

中国支付清算协会文件

中支协发〔2024〕155号

中国支付清算协会关于印发 《特约商户数字化辅助管理工作指南》的通知

各有关会员单位：

为进一步推动支付行业特约商户管理流程的数字化、标准化发展，引导会员单位稳妥利用数字化手段落实现行收单业务管理要求、开展特约商户真实性管理，根据《银行卡收单业务管理办法》《中国人民银行关于加强银行卡收单业务外包管理的通知》《中国人民银行关于加强支付受理终端及相关业务管理的通知》《金融科技发展规划（2022—2025年）》等相关政策文件，中国支付清算协会组织编制了《特约商户数字化辅助管理工作指南》（见附件），现予以发布，自发布之日起施行。

附件：特约商户数字化辅助管理工作指南

(此页无正文)



中国支付清算协会秘书处

2024年12月12日印发

附件

特约商户数字化辅助管理工作指南

第一章 总则

1.1 制定的目的及依据

为推动支付行业特约商户管理流程的数字化、标准化发展，引导会员单位综合运用大数据、人工智能、音视频、电子围栏等数字技术辅助开展特约商户管理，提高商户入网审核、巡检、风险监测、安全管理等方面工作质效，根据《银行卡收单业务管理办法》（中国人民银行公告〔2013〕第9号发布）、《中国人民银行关于加强银行卡收单业务外包管理的通知》（银发〔2015〕199号）、《中国人民银行关于进一步加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》（银发〔2019〕85号）、《中国人民银行关于加强支付受理终端及相关业务管理的通知》（银发〔2021〕259号）、《金融科技发展规划（2022—2025年）》（银发〔2021〕335号印发）、《中国人民银行办公厅关于开展深化金融科技应用推进金融数字化转型提升工程的通知》（银办发〔2022〕133号）等相关政策文件，制定本指南。

1.2 适用范围

本指南适用于从事支付清算业务的银行业金融机构、非银行支付机构等中国支付清算协会会员单位（以下统称“持

牌机构”) 开展特约商户管理活动。持牌机构在开展特约商户管理工作过程中，现行法律法规、部门规章或规范性文件有所规定的，相关管理措施不应因采用数字化技术方案而降低或替代。

其他相关业务的商户数字化辅助管理工作可参考本指南执行。

其他相关市场主体的特约商户数字化辅助管理工作参考本指南执行。

1.3 定义

特约商户数字化辅助管理，是指持牌机构在做好相关终端、系统、网络、数据等安全管理前提下，利用数字化手段对包括入网审核、巡检、风险监测等环节在内的特约商户管理全流程进行赋能优化及提质增效。

1.4 指导原则

守正创新。以服务实体经济为根本宗旨，坚守支付为民初心，不断提升支付服务整体质效，切实增强人民群众获得感、安全感和幸福感。

数字驱动。把握数字经济发展新趋势，发挥数据要素倍增作用，根据实际发展需要，稳妥运用数字化解决方案优化特约商户管理流程，提升特约商户管理服务及风险防控能力，加快支付业务数字化发展步伐。

依法合规。持牌机构要强化底线意识、责任意识，在利用数字化解决方案开展特约商户管理过程中严格遵守现行法律法规、部门规章和规范性文件等，切实承担起特约商户

收单业务管理责任，平衡好优化服务与风险防控。

安全可控。在特约商户数字化辅助管理过程中所使用的信息技术产品应符合国家及金融行业相关标准规范要求，具备保证其应用方数据支配权、产品控制权、产品选择权不受损害的属性。

第二章 特约商户入网

2.1 概述

在特约商户入网阶段（包括事前商户资料采集和处理、事中资料和资质审核、事后协议签订和终端布放及密钥管理等），持牌机构可综合运用人工智能、大数据、音视频等技术手段，辅助开展对特约商户身份信息的核实工作，确保所拓展的特约商户依法设立、从事合法经营活动。

2.2 商户识别和信息采集处理

2.2.1 资料采集

为更好遵循“了解你的客户”原则，丰富风控数据维度，提高特约商户管理的效率和准确性，持牌机构可在安全合规的前提下，在商户入网阶段采集以下信息：特约商户主体信息包括不限于基本信息、资质信息、结算账户信息、经营信息、场景信息等。其他公开信息（如有）包括不限于商户诉讼信息或违规经营信息、商户相关的工商行政处罚信息等。

