支付机构互联网支付业务风险防范指引

# 第一部分 总则

1.1 编写目的 为引导成员单位提高互联网支付业务风险防范意识，有效识别、防范互联网支付业务风险，保护成员单位及消费者的合法权益，促进互联网支付业务的健康发展，根据国家法律法规及相关规定，制定本指引。

1.2 适用范围 支付机构互联网支付业务经营活动中的风险识别、防范及处置,应遵循本指引。支付机构是指根据中国人民银行《非金融机构支付服务管理办法》规定，取得《支付业务许可证》，获准办理互联网支付业务的非金融机构。互联网支付业务是指客户通过计算机等设备，依托互联网发起支付指令，实现货币资金转移的行为。

1.3 基本要求 支付机构开展互联网支付业务活动时，应遵循平等竞争、诚实守信、安全可靠、风险可控的原则。

支付机构应建立与本机构支付业务规模、模式相适应的2 风险防范管理体系。在业务开展过程中，应根据风险状况不断完善防范措施，有效防范用户端与商户端风险。同时应依照有关法律、法规和监管部门规章、规范性文件的规定加强对资金和客户信息安全的管理，严格履行反洗钱、反恐怖融资义务，规范外包业务管理，实现行业内风险信息共享，确保有效识别、评估、监测、控制和处置互联网支付业务风险。

# 第二部分 风险管理体系

2.1 组织架构 支付机构应建立与本机构支付业务性质、规模和复杂程度相适应的风险管理组织架构，以有效识别、评估、监测、控制风险。风险管理组织架构至少应包括以下基本要素： a.董事会及其职责； b.高级管理层及其职责； c.风险管理部门及其职责； d.其它相关部门职责等。

2.1.1 董事会职责 董事会对本机构互联网支付业务风险的管理负最终责任，主要职责包括：

a.制定与本机构战略目标相一致且适用于本机构的风险管理战略和总体政策；

b.通过审批及检查高级管理层的风险管理职责、权限及报告制度，确保本机构风险管理决策体系的有效性，尽可能确保将本机构各项业务面临的风险控制在可以承受的范围内；

c.定期审阅高级管理层提交的风险报告，充分了解本机构风险管理的总体情况、高级管理层处理重大风险事件的有效性以及监控和评价日常风险管理的有效性；

d.确保高级管理层采取必要的措施有效地识别、评估、监测和控制风险；

e.批准内部审计部门提交的风险管理体系运行效果的审计报告，确保本机构风险管理体系接受内审部门的有效审查与监督；

f.制定适当的奖惩制度，有效推动本机构风险管理体系的建立完善。

g.风险管理其他重大事项。

未设董事会的支付机构由执行董事或高级管理层履行相关职责。

2.1.2 高级管理层职责 高级管理层负责执行董事会批准的风险管理战略及政策。主要职责包括： a.在风险的日常管理方面，对董事会负责； b.负责制定、定期审查和监督执行风险管理的政策、程序和操作规程，并定期向董事会提交风险总体情况的报告； 4 c.审阅风险管理职能部门提交的风险管理报告，充分了解机构风险管理的总体情况，重大风险事件处理机制及日常风险监控、评价的有效性； d.界定各部门风险管理职责及风险管理报告的路径、频率、内容，督促各部门切实履行风险管理职责，以确保风险管理体系的正常运行； e.为风险管理配备适当的资源，包括但不限于提供必要的经费、设置必要的岗位、配备合格的人员、开展风险管理培训等； f.及时对风险管理体系进行检查和修订，以便有效地应对因内部程序、产品、业务活动、信息技术系统、员工及外部事件和其他因素发生变化造成的风险损失事件。

高级管理人员，包括总经理、副总经理、财务负责人、技术负责人或实际履行上述职责的人员。

2.1.3 风险管理部门职责 支付机构应设立或指定专门部门负责风险管理体系的建立和实施，及风控措施的审批和执行。专职部门应直接对高级管理层负责并与其他部门保持相对独立，以保证风险管理的一致性和有效性。主要职责包括： a.具体指导和协调本机构的风险管理工作； b.拟定本机构风险管理制度、程序和操作规程，提交高级管理层审批； c.建立风险识别、评估、监测、控制方法及报告程序，并组5 织实施； d.建立跨部门联合工作机制，协调、解决风险管理工作中的重大问题，组织跨部门的应急联动机制和应急预案的演练工作； e.定期检查、分析相关部门风险管理情况，确保风险管理制度和措施得到有效落实； f.定期向高级管理层提交风险管理报告； g.为各相关部门提供风险管理培训，协助其履行风险管理职责、提高风险管理水平。

2.1.4 其他相关部门职责 风险管理相关部门包括：业务部门、信息科技部门、内审部门、合规部门、客服部门等。

上述部门根据职责分工对所负责的风险管理工作负直接责任。主要职责包括： a.执行风险管理的政策、程序和操作规程； b.依据本机构风险管理和内部控制的要求，制定本部门的业务制度、流程和应急预案，确保与风险管理总体政策的一致性； c.监测重点风险，定期向风险管理职能部门通报本部门风险管理的总体状况，并及时报告风险事件。

内审部门不直接负责或参与其他部门的风险管理，但应定期审计本机构的风险管理体系运作情况，监督检查风险管理政策的执行情况，对新出台的风险管理政策、程序和具体的操作规程进行独立评估，并向董事会和高级管理层报告风险管理体系运行效6 果的审计报告，跟踪、督导审计发现问题的整改工作。

2.2 风险管理制度与内部控制 支付机构应依据国家相关法律法规，按照审慎经营的原则，建立健全风险管理制度和内部控制机制。

2.2.1 风险管理制度 支付机构风险管理制度应满足全面性、有效性原则，包括但不限于以下方面： a.业务管理； b.用户管理； c.商户管理； d.资金安全管理； e.系统信息安全管理； f.反洗钱和反恐怖融资管理； g.风险事件及应急管理。

2.2.2 内部控制 2.2.2.1内部控制应当体现全面、审慎、有效、独立的原则，主要内容包括： a.内部控制应当贯穿本机构互联网支付业务全过程和全部操作环节，覆盖所有的部门和岗位，并由全体人员参与，所有决策或操作均应有案可查。

b.内部控制应以防范风险、审慎经营为出发点，本机构业务经营管理中应体现“内控优先”的要求。 7 c.内部控制应具有高度的权威性，任何人不得拥有不受内部控制约束的权力，内部控制存在的问题应能够得到及时反馈和纠正。 d.内部控制的监督、评价部门应当独立于内部控制的建设、执行部门，并有直接向董事会、监事会和高级管理层报告的渠道。 2.2.2.2支付机构内部控制应当包括以下要素： a.内部控制环境。

b.风险识别与评估。

c.内部控制措施。

d.信息交流与反馈。

e.监督评价与纠正。

2.3 风险管理方法 支付机构应按照风险的类型和特点采用有效的、具有针对性的方法对风险进行监测、分析、评估和处置，对风险事件进行分析、评估和报告。包括：制定有效的风险防范措施，监测关键风险指标，测试和审查内部控制有效性，开展风险评估，进行风险报告，聘请外部中介机构对风险管理体系进行审计和评价等。

支付机构应建立风险预警机制，以降低风险事件的发生频率；及时采取有效控制措施，减少风险事件损失；制定适当的程序报告风险状况和重大风险事件，重大风险事件应及时向董事会和高级管理层报告。 8 2.4 风险管理系统 支付机构应当建立完善风险管理系统，以有效识别、评估、监测、控制和报告风险。该系统应记录和存储与风险损失相关的数据和风险事件信息，支持风险防范和控制措施，监测关键风险指标，并可提供风险报告的有关内容。

具备条件的支付机构应建立实时监测系统，用以控制交易风险。

业务类型复杂、经营规模较大的支付机构，应建立功能更加全面的风险管理系统，针对各项业务的风险特点实施有效管理。

# 第三部分 用户风险及防范

3.1 用户注册审查

3.1.1 实名制要求 支付机构应根据审慎原则，实名开立用户支付账户，对用户身份信息的真实性负责，不得为用户开立匿名、假名支付账户。 支付机构应加强对用户支付账户的管理，为同一用户建立唯一的用户身份识别号，对该用户开立的所有支付账户进行关联、统一管理；对同一用户在同一支付机构开立多个支付账户的，应采取有效措施确保支付账户为同名账户且多个支付账户中登记的用户基本身份信息一致。

