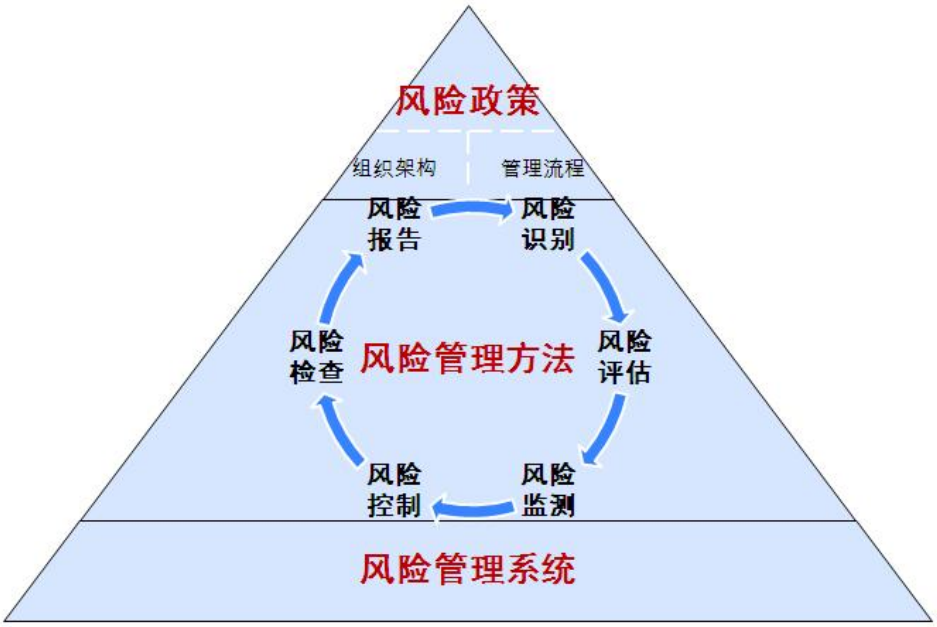
一、 互联网支付的风险管理

电子支付系统作为电子货币与交易信息传输的系统，既涉及到国家金融和个人的经济利益，又涉及交易秘密的安全；支付电子化还增加了国际金融风险传导、扩散的危险。能否有效防范电子支付过程中的风险是电子支付健康发展的关键。

风险管理是指面临风险者进行风险识别、风险估测、风险评价、风险控制，以减少风险负面影响的决策及行动过程。随着全球非金融机构支付业务的蓬勃发展，支付业务必将面临各种风险的挑战。因此，全面风险管理的重要性也逐渐凸显，并成为整个支付行业关注的焦点和工作重心。无论是监管部门、投资者、金融机构还是非金融机构，都日益认识到进行全面风险管理的必要性和迫切性，并对全面风险管理提出了明确的目标和更高的要求。

风险管理体系



风险管理体系包括风险政策、风险管理方法和风险管理系统三个层次，风险政策是手机支付风险管理的指导方针，包括各项业务规定、组织架构、管理流程等，而风险管理方法是通过风险识别、风险评估、风险监测、风险控制、风险检查、风险报告等对风险进行程序化的管理，最终通过风险管理系统进行 IT层面的支持。

首先，风险管理需要从高层做起。对于非金融机构支付业务而言，风险管理首先是与时俱进的动态管理过程。在此过程中，管理层要针对内外环境及业务结构变化，适时调整风险管理思路；要善于更新风险管理知识，不断提高风险敏感性；要及时吸收风险管理经验，不断丰富企业风险管理文化；要适应日常风险管理新需求，不断健全风险基础设施；要紧跟业务创新步伐，及时开发新的风险管理工具；要根据风险状况变化，强化内部控制机制，实现支付业务的持续稳健经营。

另外，风险管理是对支付业务领域各类风险集成化管理，作为一个类金融领域，首先需要识别出承担哪些类型的风险，再根据风险内

在的相关性进行集成化管理，不能孤立地管理某一类风险。

A. 风险识别是对支付的业务、产品、参与方、业务流程等进行全面的梳理，从中对风险的存在和发生的可能性以及风险产生的原因等进行分析判断。

B. 风险评估是在风险识别的基础之上，应用一定的方法估计和测定风险发生的概率和一旦发生所带来的损失大小，以及对整体手机支付业务所带来的影响，从而明确哪些风险需要并能够加以监控以及风险应对措施到何种程度最为适宜等问题。

C. 风险监测是通过一些风险指标，如每亿元交易的损失率、每百万客户的投诉率、当月新增可疑套现金额、当月新增可疑洗钱风险笔数等可供掌握的统计性指标，判断风险状况的变化和风险大小；另一层面，风险监测是对一定风险模型之下的实时交易数据或批量交易数据进行判断，从而根据风险模型判断当前交易的风险大小和需要采取的措施。