持牌机构可通过客户端软件、小程序等数字渠道采集特约商户信息。在采集过程中，可使用光学字符识别（OCR）等技术识别提取营业执照、法人身份证等中的统一社会信用

代码、证件号码等信息，提高信息录入效率和准确性。持牌机构应做好客户端软件或小程序的用户和权限管理，加强用户身份识别和资质审查，严格设置与本地化经营相对应的录入权限，及时清理无效用户，防范业务违规转包、冒用或借用用户为虚假商户进件等风险。

持牌机构可通过开放应用程序接口（API）等技术对接金融管理部门指定的风险信息管理系统以及外部可信数据供应商，在安全合规的前提下，获取相关风险信息。

持牌机构可对所采集商户信息的完整性、准确性和合规性进行初步系统筛排，如商户经营地址信息与搜索引擎挂链比对结果是否一致、收单结算账户是否为同名账户等。

2.2.2 数据处理

持牌机构可通过图像识别、OCR、数字证书、电子签名等技术对非结构化进件信息进行数字化转换及电子化存证；运用大数据、机器学习等技术，对数据进行分析、处理和挖掘分析，按照监管部门的相关规范要求，进行数据规则的校验，提高数据质量，为商户入网审核和后续风险管理提供标准化数据支撑。

2.3 资料及资质审核

特约商户资料及资质审核主要包括风险信息核验、主体身份核验、商户真实意愿确认等方面。持牌机构应建立健全标准化的商户入网审核流程和制度，在确保入网资料审核准确性的同时，建立系统智能审核与人工审核互为补充的资料审核机制，不断提升审核能力。持牌机构拓展特约商户时，

应当通过中国支付清算协会或银行卡清算机构的特约商户信息管理系统查询其签约、更换收单机构情况和黑名单信息。可运用图像识别、OCR、机器人流程自动化（RPA）、自然语言处理（NLP）等手段打通审核流程断点，推动实现前端到后端业务流程触发、路径选择、任务派发与质量监控，提高入网审核业务处理标准化、智能化水平。

2.3.1 风险信息核验

对获取的大量文本和数据，持牌机构可通过NLP、机器学习、大数据等技术进行信息加工，可利用大语言模型有效提取与风险相关的关键字和短语，将风险信息与机构客户进行匹配，提高风险识别的精准度。

2.3.1.1 风险信息监测

持牌机构可运用自动化信息系统与人工分析相结合的方式对风险信息进行监测与识别，根据信息涉及风险高低进行分类，针对不同风险等级采用不同的管理策略；可持续将自主发现的高风险客户及其风险信息纳入自建数据库，并视情况与外部数据源进行交叉验证，为风险监测提供数据支撑。

2.3.1.2 风险预警识别

为快速完成初筛风险的进一步识别，持牌机构可借助人工智能技术实现智能审核，减少风险初筛环节的错误命中（False Hit）。可在模糊匹配的初筛基础上，使用机器学习技术叠加预警评分模型构建二层筛查（Secondary Screening）模型。通过模型对监测预警进行评分和排序，对于低级别的预警，可采用系统自动审核与人工抽查核验相

结合的方式处理；对于高级别的预警，由专岗从业人员结合模型计算结果及依据进行人工判断处理。

2.3.2 主体身份核验

可通过开放应用程序接口（API）等技术对接公安部门联网核查系统、工商信息系统等核验渠道，对客户身份证件和营业执照真实有效性、企业法人一致性进行自动核验；并可通过上行打款验证或调用商业银行、银行卡清算机构等渠道核验银行卡要素一致性，提升客户身份认证的准确性和时效性，确保客户提供的资料信息真实有效。

可利用系统对照片、视频等资料进行智能审核，核实相关人员在拓展特约商户时是否依规开展商户信息面核或远程同步视频核实，且比对商户登记信息的真实性。

2.3.3 商户真实意愿确认

持牌机构在安全合规的前提下，可通过以下方式校验商户真实意愿：综合利用远程音视频、图像识别、活体检测等技术，对商户法定代表人或负责人进行真实意愿确认；基于视频坐席对商户申请真实意愿进行校验确认，确保由申请人本人签署相关协议，实现“亲见申请人本人签名”；将采集的客户生物特征与身份证上的图片特征进行比对，确定申请入网的客户“实名同人”；对采集的客户生物特征进行检测，判断人脸图像是否来自于真人活体，防范纸质翻拍照、电子翻拍照以及视频翻拍等攻击，防范身份伪冒风险；由商户使用指定账户打款至收单机构，验证客户本人真实交易意愿及对账户有相应权限。特约商户收单结算账户为有合法资金管