3.1.2 用户身份信息审核 支付机构在为用户开立账户时，根据账户开立主体不同，分9 为个人支付账户和单位支付账户。

个人用户申请开立支付账户时，支付机构应登记其姓名、性别、国籍、职业、住址、联系方式以及有效身份证件的种类、号码和有效期限等身份信息，并对用户姓名、性别、有效身份证件的种类和号码等基本身份信息的真实性进行有效审核。

个人用户存在以下情形的，支付机构应核对其有效身份证件，并留存有效身份证件的复印件或者影印件。

a.个人用户办理单笔收付金额人民币 1 万元以上或者外币等值 1000 美元以上支付业务的； b.个人用户全部账户30 天内资金双边收付金额累计人民币5 万元以上或外币等值 1 万美元以上的； c.个人用户全部账户资金余额连续 10 天超过人民币 5000 元或外币等值 1000 美元的； d.通过取得网上金融产品销售资质的支付机构买卖金融产品的； e.中国人民银行规定的其他情形。

单位用户申请开立支付账户时，支付机构应登记以下基本信息： a.单位名称、地址、经营范围、税务登记证号码、组织机构代码（按规定无须取得税务登记证或无法取得组织机构代码证的除外）； b.可证明该客户依法设立或者依法开展经营、社会活动的执10 照、证件或者文件的名称、号码和有效期限； c.法定代表人（负责人）和授权办理业务人员的姓名、有效身份证件的种类、号码和有效期限。

支付机构应核对单位及其法定代表人（负责人）和授权办理业务人员的有效身份证件信息，并留存其复印件或者影印件。

有效身份证件是指能够证明用户身份的相关证件。个人用户的有效身份证件，包括：居住在境内的中国公民，为居民身份证或者临时居民身份证；居住在境内的 16 周岁以下的中国公民，为户口簿；中国人民解放军军人，为军人身份证件或居民身份证；中国人民武装警察，为武装警察身份证件或居民身份证；香港、澳门居民，为港澳居民往来内地通行证；台湾居民，为台湾居民来往大陆通行证或者其他有效旅行证件；外国公民，为护照；政府有权机关出具的能够证明其真实身份的证明文件。

法人和其他组织用户的有效身份证件，是指政府有权机关颁发的能够证明其合法真实身份的证件或文件，包括但不限于营业执照、事业单位法人证书、税务登记证、组织机构代码证。个体工商户的有效身份证件，包括营业执照、经营者或授权经办人员的有效身份证件。

支付机构可通过与公安机关、工商机关及税务机关等机构的合作，对个人用户及单位用户基本身份信息的真实性进行有效审核。 11 3.1.3 用户申请资料保存 支付机构应加强对用户身份信息等资料的管理与保存，建立用户身份信息资料的分类、保管、查阅和销毁等管理制度，保证其妥善保管、有序存放、方便查阅，严防灭失、损毁和泄露。支付机构不得以任何形式对外提供用户身份信息等资料，法律法规另有规定或与用户另有约定的除外。

用户身份信息等资料，应当由支付机构按照归档要求，以纸质或电子方式妥善保存，保管期限自业务关系结束当年至少保存5 年。纸质资料应整理立卷，装订成册，编制会计档案保管清册，电子方式的资料应进行备份，按照系统信息安全管理相关制度的要求妥善保管。

对于司法部门正在调查的可疑交易或违法犯罪行为活动涉及用户身份信息等资料，且相关调查工作在前款规定的最低保存期届满时仍未结束的，支付机构应当将其保存至相关调查工作结束。

3.2 用户服务协议 3.2.1 服务协议基本内容 支付机构为用户开立支付账户的，应在用户申请开立支付账户时签订服务协议。协议内容包括但不限于： a.支付账户的开立、使用、挂失、止付和撤销的条件； b.身份验证和支付授权方式； c. 用户对支付机构核验其银行账户信息和身份信息真实性12 的授权； d.支付账户使用规则，以及违规使用的处置和责任； e.支付账户资金变动的通知方式； f.发现支付账户被盗用后的通知、处置方式和责任划分； g.用户身份信息和交易信息的保密责任； h.支付机构所提供的支付服务，包括具体的服务种类及产品功能等，及其支付服务的使用限制； i.交易风险提示，包括提示用户注意交易过程中可能存在的风险及风险发生后的相关处理措施； j.知识产权的保护，说明支付机构所享有的知识产权及相关侵权责任; k.业务争议解决方式及免责条款； l.双方的其他权利和义务。

3.2.2 风险防范内容 支付机构与用户签订服务协议时，应告知用户可能存在的风险及相关的注意事项。

协议的风险条款应包含但不限于以下内容： a.支付机构提供的各项支付服务中可能存在的风险，以及用户的注意事项； b.用户注册支付账户时可能存在的风险，如未及时更新身份资料可能引发的风险等，以及用户的注意事项； c.用户使用支付账户时，如账号登录、密码设置、交易操作13 等，可能存在的风险，以及用户的注意事项； d.用户停止使用支付账户时可能存在的风险，以及用户的注意事项； e.其他风险防范内容。

3.2.3 法律责任条款 支付机构与用户签订服务协议时，应明确与用户之间的权利与义务，并对各自承担的法律后果及法律责任进行约定。协议的法律责任条款应包含但不限于以下内容： a.注册支付账户时，双方所承担的权利义务与责任； b.使用支付账户服务时，双方所承担的权利义务与责任； c.暂停、拒绝或终止支付账户服务时，双方所承担的权利义务与责任； d.支付系统服务中断或故障时，双方所承担的权利义务与责任； e.用户使用支付账户及交易过程中产生风险损失时，双方所承担的权利义务与责任； f.用户隐私权的法律责任条款； g.支付机构知识产权的法律责任条款； h.其他法律责任条款。

3.2.4 协议变更告知 支付机构拟变更支付服务协议格式条款、收费项目、收费标准等主要内容的，应当在变更前 30 日告知用户，并提示需要变14 更的内容，未向用户履行告知义务的，变更后的条款对该用户不具有约束力。变更协议涉及新增收费项目、提高收费标准、降低优惠条件等不利于原客户权益内容的，未经原用户同意，仍应当按照原协议执行。

3.3 用户交易身份认证 3.3.1 基本要求 为保障用户身份信息及交易信息的安全，保证用户支付指令的完整性、一致性和不可抵赖性，支付机构应为支付账户提供安全可靠的身份验证和支付授权方式，并采取有效措施，在用户发出支付指令前，提示用户对支付指令的准确性进行确认。

3.3.2 技术手段 支付机构可通过密码、令牌、动态口令、安全证书、手机校验码等技术手段对用户交易身份进行认证，确保用户的交易指令由用户本人发出。

支付机构可根据用户使用的不同身份认证方式设置支付限额，以保护用户的资金安全。用户提交的身份认证信息经多次验证或在限定时间内仍未通过的，支付机构应暂停其部分或全部业务的处理，并以适当方式通知用户。

支付机构应持续更新交易身份认证技术手段，保证用户交易安全。 15 3.4 用户账户与交易监控 3.4.1 基本要求 支付机构应建立账户与交易监控系统，制定账户及交易安全监控、风险处置与报告制度，并指定专门部门、设置专职岗位或人员对用户账户及交易安全进行监控。

3.4.2 监控范围 支付机构应当对用户签约、登录、交易、付款、查询、退款以及涉及账户变动的全过程实施 7X24 小时监控，以及时发现账户盗用、欺诈交易等风险，保障用户资金及信息安全。

3.4.3 监控指标 为强化对账户及交易的监控效果，提升监控效率，支付机构应对以下指标实施重点监控： a.订单信息，包括交易双方名称或账号、商户编号、交易内容、交易金额、订单编号、交易日期和时间等； b.交易频率； c.交易额度及限额； d.商户交易集中度； e.其他。