D. 风险控制是对监测到的风险采取一定的风险控制措施，如交易阻断、交易延迟、增加交易条件、增加交易限制、交易人工确定、交易风险通知客户（如电话、短信、信函、在线提醒等）、标识交易主体风险等级。

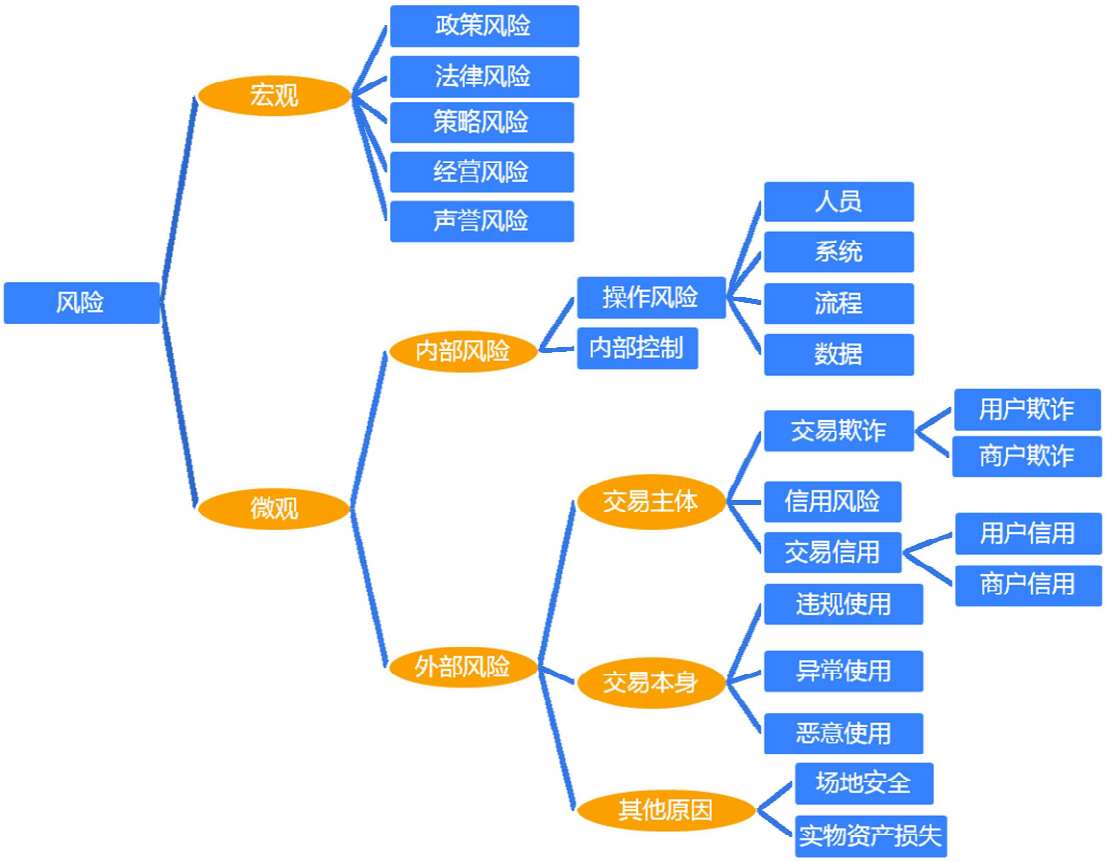
E. 风险检查是辅助定量的风险识别、风险评价、风险监测、风险控制的补充手段，通过抽查、核实相关交易数据，抽样对风险可疑客群进行短信或客服联系等方式检查当前的风险状况，是一种风险定性管理的办法。

F. 风险报告是对报告期限内的风险情况的总体说明或专项说明，包括各类风险发生的情况，相应风险控制措施的效果，以及对后续风险管理工作的建议等内容。

其次，风险基础设施是风险管理的基石。一方面是人文基础设施建设，主要包括风险治理、风险组织以及政策程序：风险治理要求管理层以及利益相关者必须认清自身职责，并在履行职责过程中高效协作，同时充分赋予资深风险专家决策权；风险组织以纵向垂直扁平化为主、以横向贯穿业务单元为辅的矩阵式架构，组织形式应随业务变化可动态调整；组织决策采取集中决策为主、分散决策为辅的模式；风险政策程序要全面、统一、配套，在坚持政策一致性的前提下，适度增加政策执行细则的灵活性，但应确保置于严密内控监督之下。另一方面，加强技术基础设施建设，包括建立风险数据集市，建立高度集成的管理信息系统，开发运用各种风险计量工具，这是实现风险管理程序化、集成化和智能化的物质基础。