理关系的非同名账户的，持牌机构可借助上述数字技术辅助核实非同名账户开户人的身份和意愿。

2.4 受理协议签订

持牌机构可通过数字证书、电子签名、电子印章等技术，对特约商户和收单机构之间签订的受理协议等有关合同文本进行加密、签名，保障电子合同的防篡改、抗抵赖，电子合同替代传统纸质文件流转，实现传统特约商户管理业务凭证的结构化数据转换以及电子化存证，确保特约商户业务管理资料存储的合法高效。

2.5 终端布放及密钥管理

持牌机构可应用安全芯片单元（SE），可信执行环境（TEE）、分布式协同认证等技术，在风险可控的环境下对智能支付受理终端在线密钥等敏感信息进行管理维护，实现智能支付受理终端的密钥分发、密钥更新、设备锁定等功能，提高支付安全水平，提升特约商户的服务体验和收单业务风险防控能力。针对智能 POS 终端商户，通过设置电子围栏管控措施，结合商户经营地址、经营模式、风险等级等合理限制电子围栏范围，确保智能 POS 终端在合理范围内使用、防范移机风险。

第三章 特约商户巡检

3.1 概述

持牌机构可探索运用大数据、地理定位（GIS）、图像识别、音视频、生物识别、数字证书、电子签名等技术手段，

在特约商户巡检管理过程中实现商户风险的智能监测、视频人工坐席实时巡检、巡检材料智能审核、商户与从业人员地理位置实时定位等，有效提升商户巡检管理全流程的标准化及业务质效。

3.2 商户分类分级管理

持牌机构可利用大数据、人工智能、地理位置定位等技术，结合商户日常交易情况建立特约商户巡检评级模型及标签体系，根据采集到的各类商户信息，结合商户类型、商户行业、地域位置或经营场景，针对不同商户类型采用不同测算方式计算商户的风险等级并进行动态调整。

针对不同业务类型的特约商户，持牌机构可在符合有关法律法规及政策文件要求的前提下，根据商户风险等级建立健全分层分级的巡检及管控机制，及时有效了解商户风险。可通过数字化技术手段，高效采集商户经营情况，通过机器智能审核与人工核验相结合的方式判断商户经营真实性，提高巡检的效率与准确性。针对风险等级较高的商户，提高巡检审核要求，人工提前介入审核处理，并提高巡检频率，定期轮询工商信息，对工商异常的商户重点核实。

3.3 巡检形式

3.3.1 概述

在符合有关法律法规及政策文件要求的前提下：

——对于实体特约商户，持牌机构可根据实际情况通过数字化技术手段辅助开展现场巡检和远程巡检，多渠道多维度核验商户经营状态，提升巡检准确性及风险识别效率。对

于有固定经营场所的实体特约商户，持牌机构应当每年独立开展至少一次面对面现场巡检。对于无固定经营场所的实体特约商户，原则上应当通过人工或智能客服同步视频等方式进行巡检。

——对于网络特约商户，持牌机构应当通过定期登录其经营网页查看经营内容、开展网络支付接口技术监测和大数据分析。可通过数据接口查询网站 ICP 最新备案情况，大数据模型分析网站实际经营场景等判断商户经营状态及情况，并保存电子记录。

3.3.2 现场巡检

持牌机构可运用图像识别、大数据等技术，对从业人员上传的门店照片、设备照片等进行审核与甄别，与工商、公安、人民银行等数据进行交叉校验，并从地理信息系统定位、图片质量、相似度、图片场景特征等维度判断门店照片真实性与业务符合性，对于符合规则阈值的预判通过，对于存在异常或可疑行为的由人工介入审核处理。