3.4.4 异常交易识别、调查与处置 异常交易是指用户在办理互联网支付业务或支付机构在提供互联网支付服务过程中因自身或外来原因产生的非正常交易。异常交易包含但不限于以下情形： 16 a.用户利用互联网支付服务从事套现、诈骗、洗钱等违法犯罪活动而产生的非正常交易； b. 不法分子通过采取恶意程序、网络钓鱼等欺诈手段，盗用用户账户或银行卡而产生的非正常交易； c.因支付业务系统及设施遭到自然或人为因素破坏，支付机构无法准确、及时地传送业务信息，或因网络攻击、网络犯罪活动导致互联网支付服务异常而产生的非正常交易。

支付机构应在其网站上公布异常交易投诉渠道及调查处理流程，结合交易监控系统及投诉信息，对异常交易进行比对分析，并启动调查程序。

支付机构应根据异常交易调查结果，采取暂停或继续交易、账户恢复原状、限制账户使用、冻结账户操作等措施。同时，根据异常交易种类、数量、后果及影响范围依照相关规定向业务监管部门进行报告。异常交易调查结果符合可疑交易报告标准的，支付机构应按相关要求向中国反洗钱监测分析中心履行报告义务。

支付机构应建立用户黑名单数据库，依据异常交易监测和调查结果，将确认存在违法或严重违规行为的用户列入该名单，并终止继续向其提供互联网支付服务。

3.5 用户账户及交易信息安全 3.5.1 用户信息安全管理 支付机构应设立或指定专门部门负责用户信息保护工作，并17 与所有接触用户账户信息及交易数据等敏感信息的员工签署保密协议，明确员工需要承担的保密责任以及员工离职时的脱密期。

支付机构应严格控制员工对用户账户信息及交易数据等敏感信息的访问权限，访问权限的分配应遵循分级授权的原则，访问记录应当留存备查，避免单个员工对用户账户信息及交易数据等敏感信息的完全控制。

未经用户授权，支付机构不得为任何单位或个人查询用户身份信息及交易信息资料，不得将用户身份信息及交易信息向任何第三方提供，法律法规另有规定的除外。

3.5.2 信息变更管理 支付机构应制定用户信息变更操作制度及流程，用户申请变更身份信息的，支付机构应在核实用户身份后予以更新。在用户业务关系存续期内，支付机构应当及时提示用户更新身份信息。 对于有效身份证件将超过有效期的用户，支付机构应当在失效前 60 天通知其及时更新，并予以有效核验。单位用户应按相关规定留存其有效身份证件的复印件或者影印件；个人用户存在3.1.2有关要求情形的，应留存其有效身份证件的复印件或者影印件。

对于有效身份证件已过有效期的用户，支付机构为其办理首笔业务时，应要求重新提供有效身份证件信息，并予以有效核验。单位用户应按相关规定留存其有效身份证件的复印件或者影印18 件；个人用户存在 3.1.2有关要求情形的，应留存其有效身份证件的复印件或者影印件。

3.5.3 账户挂失管理 支付机构应当制定并公布用户账户挂失操作制度及流程，用户因密码丢失或遗忘申请账户挂失的，支付机构应首先引导其通过自助或人工方式找回密码；用户因账户盗用等异常情况申请账户挂失的，支付机构应根据用户申请，在核实用户身份后对挂失账户进行限制账户使用、冻结账户操作等处理。

3.6 用户安全教育服务 3.6.1 用户安全提示 支付机构对用户的安全提示应覆盖其使用互联网支付产品完成支付活动的全过程和所有环节，提示用户注意账户、银行卡使用及个人信息安全，并提供相应的安全防范措施。

支付机构还应当以适当的方式，包括但不限于公告、邮件、短信、站内信等向用户提示当前主要支付安全风险。

3.6.2 日常安全教育 支付机构应当建立用户日常安全教育制度及流程，设立专门客服渠道解答用户安全问题，在网站页面应当设置安全教育板块。

支付机构在设计相关产品时应包含对用户进行安全提示或安全教育的内容，培育用户良好的支付安全习惯。

支付机构可定期或不定期开展互联网支付安全宣传培训活19 动，对用户进行安全教育。

3.7 业务投诉、差错及争议管理 支付机构应当建立业务争议、投诉处理机制，在网站公布争议受理渠道及流程，成立或指定经专业培训的争议、投诉处理部门，设置专岗，提供至少 5x8小时的服务。支付机构应在 5个工作日内处理相关争议或投诉，并及时将处理结果告知用户。

# 第四部分 商户风险及防范

4.1 商户拓展 4.1.1 禁止发展的商户 a.非法设立的经营组织； b.特殊行业商户，包括本国法律禁止的赌博及博彩类、色情服务类、出售违禁药品、毒品、黄色出版物、军火弹药等以及其他与本国法律、法规相抵触的商户； c. 以返利为名招徕客户实现传销或非法集资目的的商户或经营组织。

4.1.2 谨慎发展的商户 a.虚拟商品销售（包括充值卡、游戏点卡）等易发生套现、伪冒交易的商户； b.提供中介咨询服务类商户； c.接受用户预付款的商户； d.以个人账户作为结算账户、注册资本低或成立时间短、无20 实体店面的商户； e.注册地或经营场所在境外的商户； f. 代购类商户； g. 从事民间融资、贷款等类型业务的商户; h. 商户或其法定代表人、负责人已被列入中国人民银行指定的不良信息系统的商户。

4.2 商户资质审核 4.2.1 基本要求 支付机构应对商户的基本信息、资信记录、经营状况等进行全面审核与调查，以核实商户基本信息的真实性，并判断其是否满足商户准入的基本条件。

商户资质审核应由专人负责，不得与商户拓展等岗位兼岗，审核渠道包括但不限于电话调查、现场调查和间接调查等。

4.2.2 审核内容 支付机构与商户签约前，为防范风险可对以下内容进行审核： a.营业执照、税务登记证、组织机构代码证，法人代表或商户负责人身份证等； b.商户网站域名是否可以正常访问，网站信息是否定时更新； c.是否取得 ICP证或有 ICP备案； d.系统数据安全和人员配置是否有保障，业务制度体系是否21 完备； e.商户提供的商品及服务内容是否合法合规； f.服务条款、客户隐私声明、安全管理声明是否完整,有关退货、退款、送货和交易取消政策是否齐全; g.客户服务体系是否健全； h.网站内容。

对平台类商户应增加以下审核内容： a.二级商户实名制落实情况； b.平台类商户的信用评价体系和风险控制措施； c.平台类商户对二级商户交易信息上送和保管能力。

4.2.3 风险评级与分类管理 支付机构在审核商户基本情况的基础上，应对其进行风险等级划分。通过对商户的信用风险、欺诈风险和合规风险等各项基本要素进行评分，形成反映商户整体风险水平的评价分值，作为与商户签约的决策依据，并根据分值不同对商户采取差异化的风险管理措施。对风险等级较高的商户，应采取的交易风险管理措施包括但不限于：：设置商户单笔或当日交易限额、交易监测、物流审查、现场检查、缴存风险准备金、延迟清算等。

商户签约后，支付机构应结合商户的日常交易行为和风险管理状况，动态调整商户风险等级和相关管理措施。

4.2.4 未通过审批商户的记录 对于未能通过审批的商户，支付机构应建立内部的登记留存22 制度，对商户基本信息和拒绝原因进行详细记录，并及时进行更新汇总，为后续新商户的审批查询提供参考，防止不良商户多次提交欺诈申请。

4.2.5 申请资料保存管理 支付机构应妥善保存下列资料的影印件或扫描件备查： a.商户营业执照 b.税务登记证 c.组织机构代码证 d.法定代表人或商户负责人有效身份证件 e.商户 ICP证 f.商户信息调查表 g.商户受理协议书 h.对商户日常风险管理的相关表格，如商户日常检查表、《特约商户风险管理自查问卷》等。

