核心环节的，相关业务应由银行业金融机构、非银行支付机构、清算机构等持牌机构开展。会员单位应按照“谁提供支付服务谁负责”的原则，对用户的账户与交易安全、资金安全、信息安全等承担主体责任。

第六条 会员单位应以服务实体经济和便利人民生活为根本导向，聚焦用户真实需求，提升支付服务的可得性、便利性和普惠性，不得进行歧视性差别对待。

第七条 会员单位应确保相关技术应用始终服从于用户权益保护、金融安全稳定和增进社会福祉，防范技术滥用、算法歧视、过度诱导消费。应兼顾不同群体数字技术能力差异，保留必要的人工服务和替代性支付渠道，防范因技术应用加剧数字鸿沟。

第八条 会员单位应坚持开放合作，共同维护公平、开放、健康的智能体支付应用生态，不得通过排他合作、强制捆绑、低价补贴等方式限制用户选择，不得扰乱市场经营秩序。

第三章 智能体管理

第九条 会员单位应在“了解你的客户（KYC）”的基础上，探索建立“了解你的智能体（KYA）”机制，对接入支付链路的智能体身份进行识别、验证，对使用智能体支付应用服务的用户进行实名制管理，通过协议等形式明确智能体与用户的对应关系。

第十条 会员单位应探索按照高中低风险等级对接入支付链

路的智能体进行分级分类管理。重点关注智能体的模型来源、身份标识、权限边界、接口调用和行为特征，严防恶意智能体接入相关支付业务场景。

第十一条 会员单位应探索将智能体的身份、验证、分级、与用户的对应关系等相关信息在支付全链路上进行传递，强化智能体支付应用全生命周期安全管理。

第十二条 会员单位在开展智能体支付应用时，应使用经有关主管部门登记、备案的智能体。与外部智能体开发者、服务提供者等开展合作时，应常态化开展合作风险评估、尽职调查、监督管理，督促其严格落实相关法律法规及监管要求，通过合作协议明确安全管理要求及权责义务，切实守住安全底线。

第四章 授权管理

第十三条 会员单位应明确智能体支付应用的授权边界，与用户签订相关授权协议。应在授权协议中明确交易限额、扣款账户和优先级、有效期等关键内容，并约定用户授权智能体代其执行操作、访问数据、调用应用程序接口（API）等权利义务。

第十四条 会员单位应加强用户支付意愿核实，采用有效手段对用户身份、交易意愿进行严格核验。

第十五条 会员单位应按照用户授权执行支付指令，严防越权支付行为，保障支付交易的完整性、真实性、可追溯性。

第十六条 会员单位应保障用户撤销授权的权利，确保用户资金和信息安全。

第五章 安全管理

第十七条 会员单位应建立健全智能体支付应用的资金安全管理机制，通过交易限额等方式，切实防范智能体超额支取、越权划转用户资金的风险。

第十八条 会员单位应探索建立关键交易节点的可信存证机制，对用户授权、模型决策、支付指令、风险控制等关键过程形成可验证、可追溯、不可篡改的证据链，为交易争议处理、责任认定等提供证据校验。

第十九条 会员单位应按照“谁应用人工智能技术谁负责”的原则，将智能体算法和模型风险纳入全面风险管理体系，并在稳健性、透明性、可追溯性、输出可靠性等方面持续评估，防范模型黑箱、模型幻觉等风险，确保有智能体参与的支付交易可解释、可审计。

第二十条 会员单位应建立健全模型安全防护与风险监控机制，防范注入攻击、交易指令篡改、越权交互等风险，对可疑交易、指令执行异常等开展持续监测、预警与处置。

第二十一条 会员单位应坚持“用户授权、最小必要、全程防护”原则，在自身业务范围内充分评估潜在风险，严格遵守数据安全和隐私保护要求，防范在采集、传输、处理、存储、使用用户数据的过程中可能存在的数据过度采集、泄露、篡改、非法留存及滥用风险。

第二十二条 会员单位应遵循增进人类福祉、尊重生命权利、

坚持公平公正、合理控制风险、保持公开透明的科技伦理原则，将科技伦理要求贯穿智能体支付应用全过程，强化科技伦理风险防控，推动负责任的智能体技术应用，依法合规开展人工智能科技伦理审查。

第六章 风险管理

第二十三条 会员单位开展智能体支付应用，应按照所适用的法律法规及监管要求，制定与智能体支付应用相适配的反洗钱、反恐怖融资、反电信网络诈骗、打击赌博等内部管理机制，严格落实相关合规要求，严禁利用智能体开展非法支付活动。

第二十四条 会员单位应建立突发事件应急处理机制。一旦发生群体性纠纷等各类重大风险突发事件的，应及时启动突发事件应急处理预案，并配合监管部门、行业自律组织等开展情况摸排、风险研判与应急处置。

第二十五条 会员单位应根据智能体支付应用的功能属性和风险等级，建立分级分类的管理机制。对于跨智能体平台调用、大额交易等场景，应在充分评估、测试验证和持续监测基础上审慎开展。

第二十六条 会员单位应审慎探索开展智能体自主发起支付交易等智能体支付应用。在智能体自主支付等应用落地实施前，应向中国支付清算协会报备，会员单位切实承担保障用户资金安全等主体责任，并通过相关业务评估和安全测试，充分开展业务有效性、技术安全性、伦理符合性等方面评估验证，配套人工服

务、风险监控、舆情监测、应急处置、回退机制等保障措施，防范智能体支付应用风险。

第七章 消费者权益保护

第二十七条 会员单位应建立健全智能体支付应用的投诉受理机制，明确受理责任部门和责任人，向用户告知客服电话、在线客服等投诉受理渠道。会员单位应及时处理用户提出的差错争议和投诉，处理投诉应当遵循合法性、客观性等原则。

第二十八条 会员单位应为用户提供便捷的智能体支付应用关闭、信息查询的通道。应以清晰、可理解的方式向用户展示服务内容、授权规则、任务执行结果，切实保障用户的自主选择权。

第二十九条 会员单位应积极开展消费者教育，帮助用户理解智能体支付应用的业务功能、授权方式及潜在风险，提升消费者风险防范意识。

第三十条 会员单位应为老年人、未成年人等群体用户设置更加审慎的风险提示、权限控制和交易保护措施。根据老年人的实际需求，实时或定期主动推送智能体支付交易相关信息，在显著位置提供支付账单等相关信息一键查询、智能体支付应用一键关闭等功能。鼓励会员单位为老年人开通专属人工客服。

第八章 附 则

第三十一条 本公约与国家法律、法规和监管部门规章不一致的，依照有关法律、法规和监管部门规章执行。

第三十二条 中国支付清算协会在中国人民银行的指导下，组织对会员单位公约执行情况的监督。会员单位违反本公约的，任何单位和个人可向中国支付清算协会反映情况，并提供有效证明材料，中国支付清算协会将依规及时查证和处理。

第三十三条 本公约由中国支付清算协会负责解释和修订。

第三十四条 本公约自中国支付清算协会发布之日起实施。