从业人员可通过手机终端使用近场通信（NFC）或 OCR 识别读取身份证件信息，并通过活体检测、生物识别、可信身份认证平台（CTID）等方式进行商户法人身份校验。

持牌机构可利用小程序采集巡检信息。相关巡检工作人员应在巡检现场录入信息，录入时应开启小程序定位功能，并确保巡检地址与商户登记地址的一致性。

3.3.3 远程巡检

持牌机构可通过工商等公信力机构预采集部分商户信息，按时向商户发送巡检提醒，辅助商户进行自助巡检材料提交。通过生物识别、图片上传地理位置与商户经营地理位置校验等手段确保资料提交时提交人和经营场所的真实性；通过 OCR、图像识别等技术，提取纸质材料中的文字和图像信息，提高商户巡检材料输入效率，并进行真实校验。

3.4 巡检手段

3.4.1 概述

持牌机构可利用 API 等技术对接权威机构数据，对商户的营业执照、企业法人信息、法定代表人信息、受益人信息、网站工信部 ICP 备案等资质进行校验。通过各种数字技术工具（如大数据、人工智能等）对商户的真实性、经营的合法性进行多维度交叉验证。

3.4.2 视频核验

持牌机构可运用智能物联网（AIoT）、实时音视频交互（RTC）、远程见证、数字存证等技术手段开展视频核验。持牌机构发起巡检指令，在完成商户信息校验后联系商户或现场从业人员接入远程视频坐席，由商户或现场从业人员配合开展视频巡检。后台人工坐席从业人员通过实时音视频连接商户或现场从业人员，实时了解现场经营场景、收单设备、巡检过程并留存巡检记录。

通过商户或现场从业人员与后台视频坐席从业人员配合开展视频巡检，可基于协同认证、音视频双录数字存证等提升特约商户风险防控能力和作业效率，确保对特约商户业

务办理（如巡检、设备交割）真实意愿的线上核验，在完成巡检后由商户进行电子签名，保障过程可追溯、抗抵赖。

3.4.3 图像比对

持牌机构可利用图像识别、机器学习、大数据等技术，对商户相关照片进行图片真实性、相似度、场景符合度等维度校验，并判断审核结果。对商户照片进行图像场景识别，对设备照片提取设备编号，通过模型比对分析，给出匹配率、差异率等数据，辅助从业人员快速完成商户巡检。

3.4.4 位置校验

持牌机构可利用可信定位技术，基于终端设备提供可信环境或多台设备协同认证后不可被篡改、伪造的位置数据。运用地理位置服务、电子围栏等技术手段，通过获取照片上传、人员签到的地理信息系统地标定位与商户地址的地理信息系统位置做比较，确保现场巡检时上传图像在商户门店附近。通过商户管理类移动客户端应用软件完成地址地理位置信息上报、门店照片上传、支付受理终端与收款条码地理位置检测等方式，确保商户经营及终端运行位置符合有关业务要求。

3.5 事后排查

持牌机构可利用数字技术手段对巡检时存在问题的商户展开进一步摸排，针对商户经营状况异常、门店照片存疑、地理信息系统定位误差较大、受理终端异常等情况，结合商户经营资质、交易模式分析、商家沟通等方式对商家进行全方位排查，根据排查情况要求商户实施针对性整改。

第四章 风险防控

4.1 概述

持牌机构可运用大数据技术，在获得授权的前提下，对商户基础信息、工商信息、历史交易行为等进行分析挖掘与处理，构建商户风险评估模型，多维度进行风险评估，提升商户入网审核的准确性。同时，按照设置规则对商户场地变化、欺诈风险等进行排查，提前发现潜在风险，辅助开展巡检管理、提前干预与风险处置等工作。综合运用机器学习、知识图谱、图计算、大模型等人工智能技术手段，对持牌机构获得的内外部数据进行特征学习和样本训练，完善风险评价指标内容及其权重，持续优化风控模型性能，提升风控精准度。

4.2 事前风险管理

4.2.1 基础数据

持牌机构建立健全支持多维度、多渠道、多模态信息整合的特约商户基础信息数据库，信息内容应符合相关法律法规及政策文件要求，包括但不限于统一社会信用代码、法定代表人身份证号码、营业执照图像、身份证图像、商户门头店内照、联系手机号、结算账户、实际经营地址、运营网址及申请设备等。建立健全企业级风险商户名单库和风险案件库，通过中国支付清算协会风险信息共享系统互通风险商户名单信息，禁止准入或及时清退黑名单商户。