支付机构与商户解约时，从协议终止日起，商户相关资料至少应保存五年以上。

4.3 服务协议 4.3.1 基本要求 支付机构应与商户签订标准的受理协议书，明确双方权利与义务。

4.3.2 风险防范条款 支付机构在与商户签订的协议文本中，应明确包含以下风险23 条款： 禁止性规定： a.商户不得将相关网关接口、标识等用于受理协议许可范围以外的用途，也不得供受理协议许可范围以外的第三方进行交易的使用。对于违反该条款的，支付机构保留向商户追索损失及要求额外罚款的权利。

b. 未经支付机构书面允许，商户不得将受理业务委托或转让给第三方。

经营义务： a.商户应对所提供资料的真实性负责，保证其经营活动和范围的合法性； b.信息资料、业务状况或商户基本情况发生变更时，商户应及时通知支付机构： i.信息资料变更包括：商户注册信息、服务器及网站地址（URL 及 IP）、网站名称、联系方式、开户银行及收款账户等发生变更； ii. 业务状况变更包括：经营变化（如中断或终止）、商品和服务以及提供方式（如主营业务范围，送、退货方式）等发生变更； iii.商户基本情况变更包括：商户资本及所有权变更（如注册资本的增减、重大的债务变化）。

c. 商户需确保有关商品和服务描述完整，有关退货、退款、24 送货和交易取消政策齐全，有关客户服务体系健全。

d. 商户要妥善、及时处理互联网支付业务产生的差错和争议，维护消费者合法权益。

e.商户应加强对相关网站、支付设备及软件的日常维护和管理，保证系统的安全稳定性，并遵守国家有关互联网支付安全的法律法规规定，确保交易以及账户信息的安全，否则支付机构有权限定商户的支付金额或中止合作，并要求商户承担相应的违约责任。

f.商户存在篡改交易数据、未按要求上送交易验证信息、为洗钱、套现提供便利等违规操作，应承担相应责任。

g.在发生欺诈交易后，商户应履行配合相关机构进行风险事件协查的义务，包括但不限于提供商户或二级商户签约时留存的基本信息、支付交易信息、客户信用记录、持卡人基本信息等。 h.平台类商户应配备相应的系统、人员和完善的制度，对其二级商户的交易实施有效识别、追溯及在必要时暂停业务的管理。同时，须承担因二级商户发展和管理不善造成的风险损失，下设的二级商户不得再发展下一级商户。

i.交易订单保存条款。商户应对交易订单保存至少 1年。因保存不当或遗失订单而造成的经济损失由商户承担。

保密条款： a.商户不得存储除基本的交易信息以外的其它数据（如网上支付密码、卡片有效期、CVN2等）。 25 b. 除了交易需要或法律要求，商户不得将账户及交易数据信息披露给第三方。

c. 商户必须将包含账户及交易数据信息的所有载体保存在安全区域，并确保只有被授权人员才能接触；包含账户及交易数据信息的所有载体在失效后应立即销毁，不得留存。

d. 业务处理流程应当确保信息安全。

风险控制措施条款： a.经风险状况评估确认为高风险商户的，支付机构有权调整商户交易款结算时限和方式。若商户违反协议，或从事欺诈交易的，支付机构可延迟对商户款项的结算。

b.根据商户风险属性或风险评级，支付机构可要求商户缴纳一定额度的保证金，用于对商户违约造成的损失进行赔付。

c.因商户违规操作、出现风险事件、违反协议规定等情况，支付机构可立即终止商户服务协议。

d.调查商户疑似欺诈交易期间，支付机构可暂时扣留有关交易的结算资金，并须及时告知商户。

e.商户出现以下情况且经通知、协商未做出改进的，支付机构有权终止对该商户的服务： i.在正式运行 3个月内无交易； ii. 因商品质量、配送问题而遭客户多次投诉； iii.商户因经营不善，已破产或停业的； iv. 被监管机构和司法机关认定为需要关闭的； 26 v. 违反保密义务的； vi. 有其他严重影响双方合作行为的。

其他条款： a.商户风险信息使用条款。在正常业务范围内，商户同意支付机构使用其风险信息（包含但不限于商户基本信息、商户经营及其风险情况等）。

b.交易查询及追索规定。协议终止后，支付机构对协议终止前的交易仍有查询及追索权。

c.支付机构的债权保证。在商户宣布破产时，应保证支付机构的债权人地位。

4.4 商户日常管理与监控 4.4.1 商户日常风险教育 支付机构与商户建立业务关系前，应对商户进行至少一次包括风险防范要求及技能的培训。业务存续期间内，支付机构应根据业务发展和风险控制需要，对商户进行定期或不定期的培训，可采用现场或远程方式，原则上一年内不得少于一次，并保留培训记录，以备查核。

4.4.2 商户风险检查与管理 支付机构应根据业务发展和风险控制的需要，定期对商户风险情况进行检查，并保留回访和培训的记录。检查的方式可以采用商户自查、支付机构检查以及委托专门机构代查相结合的方式，检查内容包括业务检查及技术安全检查。 27 发现异常或违规情况，应要求商户及时整改并提出有效的风险防范措施，必要时按照相关规定及时中止与商户的协议。

支付机构应采取必要的技术手段保证商户账户资金安全，具体手段包括但不限于：Usbkey、Token、数字证书、手机短信验证码等。

支付机构应以电话或网络方式为商户提供业务及风险咨询服务，并明确告知商户。

4.4.3 日常交易监控 支付机构应建立对互联网支付业务的交易监控机制，配备专门人员，对商户日常交易进行监控，并对可疑交易进行调查处理。依托风险管理系统，运用信息化手段来加强商户的风险监控和管理。

支付机构应根据自身风险策略，在风险管理系统中对互联网支付业务设置相应的商户风险监控指标。支付机构可根据商户的风险等级，建立动态的商户交易限额控制机制，细化针对不同类型商户的交易限额标准。

4.4.4 交易信息上送及保管 支付机构应要求商户上送完整的交易信息，确保支付机构保存详细的交易记录数据，应包括如下信息： a.交易发起方 IP地址； b.商品或服务内容描述 、物流配送信息； c. 二级商户名称、商户服务类别码等。 28 支付机构应对上送交易数据至少保存五年，以便追溯。

4.4.5 商户调查与处置 日常交易监控与商户检查中，发现商户存在违规迹象时,支付机构应立即进行调查。调查疑似套现等商户欺诈时，应综合采取如下措施进行处理，以及时发现风险，阻止商户欺诈行为，避免更大损失： a.向商户索取单据及相关凭证； b. 向银行等有关机构证实交易； c. 暂时扣留结算资金； d. 前往商户实施现场调查； e. 对有嫌疑商户实施后续监控和调查。

当确认商户存在违法、违规、欺诈行为且情节严重，或对商户采取警告、整改、暂停交易等处罚措施无效的，应立即终止商户协议、及时清退,并于协议终止后十个工作日内，将商户信息录入人民银行指定的不良信息系统。

支付机构应积极协助公安司法机关、相关主管单位及合作银行对商户违规违法事件进行调查，配合采取相应措施。

4.5 商户风险类型及防范 4.5.1 信息泄露 4.5.1.1 风险描述 商户违反保密条款，违规保存或将交易中采集的银行账户信息、支付账户信息和交易数据等信息，泄露给无关第三方，被泄29 露的信息具体包括: 银行账户信息：涉及银行卡号、有效期、CVN2、 与支付相关的各类密码等；涉及持卡人姓名、身份证号、联系方式、其他证件号码等身份信息； 支付账户信息：涉及支付账户用户、密码和联系方式等； 交易数据信息：涉及交易金额、交易商品等。

4.5.1.2 防范手段 在合作协议中明确支付机构与商户的责任与义务。要求商户遵循本指引的信息安全管理要求，切实了解商户对于信息泄露等风险的防范措施，加强对商户相关人员的风险培训与日常管理。 采用各类安全支付手段，防止信息泄露，提升支付的安全性。 4.5.2 套现 4.5.2.1 风险描述 商户与消费者或其他第三方勾结，或商户自身开立买卖双方的账户，进行无商品交付的虚假交易以此套取现金的行为。