（一）支付领域总体风险

《中央企业全面风险管理指引》对风险的定义是 未来的不确定性对企业实现其经营目标的影响 。企业风险一般可分为战略风险、财务风险、市场风险、运营风险、法律风险等；也可以能否为以能否为企业带来盈利等机会为标志，将风险分为纯粹风险（只有带来损失一种可能性）和机会风险（带来损失和盈利的可能性并存）。支付领域总体风险有如下类型：



A、宏观层面风险

a)政策风险：因第三方支付或相关领域政策不明朗为支付业务带来的风险

b)法律风险：自身和交易方因没有遵守法律或监管法令的规定而带来财务损失、合约无法执行、监管处罚、诉讼等的风险

c)策略风险：因经营战略或策略层面的失误而导致的整体损失

d)经营风险：因技术层面或营运层面落后于竞争对手而导致企业无法实现经营目标的风险

e)声誉风险：因为不可预期的突发事件而导致的声誉受损带来的风险。

B、微观层面风险　　内部风险

a)操作风险：因为不完善或有缺陷的流程、人员、系统而导致的资金损失，如员工欺诈、员工操作失误、数据传输被攻击、应用系统

设计缺陷被黑客利用、计算机病毒入侵主机

b)内部控制

C、微观层面风险　　外部风险

a)交易主体

用户交易欺诈，涉及账户安全风险，对用户账户形成直接资金损失的欺诈，或虚报用户账户安全风险

商户交易欺诈，涉及账户安全风险，对商户账号形成直接资金损失的欺诈，或虚报商户账户安全风险

信用风险，因恶意透支导致的资金损失。

交易信用，分为用户交易信用和商户交易信用两部分。前者如用户恶意退货，后者如商家收款后不发货或货品不符合要求、恶意倒闭等。

b)交易本身

违法使用，包括洗钱（大额交易、可疑交易）、赌博、贩毒、逃税等，

违规使用，包括套现和套利等，前者如将信用卡中银行信贷资金通过手机支付平台转换为现金而逃避银行手续费和罚金的风险；后者如代理商为骗取佣金、红包或其他奖励的舞弊行为和用户交叉持有产品而逃避手续费或套取更多奖励的风险。

恶意使用，其他对支付平台带来不良影响或后果的交易行为。

c)其他外部风险

实体资产损失

工作场所安全事件

（二）风险控制策略与措施

1.风险控制整体策略

风险控制整体策略是：事前审核，事中监控，事后处理。

A. 事前审核：（a）商户的识别与管理；（b）根据业务和产品特点分层管理。

B. 事中监控：（a）高风险业务重点监控；（b）日报、特殊报表、实时提示。

C. 事后处理：

a) 协助查询：涉及风险交易或商户的查询、提供公安所需数据；

b) 案件处理：商户欺诈、个人诈骗或黑客交易

c) 总结经验教训

d) 调整工作流程

e) 修改系统功能

f) 调整商户审核内容

g) 调整银行接口应用范围

2.风险控制方式

风险管理的方式主要包括：规避风险；预防风险；转移风险；自留风险。

A. 规避风险：即消极躲避风险。这一策略就不宜采用：(a)可能会带来另外的风险。(b)会影响企业经营目标的实现

B. 预防风险：采取措施消除或者减少风险发生的因素。

C. 转移风险：在危险发生前，通过采取出售、转让、保险等方法，

将风险转移出去。

D. 自留风险：企业自己承担风险。途径有：(a)小额损失纳入生产经营成本，损失发生时用企业的收益补偿。(b)针对发生的频率和强度都大的风险建立意外损失基金，损失发生时用它补偿。对于较大的企业，可建立专业的自保公司。

3.不同业务阶段的风险控制重点

在商户准入阶段，主要面对的是商户欺诈、商户经营性质不合规风险；在交易支付阶段，主要面对的是账户盗用、信息泄露、交易欺诈、批量账户控制、银行卡盗用、套现、钓鱼、拒付、洗钱。在账务结算阶段，主要面对的是业务规则漏洞，操作失误/违规风险。

风险控制会从：账户安全、反欺诈、商户风险防范和金融风险防范四类。

A. 账户安全：保证账户及资金安全，处理账户被盗用和信息泄露案件。

B. 反欺诈：对批量申请账户进行监查核控制，同时防范和处理钓鱼欺诈案件。

C. 商户风险防范：针对商户的欺诈行为和商户经营性质不合规行为。严格控制准入，并对发现的问题限期整改，如果整改不能通过，则强制解约。

D. 金融风险防范：主要防范和处理被盗银行卡的案件，同时监控日常交易，并设定反套现和反洗钱规则，对违规交易和现象进行上报和处理。

4.风险识别与评估管理办法

第一章　总则

第一条、 为了准确识别、评估风险，实现对风险及时、全面、统一、有效的管理，根据相关管理政策，制定本办法。

第二条、 本办法适用于公司各总部。

第三条、 本办法所称风险识别与评估是指根据风险控制的基本原理，按照规定的工作流程，采用一定的方法，对风险内部控制效果进行的内部评价活动，是公司风险管理部持续改进的基础工作和关键环节。