4.2.2 风险评级

持牌机构可运用机器学习等人工智能技术，综合商户基本信息、业务特性、地域风险、行业（职业）等风险子项评分结果，结合历史交易、内部触发案例数、外部渠道预警、公检法协查情况及舆情等信息，开展商户初始及持续风险评级，增强风险特征刻画能力，提升风险分级管理精准度。

4.2.3 限额管理

持牌机构建立健全特约商户限额管理体系，结合商户类型、开通业务类型、商户风险评级等，及时进行商户单笔、日、月及年维度金额或次数的额度计算和动态调整，确保交易额与商户规模相匹配，有效防范交易额异常激增等风险。

4.3 事中风险防控

4.3.1 交易监测

持牌机构可采用机器学习、风险态势感知等技术，构建事中交易风险监控体系，根据用户信息、交易金额、交易时间、交易频次、资金源，商户区域、行业及商户类型等综合研判交易风险，对异常交易采取阻断、增强核验及人工辅助判断等管控措施。着重分析研判交易突增态势，异常增长交易行为模式，防范大规模风险事件发生。

4.3.2 行为监测

持牌机构可基于无监督机器学习的异常检测技术、知识图谱等能力构建商户行为模型，检测偏离正常模式商户行为，识别和预防异常登录行为操作，监测异常时间、位置或设备登录，以及频繁变更结算账户等操作。构建商户和设备关联

网络，及时跟踪并捕捉多度关联中的恶意设备，有效识别恶意 IP、设备及地理定位系统位置中的欺诈行为。

4.4 事后风险防控

4.4.1 风险处置

持牌机构可搭建智能化处置决策平台，按不同风险等级与场景执行阻断、挂起、预警、放行及人工批准等决策，可采取冻结商户、暂停交易、延迟结算、冻结风险资金及收款限额等风险组合措施。

4.4.2 可视化指标

持牌机构可构建核心风险指标体系，基于量化指标分析审视、反哺风险策略，借助指标表现复盘风险业务，定位原因与风险特征，适时调整风险监控策略参数，提升风险监控策略管理数字化水平。量化指标体系可包括规则模型策略、风险控制情况及风险态势感知等。

4.4.3 持续识别

持牌机构可定期通过权威信息接口核实商户基础及经营信息变化。对于信息有变更的商户，及时要求商户更新营业执照、法定代表人身份证明等材料，通过图像合成篡改识别、图像相似度比对等模型能力比对、审核图像内容与真实性。

4.4.4 关联反查

持牌机构可借助知识图谱模型，对已识别或已确认的风险交易或商户开展进一步分析研判，以点带面挖掘衍生风险或潜在风险关联方，并进行整体闭环处理。针对客户投诉内

容，可利用大模型开展投诉文本分析分类，提升基于投诉数据的风险信息捕获能力，辅助识别并挖掘风险商户，完成风险反查与风险闭环工作。

第五章 安全管理

5.1 概述

持牌机构应严格按照《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国消费者权益保护法》等国家法律法规及金融行业相关政策文件要求进行安全管理，采取安全管理措施保障用户的合法权益不受侵害。

5.2 终端安全

持牌机构应通过定期系统更新、设置强密码等方式确保支付受理终端设备安全，对支付受理终端进行严格的访问控制，禁止未授权人员访问或操作终端。定期对支付受理终端系统和应用进行安全扫描和漏洞检测，及时发现和修复可能存在的安全隐患，防范黑客入侵与恶意软件，保障交易安全。

5.3 系统安全（商户数字化辅助管理系统）

持牌机构应建立健全完善主机及系统安全基线，对主机及系统的安装、访问、操作、监控等环节加强安全管控，同时应根据信息系统建设与运行情况，不定期开展信息安全风险评估活动，发现潜在安全漏洞，并对漏洞修复与验证进行有效记录与管理。

5.4 通信安全

持牌机构应建立健全网络安全管理策略，对网络的建设、接入、传输、用户接入、各个网络安全域之间的防护、日常管理等方面加强安全管控。应建立重要信息与外界传输或交换的安全约束措施，对生产网络和办公网络中的各种数据交换活动进行管控与保密责任的宣贯。