4.5.2.2 防范手段 严格执行实名审核制度，充分利用联网核查身份信息系统、公安部户籍查询系统，并多方了解特约商户的经营背景、营业场所、经营范围、财务状况等信息。

在商户入网协议中明确商户有防范套现风险的义务，一旦发生套现行为，应采取暂停该商户交易或关闭商户等措施，并由商户承担可能出现的损失；在商户协议中，明确规范退货渠道，不30 得进行现金退货或采用预付费卡等易引发套现的形式退返现金；将疑似有套现嫌疑的商户负责人信息、营业执照等相关证件信息加入黑名单或灰名单，作为入网审核时的参考依据。

按照商户服务类型制定单笔、当日累计交易限额，并根据互联网欺诈形势对限额进行动态调整。

建立商户交易监控机制，针对套现商户交易特征制定相应的侦测规则。

4.5.3 恶意倒闭 4.5.3.1 风险描述 以欺诈为目的，发生商户负责人卷款潜逃、商户倒闭等风险事件，引发缴纳预付款的用户投诉，给支付机构带来退款损失的情形。

4.5.3.2防范手段 为商户提供互联网支付服务前应首先查询人民银行指定的不良信息系统，防止恶意倒闭商户在被某一支付机构发现后转移重复申请；对易发生恶意倒闭商户要求其缴纳风险保证金，并采取延迟结算的措施。加强交易监控，及时发现有恶意倒闭嫌疑的商户，并采取风险控制措施。

4.5.4 非法页面信息 4.5.4.1 风险描述 商户在其网站页面发布或登载诸如提供套现、赌博服务等信息招徕客户，通过互联网从事违法违规交易，给支付机构带来损31 失。

4.5.4.2 防范手段 支付机构应加强对签约商户的日常检查，运用“网络爬虫”等相关技术，对商户的网站内容进行扫描，扫描频率不得低于每周一次。在扫描中通过对敏感字段的过滤，筛查出发布违规信息的商户，并根据商户日常管理要求进行调查处置，对存在违规经营的商户应根据情节轻重采取口头警告、暂时关闭、录入黑名单、清退等手段进行处置。

对平台类商户，应要求其对下辖二级商户采取同样的风险管控措施，要求其将所辖商户页面内容定期进行检查，并向支付机构反馈检查结果。

4.5.5 网络钓鱼 4.5.5.1 风险描述 网络钓鱼指不法分子利用公共网络环境的漏洞，通过伪造交易链接将客户引导到虚假的支付页面；或向客户支付交易终端植入木马病毒等恶意程序，诱使客户将交易订单款项支付至指定账户或盗用其账户资金。

4.5.5.2 防范手段 加强对互联网支付用户安全意识的教育，提示常用的欺诈手段，并在交易过程中提示客户注意不明链接及文件的接收，如发现异常情况应及时与银行或支付机构联系；要求商户注意交易环境的安全维护，防止网站被攻击或恶意利用，在网站安装安全控32 件、杀毒软件，并定期对虚假链接进行安全扫描。

在客户支付订单之前，及时向客户发起订单确认，确认信息包括但不限于：发起人、发起时间、收款人、支付金额、商户名称、购买商品类型等；对虚拟充值、游戏通讯类商户设置特殊的单日、单笔交易限额；针对商户被钓鱼网站利用引发的订单替换，可在站内及站间采用具备防钓鱼功能的技术接口进行防范。

加强交易监控，关注短时间内发起订单和订单支付不在同一终端的连续多笔交易、发起订单和订单支付时间间隔过长、同一终端短时间内连续发起多笔订单等异常交易行为。

4.5.6 其他欺诈 除上述主要风险类型以外，商户存在经营情况与注册信息不符,从事违反国家法律、法规和政策规定的业务（如赌博或者其他非法活动）等，给支付机构和客户造成损失的情形。支付机构应通过加强交易监控、加大商户检查力度或严格商户协议约定等方式约束商户违法违规行为。

# 第五部分 资金安全管理

支付机构应严格按照业务监管部门相关支付结算管理制度和规定,依据与客户签订的服务协议，办理资金的结算业务,确保客户资金及时、准确划转及核算。

支付机构应遵循《支付机构客户备付金存管暂行办法》相关规定，确定备付金存管银行，签订备付金存管协议，加强备付金33 管理，保障客户备付金资金安全。

5.1 备付金银行账户 5.1.1 账户的开立和撤销 支付机构应设立或指定资金结算部门，或实际履行资金结算职能的部门负责备付金银行账户的开立、变更、撤销，网上银行等功能的开通、变更、关闭以及相应操作权限的配置管理工作。 支付机构对备付金银行账户的开立、使用情况、账户权限建立审核和监督机制，对账户密码泄露、账户盗用以及越级操作等异常情况应及时通报风险管理部门并采取相应处理措施。

支付机构开立备付金银行账户时，资金结算部门应对拟开立的备付金银行账户名称、性质以及数量的合规性进行审核，并及时与开户行核实账户开立信息。

备付金银行账户撤销前，资金结算部门应核实以下事项： a.待销账户已无任何交易、退款等业务发生，无结余资金； b.账户内存在余额的，已将余额划转至承接账户。承接账户应符合《支付机构客户备付金存管暂行办法》要求； c.已有确定的方法或途径保障该账户销户后不会影响原支付订单的退款。

备付金银行账户开立或销户后，资金结算部门应确保将开户或销户信息及时通知财务等相关部门。开户信息包括账户名称、开户行、账号、开户日期、账户性质（汇缴账户、收付账户）等。销户信息包括账户名称、开户行、账号、销户日期等。 34 5.1.2 网银安全管理 开通备付金银行账户网银功能时，资金结算部门应及时设置、登记并转交网银 USBKey 数字证书管理、使用权限。关闭网银功能时，应收回该账户的网银 USBKey数字证书，并及时登记、统一保管。

资金结算部门应按照逐级授权、职责分离的原则设置、修改、取消网银操作权限。网银权限名单应定期清理，确保授权合理。网银证书应按照分级授权由专人保管，不得带离操作岗位。营业终了，应将操作证书放入保险柜保管，并做好出入记录。

网银密码应定期更换，当有密码使用者离职或者换岗后，应立即更改密码; 资金结算部门应不定期检查网银证书或密码的出入库记录和交接记录。

支付机构应定期对使用 USBKey 数字证书的计算机进行杀毒，防止病毒或者木马非法获取 USBKey 数字证书信息、损坏USBKey数字证书硬件。

5.2 岗位设置与权限 支付机构应遵循职责分离、相互制约的原则，合理设置资金结算、资金管理及财务稽核等岗位，严格分离资金支付的审批与执行、资金的保管、记录与盘点清查、资金的会计记录与审计监督等职能；严禁一人兼任非相容的岗位或独自完成结算全过程的业务操作，做到结算操作与结算对账、业务经办与会计账务处理、业务操作与风险监控、经办与复核及授权相分离。 35 支付机构应遵循“最小授权” 及“按需使用”的原则，设置结算业务操作权限。对提取、修改资金结算及会计核算数据等操作应建立严格的审批、审计和监督检查机制。

对涉及交易资金、客户账户资金变动的操作，包括但不限于商户结算、支付账户提现、商户退款、调账等行为，应至少实行双人、双权限操作。

5.3 商户资金结算 支付机构应确保备付金账户可用、余额充足；头寸不足的，支付机构应按相关规定，及时调整备付金专用存款账户间头寸。 支付机构应准确核算商户待结算资金，并依据与商户签订的支付服务协议，将款项直接结算至协议约定账户。支付机构不得委托他人代理结算。

商户结算规则、结算银行账户发生变更的，支付机构应取得商户的变更申请函件，并确认商户身份后予以及时办理。

支付机构结算时发现存在可能导致资金差错的情况时，应立即终止相关的付款操作，并及时查询、核实，确认无误后再安排付款。

支付机构在监控中发现异常交易或存在争议交易时,应及时采取暂扣、延迟结算等措施加以防范，或通过收取保证金等方式规避风险。

支付机构应按业务监管部门相关规定保留重要凭证、操作记录和操作日志，以便审计和查验。 36 5.4 资金退回及交易退款 支付机构为客户办理充值资金退回、退款业务,或支付机构办理差错资金退回，应遵循原路退回的原则，退回至原支付账户或银行账户，不得截留或退至其他账户；原账户已销户的，支付机构应主动联系客户或发卡机构，确保将相关款项退回客户本人账户。

5.5 手续费 支付机构与商户、合作方（如银行）应签订协议约定收费标准；如需变更，应办理书面变更手续。

支付机构发现计费数据处理异常或疑似异常的，应及时审核确认；计费数据存在差错的，应及时进行调整、修正。

支付机构应指定专门部门负责手续费核算、制表、收付款、开票等工作，按期收取、结转费用；当期未收、未付款应累计至下一结算期结算。

5.6 资金对账 支付机构应每日对其业务系统的交易记录及相关账表进行对账，对账应包括以下内容： a.系统日切时汇总交易账户流水，将交易账户的明细账与总账进行核对； b.系统日切时将各银行电子对账单与系统中的交易明细进行核对。 37 与银行对账周期另有约定的，按照约定周期对账。

资金结算部门应设立专岗定期对所有备付金银行账户收付款情况及交易流水、结存余额进行核对，核对的内容应包括： a.该备付金银行应入账金额与实际入账金额是否一致； b．该备付金银行手续费收取方式和实际收取的手续费用是否与系统中的计费信息或与银行协议约定的一致； c．实际退款、回提金额与系统中的退款、回提金额是否一致； d．资金调拨是否及时足额到账； e.其他应核对账务。

5.7 资金差错处理 支付机构完成资金结算后，应及时检查支付指令是否有效、交易状态是否相符。当银行反馈付款或退款资金的状态可疑时，支付机构应遵循谨慎性原则，在查明原因后，再进行相关处理。业务系统显示扣款成功，银行显示未扣款的，应根据银行对账单进行调账，并及时通知客户；银行显示扣款成功，业务系统中未划账成功的交易，应按照银行扣款记录标记扣款成功状态。

支付机构应确保账实相符，对未达账项、账款差错应尽快查明原因，清理挂账项目须经严格授权；支付机构应留存并妥善保管原始记录资料及处理结果资料。 38 5.8 风险准备金计提 支付机构应该按照业务监管部门要求的计提比例计提风险准备金，开立风险准备金专用存款账户，并对计提比例进行及时调整。

# 第六部分 系统信息安全管理

6.1 组织机构及管理制度 6.1.1 组织机构 支付机构应设立或指定专门部门负责本机构系统信息安全管理，组织制定、发布相关制度、规范，协调处理系统信息安全管理工作中的关键事项，对涉及重大风险事宜进行决策，明确各相关部门系统安全保障职责及人员配置，组织跨部门应急演练等。

负责本机构系统信息安全管理的部门应配备专职人员，实行A、B岗制度，专职人员不可兼任其他岗位。

6.1.2 管理制度 系统信息安全管理制度应贯穿业务运作、系统设计、编码、测试、集成、运行维护以及评估、应急处置全过程，包括安全制度、安全规范、安全操作规程和操作记录手册等。

安全管理制度应具有统一的格式，并进行版本控制。支付机构应定期组织相关部门和人员对安全管理制度体系的适用性和有效性进行审计，针对不足及时进行修订完善。 39 6.2 网络安全管理 6.2.1 网络结构安全要求 a.应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段；应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段； b.应绘制、维护与当前运行情况相符的网络拓扑结构图，区分可信区域和不可信区域； c.应保证防火墙、交换机等主要网络设备的业务处理能力具备冗余空间，满足业务高峰期需要； d.应保证网络各个部分的带宽满足业务高峰期及业务发展需要； e.应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。

f.应在业务终端与业务服务器之间进行路由控制，建立安全的访问路径； g.采用IP伪装技术隐藏内部IP，防止内部网络被非法访问。 6.2.2 访问控制要求 a.应在网络边界部署访问控制设备，启用访问控制功能； b.应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级； 40 c.应对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET等协议命令级的控制； d.应在会话处于非活跃状态达到一定时间，或会话结束后终止网络连接； e.应限制网络最大流量数及网络并发连接数； f.重要网段应采取技术手段防止地址欺骗； g.应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户； h.应限制具有拨号访问权限的用户数量。

6.2.3 安全审计要求 a.应对网络设备运行状况、网络流量、用户行为等进行日志记录，并至少保存 6个月； b.审计记录至少应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； c.应能够根据记录数据进行分析，并生成审计报表； d.应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。

6.2.4 入侵防范 a.应部署入侵检测/防御系统，并在网络边界处监视和记录以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等； b.当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击41 目的、攻击时间，在发生严重入侵事件时应提供报警。

6.2.5 恶意代码防范 a.应在网络边界处对恶意代码进行检测和清除； b.应维护恶意代码库的升级和检测系统的更新。

6.2.6 网络设备防护 a.网络设备用户的标识应唯一； b.应对登录网络设备的用户进行身份鉴别； c.主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别； d.身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换； e.当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； f.应对网络设备的管理员登录地址进行限制； g.应实现设备特权用户的权限分离; h.应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施； i.应定期检查网络设备运行状况和软件版本信息，定期对网络设备配置文件进行备份。

6.2.7 身份鉴别 a.应对登录操作系统和数据库系统的用户进行身份标识和鉴别，严禁匿名登录； 42 b.操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换； c.应启用登录失败处理功能，可采取结束会话、限制非法登录次数、锁定账户和自动退出等措施； d.当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听； e.应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性。

f.应采用两种或两种以上组合的鉴别技术对管理用户进行身份识别，并且身份鉴别信息至少有一种是不可伪造的。

6.2.8 边界完整性检查 a.应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断； b.应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

6.3 系统运维管理 6.3.1 物理环境管理 a.各系统运行部门应按照国家计算机房安全管理的有关规定加强管理，并保持机房清洁、整齐、有序，制定相应的制度和规则，做好机房的安全工作。 b.禁止将易燃、易爆、易腐蚀和磁性物品等可能影响运行的危险品带入机房；禁止将食物、饮料带入机房。 43 c.支付各环节涉及的机器、网络设备等需专网专用，不得与其他业务的开展重合。

d.支付系统设备（包括计算机软硬件、网络、安全设备等）应实行专人管理。禁止将支付系统设备挪作他用。 e.支付系统网络设备、各直接参与者的前置机设备由网络部门统一负责安全管理。 f.任何人员进出数据中心机房需登记、涉及重要数据的区域需提前申请并由相关责任人陪同方可进入、参观人员仅可访问指定授权区域。

g.支付系统使用的存储介质，应进行严格的病毒检查，防止计算机病毒侵入。 h.未经批准，支付系统设备不得与其它设备、网络连接。

i.当遇到重大故障 (如支付中断超过 2 小时以上时)或需停机维护时，及时将故障情况或维护申请上报给所在地中国人民银行分支机构，并书面报告故障原因、影响及补救措施。

6.3.2 设备管理 a.应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理。

b.应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等。 44 c.应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作。

d.应对信息系统相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理。

e.应做好设备登记工作，制定设备管理规范，落实设备使用者的安全保护责任。

f.需要废止的设备，应由指定专门部门使用专用工具进行数据信息消除处理，如废止设备不再使用或调配到其他单位，应备案并对其数据信息存储设备进行消磁或物理粉碎等不可恢复性销毁处理，同时备案。

g.设备确需送外单位维修时，应指定专门部门彻底清除所存的工作相关信息，必要时应与设备维修厂商签订保密协议，与密码设备配套使用的设备送修前必须请生产设备的科研单位拆除与密码有关的硬件，并彻底清除与密码有关的软件和信息，并派专人在场监督。

h.制定规范化的设备故障处理流程，建立详细的故障日志(包括故障发生的时间、范围、现象、处理结果和处理人员等内容)。

i.应确保信息处理设备必须经过审批才能带离机房或办公地点。

j.应对设备进行分类和标识,建立标准化的设备配置文档。 45 k.新购置的设备应经过测试，测试合格后方能投入使用。

l.应做好设备登记工作，制定设备管理规范，落实设备使用者的安全保护责任。

6.3.3 数据安全及备份恢复 6.3.3.1数据的存储和传输 a.支付机构应采取有效措施，保障系统数据信息的完整性和安全性。

b.支付机构应能够监测到系统管理数据、客户身份信息、支付业务信息等重要数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

c.支付机构应采用加密或其他有效措施实现系统管理数据、客户身份信息、支付业务信息、会计档案信息等的保密性。

支付机构应采取相应技术措施，在数据传输过程中确保支付指令的完整性、一致性和不可抵赖性。

6.3.4.2数据备份和恢复 a.应识别需要定期备份的重要业务信息、系统数据及软件系统等； b.应建立备份与恢复管理相关的安全管理制度，对备份信息的备份方式、备份频度、存储介质和保存期等进行规范； c.应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略须指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法； 46 d.应建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存； e.应定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。