5.5 数据安全

持牌机构应遵循“用户授权、最小够用、全程防护”原则，充分评估潜在风险，加强数据全生命周期安全管理，严防用户数据的泄露、篡改和滥用风险。数据采集时，通过隐私政策文件、个人信息授权书等方式明示用户数据采集和使用目的、方式以及范围，获取用户明确授权后方可采集。数据存储时，通过如数据泛化等技术将原始信息进行脱敏，并与关联性较高的敏感信息进行安全隔离、分散存储，严控访问权限，降低数据泄露风险。数据传输时，采用加密通道进行数据传输。数据使用时，可借助加密技术，在不归集、不共享原始数据前提下，仅向外提供脱敏后的计算结果。

5.6 个人金融信息保护

持牌机构应严格按照《个人金融信息保护技术规范》（JR/T 0171—2020）等金融行业相关标准规范等要求，对于在特约商户数字化辅助管理中采集使用的个人金融信息，在相关个人金融信息收集、传输、存储、使用、删除、销毁等生命周期各环节全面进行安全防护，切实保障个人金融信息安全，有效防范信息泄露风险。

5.7 人工智能算法安全

持牌机构在特约商户数字化辅助管理中使用人工智能算法的，可按照《人工智能算法金融应用评价规范》（JR/T 0221—2021）、《人工智能算法金融应用信息披露指南》（JR/T 0287—2023）等金融行业相关标准规范要求，从安全性、可解释性、精准性和性能等方面对在特约商户数字化辅助管理中使用的的人工智能算法进行评估管理，适时开展算法信息披露活动，增强人工智能算法的可解释性和透明度，切实维护客户合法权益。

5.8 业务连续性

持牌机构应持续提供业务连续性保障能力，建立符合业务连续性管理要求的备用资源，如备用业务和办公场所资源、备用信息系统运行场所资源、备用信息技术资源、备用人力资源等，以及电力、通讯、消防、安保等资源。同时制定应急预案，定期演练，确保在突发事件时能快速切换，保证业务持续运行不中断。

第六章 附则

6.1 强化组织保障

6.1.1 持牌机构应建立健全前、中、后台的风险管理联动机制，强化产品设计、商户准入、交易监测、审计监督、调查处置等环节的风险全生命周期管理。

6.1.2 持牌机构应加强统筹规划和组织保障，建立健全协同有力、务实高效的特约商户数字化辅助管理工作机制，强化业务、风险、合规、开发、运维等部门的一体化协作。

6.1.3 持牌机构应建立健全特约商户数字化辅助管理监督机制，定期对工作的开展情况进行监督检查，及时发现并督促解决遇到的困难和问题。

6.2 开展培训与沟通

6.2.1 持牌机构应组织开展对相关从业人员的数字化辅助管理工作培训，提高事前、事中、事后风险防范意识和水平。

6.2.2 持牌机构应组织开展针对特约商户数字化辅助管理流程中巡检管理、争议处理、隐私保护、洗钱及欺诈风险防控等方面的培训和风险教育，提高特约商户风险防范意识。

6.3 强化风险内控

6.3.1 持牌机构应建立健全特约商户数字化辅助管理的各项规章制度，包括风险评估、监测、预警、处置、内控等方面制度，确保风险防控有章可循。

6.3.2 持牌机构应严格践行安全发展观，遵守相关法律法规和政策规范要求，守牢业务合规红线，强化数据安全、算法安全和个人信息保护，推动创新与安全协同发展。

6.4 加强数字能力建设

6.4.1 持牌机构可探索建设支持结构化与非结构化的企业级大数据平台和多元数据资源目录管理辅助工具，加强数据治理，提炼特约商户数据资源的基础管理属性、业务属性和技术属性，编制企业级数据字典和数据资源目录，构建统一数据视图，为特约商户数字化辅助管理的数据处理、风

险监测、风险管控、融合应用等提供支撑。

6.5 本指南相关用语含义如下：

电子围栏，通过信息化手段，规范支付受理终端的使用范围、布放的虚拟地理边界。

态势感知（SA, Situational Awareness or Situation Awareness），是指对一定时间和空间内的环境元素进行感知，并对这些元素的含义进行理解，最终预测这些元素在未来的发展状态。

风险态势感知，是指将态势感知的相关理论和方法应用到风险管理领域中。风险态势感知可以使风险管理人员宏观把握整体安全状态，识别出当前存在的问题和异常活动，并作出相应的反馈或改进。通过对一段时间内的风险状况进行分析和预测，为管理决策提供有力支撑和参考。

6.6 本指南由中国支付清算协会负责解释。

6.7 本指南自发布之日起施行。