6.4 应急管理 支付机构应制定与其业务规模、复杂程度相适应的应急和业务连续方案，建立恢复服务和业务连续运行保障机制，并定期检查、测试，确保有效性。应急管理要求包括： a.在统一的应急管理框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容； b.从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障； c.对系统相关的人员进行应急预案培训，应至少每年举办一次培训； d.定期对应急预案进行演练，并根据实际情况进行修订调整。

# 第七部分 支付机构反洗钱和反恐怖融资管理要求

非金融支付机构应切实遵守《中华人民共和国反洗钱法》、《支付机构反洗钱和反恐怖融资管理办法》等法律法规，全面履行反洗钱及反恐怖融资义务。

## 7.1 基本要求

支付机构应建立内部的反洗钱和反恐怖融资的管理组织架构，建立和完善反洗钱和反恐怖融资的内控制度体系，制定反洗钱和反恐怖融资操作规程，全面履行反洗钱及反恐怖融资义务。

## 7.2 组织架构及职责要求

### 7.2.1 领导机构及职责

支付机构应设立以机构负责人为组长、职能部门负责人为副组长，各相关部门负责人为组员的反洗钱和反恐怖融资领导机构，全面负责反洗钱和反恐怖融资工作，主要职责包括：

a.反洗钱和反恐怖融资工作的整体协调、规划;

b.建立、健全反洗钱和反恐怖融资工作管理机制，组织、安排相关制度和流程的建设；

c.组织相关部门和人员履行可疑交易报告义务， 配合监管机关和司法机关开展对可疑交易的调查；

d. 建立与业务监管部门、司法机关的报告与沟通机制。

### 7.2.2 职能部门及职责

支付机构应设立或指定专门部门负责具体开展反洗钱和反恐怖融资工作，督促和指导各相关部门执行各项法律、法规、制度，并设置反洗钱和反恐怖融资专门岗位，主要职责包括：

a.根据领导机构要求，建立、健全反洗钱和反恐怖融资工作机制，制定和修订有关制度、规章及操作规程，并组织实施；

b. 汇总反洗钱和反恐怖融资数据及可疑交易信息报表，并报领导机构审批后，及时上报中国反洗钱分析监测中心；

c. 协助业务监管部门和司法机关开展反洗钱和反恐怖融资调查；

d. 组织、推动内部开展反洗钱和反恐怖融资预防、监控、协查和报告，并定期进行监督检查；建立内部报告制度，定期提交领导机构；

e. 定期组织内部的反洗钱和反恐怖融资培训、宣传工作；

f. 履行法律、法规规定的支付机构其它反洗钱和反恐怖融资的工作职责。

### 7.2.3 相关部门职责

7.2.3.1相关部门负责人职责

各相关部门、分支机构、外派机构负责人对本部门或本分支机构反洗钱和反恐怖融资工作负责，主要职责包括：

a.在开展业务过程中严格落实反洗钱和反恐怖融资相关规定, 推动本部门内控制度的完善；

b. 对可疑交易信息进行汇总分析并报告职能部门；

c. 组织部门内员工的反洗钱和反恐怖融资宣传、培训，对用户或商户进行反洗钱和反恐怖融资宣传、教育；

d. 配合机构反洗钱和反恐怖融资职能部门的工作，履行相关职责。

7.2.3.2联络员职责 支付机构各部门、分支机构、外派机构应指定专人作为反洗钱和反恐怖融资联络员， 协助部门负责人开展反洗钱和反恐怖融资日常工作。主要职责包括：

a.及时全面地向本部门员工传递反洗钱和反恐怖融资工作信息，督促本部门完成各项反洗钱和反恐怖融资工作；

b. 具体落实本部门反洗钱和反恐怖融资宣传、培训工作；

c. 组织本部门的反洗钱和反恐怖融资相关制度的内部审计工作，定期检查工作开展情况，跟进整改和完善情况；

d. 记录报告可疑交易信息，及时向部门负责人和职能部门报告本部门反洗钱和反恐怖融资工作中存在的问题，提出工作建议。

e. 履行其他反洗钱和反恐怖融资工作职责。

各部门联络员与职能部门专门岗位人员组成反洗钱和反恐怖融资工作小组，负责反洗钱和反恐怖融资执行及研讨反洗钱工作问题。

## 7.3 客户身份验证及资料保存

支付机构应当勤勉尽责，建立健全客户身份识别制度，遵循“了解你的客户”原则，针对具有不同洗钱和恐怖融资风险特征的客户、业务关系或者交易应采取相应合理的措施，了解客户及其交易目的和交易性质，了解实际控制客户的自然人和交易的实际受益人。

### 7.3.1 客户身份识别要求

支付机构在开展以下业务时，应遵循用户及商户发展策略相关要求，严格落实客户身份识别制度,留存相关资料并履行保密义务：

a.支付机构为用户开立支付账户；

b. 同一客户的多个支付账户建立关联；

c. 商户拓展及资质审查；

d. 用户及商户身份信息变更。

### 7.3.2 重新识别客户要求

支付机构应根据规定在出现以下情形时，重新识别客户：

a.客户要求变更姓名或者名称、有效身份证件种类、身份证件号码、注册资本、经营范围、法定代表人或者负责人等的；

b. 客户行为或者交易情况出现异常的；

c. 先前获得的客户身份资料存在疑点的；

d. 支付机构认为应重新识别客户身份的其他情形。

### 7.3.3 客户信息留存

支付机构应按照人民银行规定内容妥善保存客户身份资料和交易记录，保证能够完整准确重现每笔交易。客户身份资料包括各种记载客户身份信息的资料、辅助证明客户身份的资料和反映支付机构开展客户身份识别工作情况的资料 支付机构保存的交易记录应当包括反映以下信息的数据、业务凭证、账簿和其他资料：

a.交易双方名称；

b. 交易金额；

c. 交易时间；

d. 交易双方的开户银行或支付机构名称；

e. 交易双方的银行账户号码、支付账户号码、预付卡号码、特约商户编号或者其他记录资金来源和去向的号码。

支付机构在开展客户身份识别的业务时，应按照保证完整准确重现每笔交易的原则保存交易记录。

### 7.3.4 客户身份资料和交易记录保存系统

支付机构应当建立客户身份资料和交易记录保存系统，实时记载操作记录，防止客户身份信息和交易记录的泄露、损毁和缺失，保证客户信息和交易数据不被篡改，及时发现并记录任何篡改或企图篡改的操作。

支付机构应当完善客户身份资料和交易记录保存系统的查询和分析功能，便于反洗钱和反恐怖融资的调查和监督管理。并按照监管部门规定的格式及期限保存客户身份资料和交易记录。在出现支付机构终止支付业务时，应当按照中国人民银行有关规定处理客户身份资料和交易记录。

## 7.4 可疑交易报告

a.支付机构应对本机构的全部交易开展监测和分析，及时报告可疑交易；

b.根据客户特征和交易特点，支付机构应制定和完善符合本机构业务特点的可疑交易标准，向中国人民银行、总部所在地的中国人民银行分支机构和中国反洗钱监测分析中心备案；

c.支付机构应建立完善有效的可疑交易监测分析体系，明确内部可疑交易处理程序和人员职责，并指定专门人员，负责分析判断是否报告可疑交易；

d.支付机构应结合客户身份信息和交易背景，对客户行为或交易进行识别、分析，有合理理由判断与洗钱、恐怖融资或其他犯罪活动相关的，应在发现可疑交易之日起 10 个工作日内，由其总部以电子方式向中国反洗钱监测分析中心提交可疑交易报告。可疑交易报告的具体格式参照中国人民银行规定。

支付机构应将已上报可疑交易报告的客户列为高风险客户，持续开展交易监测，仍不能排除洗钱、恐怖融资或其他犯罪活动嫌疑的，应在 10 个工作日内向中国反洗钱监测分析中心提交可疑交易报告，同时以书面方式将有关情况报告总部所在地的中国人民银行分支机构。

支付机构应完整保存对客户行为或交易进行识别、分析和判断的工作记录及是否上报的理由和证据材料；

e.支付机构在履行反洗钱和反恐怖融资义务过程中，发现涉嫌犯罪的，应立即报告当地公安机关和中国人民银行当地分支机构，并以电子方式报告中国反洗钱监测分析中心；

f.支付机构怀疑客户、资金、交易或者试图进行的交易与恐怖主义、恐怖活动犯罪以及恐怖组织、恐怖分子、从事恐怖融资活动的人相关联的，无论所涉及资金金额或者财产价值大小，都应当提交涉嫌恐怖融资的可疑交易报告；

g.支付机构发现或者有合理理由怀疑客户与国务院有关部门、中国人民银行、司法机关、联合国安理会要求或发布的信息相关的，应立即报告当地公安机关和中国人民银行当地分支机构，并以电子方式报告中国反洗钱监测分析中心；

h.支付机构各部门、各岗位均负有可疑线索的发现和分析职责。员工发现可疑情形但不能完全判断是否为可疑交易的，需及时报告反洗钱和反恐怖融资专岗及部门负责人。

i.对反洗钱和反恐怖融资可疑交易审核过程及审核结论应当进行记录，由参与审核人员确认，并进行归档；

## 7.5 反洗钱和反恐怖融资调查

a.支付机构应当积极配合中国人民银行及其分支机构实施反洗钱和反恐怖融资调查，根据监管条例如实提供调查材料、配合执行监管部门提出的要求，不得拒绝或者阻碍；

b. 支付机构应当按照中国人民银行规定提供有关文件和资料，不得拒绝、阻挠、逃避监督检查，不得谎报、隐匿、销毁相关证据材料。并对其所提供的文件和资料的真实性、准确性、完整性负责；

c. 支付机构应当按照中国人民银行的规定，向所在地中国人民银行分支机构报送反洗钱和反恐怖融资统计报表、信息资料、工作报告以及内部审计报告中与反洗钱和反恐怖融资工作有关的内容，如实反映反洗钱和反恐怖融资工作情况，并配合人民银行现场检查；

d. 在反洗钱和反恐怖融资调查工作调查期间，凡涉及客户身份资料和交易记录的，应遵循相关规定的最低保存期，如在保存期届满时调查仍未结束的，支付机构应将其保存至反洗钱和反恐怖融资调查工作结束；

## 7.6 宣传培训

a.支付机构应强化本机构反洗钱和反恐怖融资宣传、培训工作力度，提升全员合规意识及业务素质；未经培训的员工，不得从事与反洗钱和反恐怖融资相关的工作。

培训内容包括但不限于：反洗钱和反恐怖融资政策、法律、法规和基本状况；本机构反洗钱和反恐怖融资制度、程序和措施；可疑交易分析、识别和报告的要求和技巧；客户尽职调查的内容和要求。

b. 支付机构应对客户进行反洗钱和反恐怖融资宣传和教育。

## 7.7 保密制度

支付机构及其工作人员对依法履行反洗钱和反恐怖融资义务获得的客户身份资料和交易信息应当予以保密，法律法规另有规定的除外。

## 7.8 内部控制

### 7.8.1 自查评估

支付机构应当根据业务监管部门的要求，定期或不定期对机构的反洗钱和反恐怖融资开展情况及风险情况进行自查。

### 7.8.2 内部审计

支付机构审计部门应定期对本机构的反洗钱和反恐怖融资工作进行内部审计，及时发现工作缺陷，提出整改意见。

### 7.8.3 考核制度

支付机构应设立反洗钱和反恐怖融资的考核制度，对于做出突出贡献的部门和个人，给予表彰或奖励；对于内部审计过程中发现的违规问题，以及未按照有关要求开展反洗钱和反恐怖融资工作、未按照要求保守秘密等，致使该机构遭受重大损失和重大影响的，由内部审计部门根提出处罚意见供领导机构做出处罚决定。

# 第八部分 风险信息共享和风险事件处理

8.1 基本原则

为有效防范和控制支付风险，协会建立与各成员单位之间的风险信息共享、风险事件协同调查机制，提高成员机构防控风险能力和调查处理风险事件的效率。

协会及各成员单位建立风险联系人网络，负责风险信息共享、风险事件报送和调查工作。

各成员单位在开展风险信息共享和事件报送、协助调查时，应遵守国家法律，坚持保密原则。风险共享信息和风险事件信息仅供共享单位内部使用，任何机构不得泄漏、披露有关内容，法律法规另有规定的除外。

8.2 风险信息共享内容 经成员单位同意，协会作为风险信息共享平台提供方，负责建立、维护风险信息共享机制，成员单位通过向协会提供信息或提交信息查询请求，实现各成员单位之间的风险信息共享。

参与共享的各成员单位应根据统一的风险信息共享要素内容，及时提供真实、完整的风险信息并予以定期更新；风险信息使用方须承担保密义务，不得擅自向客户或社会公开。

风险信息共享要素包括但不限于：风险信息类型、具体内容、风险信息主体名称、报送理由、时间等。

对符合以下条件之一的商户及用户，各成员单位应终止向其提供互联网支付服务，并向支付清算协会报送风险信息。

8.2.1 风险商户

a.属于相关法律法规明令禁入类商户，包括非法设立的经营组织、特殊行业商户等类型商户；

b.被监管部门、司法部门风险提示的涉及套现等违法违规行为的高风险商户；

c.支付机构自行侦测发现的涉及套现、洗钱、伪冒交易等欺诈行为的高风险商户。

8.2.2 风险用户

a.被证实以虚假或变造的身份证明资料开设互联网支付账户的用户；

b.被监管部门、司法部门提示的涉及套现等违法违规行为的高风险用户；

c.成员单位自行侦测发现的涉及套现、洗钱、伪冒交易等欺诈行为的高风险用户。

8.3 风险事件的划分

风险事件的等级划分应区分重大风险事件、普通风险事件，可参照如下标准进行划分：

重大风险事件包括：

a.账户信息泄露类：涉及 200个以上账户信息发生疑似信息泄露的，或 100个以上账户信息确认发生信息泄露的。

b.套现：疑似套现总额达到 200万元以上的，或确认套现总额达 100万元，或平台类商户组织进行大规模套现活动的。

c.由监管部门、司法机关通报的互联网支付风险案件；

d.经由媒体报道或客户投诉的影响范围较大、社会反响强烈的风险事件；

e.确认损失超过 100万元以上的风险事件。

8.4 风险事件的处理 各成员单位应建立风险联系人机制，负责协调开展风险事件58 调查等相关工作。

各成员单位应及时向监管机构和协会报送各类风险事件、响应各类风险提示，并配合监管部门、司法机关和其他成员单位，调查风险事件。

# 第九部分 纪律与责任

支付机构开展互联网支付业务应参照本指引构建完善的风险管理体系，落实风险管理措施，积极防范支付业务风险。协会将充分发挥自律职能，根据本指引要求协调会员单位做好风险管理工作，并将其纳入自律监督检查内容。

对因会员单位风险管理制度不完善或未有效落实本指引风险管理措施而导致发生重大风险事件，对行业造成负面影响的，将依据《网络支付行业自律公约》有关自律性惩戒措施对其进行处理。

# 第十部分 附则

本指引与国家法律、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。

本指引自发布之日起实施。

本指引由中国支付清算协会网络支付应用工作委员会负责修订和解释。