第四条、 风险识别与评估工作遵循下列原则：

（一） 全面性原则。要对公司所有业务、经营管理活动过程中的风险进行识别与评估，包括对周期性或临时性活动的风险进行甄别。

（二） 主动识别原则。在引入新的活动或程序，或对原有活动和程序进行修改之前以及在环境和条件发生变化时，要进行风险的识别与评估，确保任何新的和以前未予控制的风险得到识别和控制。

（三） 适用性原则。风险控制方案的制订考虑公司风险控制现状、控制目标的需要、法律法规、监管要求以及技术和财务因素，确保控制方案有效、合理、经济、适度，同时防止控制过度和控制无效。

（四） 持续改进原则。风险可接受时，对风险进行监测和评

审，确保持续可接受；不可接受时，确定控制目标并制定控制方案，对控制方案的执行情况进行跟踪监测，并根据监测结果持续改进控制目标与控制方案。

第五条、 本办法涉及的专有名词定义如下：

（五） 风险点：指风险因素在业务流程中环节的反映和表现。

（六） 可能性：用作对事件发生概率或频率的定性描述。

频率：是指在一段时间内发生次数来表达事件发生率的量度。

概率：是指以特定事件或结果与可能发生事件或结果的总数之比来量度的特定事件或结果的可能性。

（七） 影响性：是以定量或定性的方式表示的一个事件的结果（一个事件可能有多个与其相关的结果）。

（八） 损失：指任何财务或其他方面的负面影响。

（九） 固有风险：指在没有考虑控制活动的有效性或其他减小风险的措施没有付诸实施之前已经存在的风险。

（十） 剩余风险：指在现有的控制活动或其他风险减轻措施所不能完全清除的风险。

第二章 风险识别与评估的组织

第六条、 公司应当全面识别和评估经营管理各个环节、各项业务流程中的风险，并应当特别关注重点岗位和重点业务环节风险的识别与评估。

第七条、 发生下列情形之一的，公司应当及时组织风险识别和评估：

（十一） 风险管理政策修改；

（十二） 新产品和新业务开发；

（十三） 新设备和新系统应用；

（十四） 重大事故、险情、案件、隐患发生时；

（十五） 业务流程发生较大变化时；

（十六） 组织机构变革；

（十七） 法律法规、监管要求发生变化；

（十八） 同业发生新的风险损失事故且可能本部门存在同样问题时；

（十九） 其他需要开展风险识别与评估的工作情形。

第八条、 风险日常识别与评估由各职能部门、分子公司在其职责范围内随时进行，并将识别评估工作记录在报告本部门、单位分管领导的同时，抄报风险管理部。

第九条、 风险定期识别与评估由风险管理部组织开展。

第十条、 定期风险识别与评估应当由风险管理部组织撰写及上报。

第十一条、 风险评估过程中应当填写《风险识别与评估工作表》，并留存备查。

第十二条、 风险识别与评估结果应当形成书面评估报告，报告的主要内容包括评估工作实际开展情况的描述、评估的基本结论和改进建议等。

第十三条、 风险管理部应收集整理本单位风险管理数据，持续改

进和加强风险管理工作。

第三章　风险识别

第十四条、风险识别包括确定风险的来源，风险产生的原因，描述其风险特征和确定哪些风险事件有可能产生风险。风险识别应当在公司的经营管理中持续进行。

第十五条、风险识别按照流程或业务活动确认、损失事件识别、风险点描述、对应流程环节、风险点编码的顺序进行。

第十六条、流程或业务活动确认。确认需要评估的流程或业务活动，仔细研究需要评估的流程或业务活动的特点，并对流程和活动划分阶段，绘制流程图，对每一阶段逐一评估风险。

第十七条、损失事件识别。针对流程或活动的每一阶段，分析可能发生的损失事件，将可能发生的损失事件分类评级。

第十八条、风险点描述。将该风险在流程环节的表现作为风险点，以更清晰地显示风险因素在流程环节的表现形式。

第十九条、对应流程环节。将风险点与流程中的环节相对应，并在流程图中对应的流程环节上依次标上序号。

第二十条、风险点编码。以流程环节编码加上风险因素编码确定唯一的风险点编码。

第四章　风险评估

第二十一条、公司应当在风险事项识别的基础上应当对风险发生的可能性、影响性以及风险等级进行评估。

第二十二条、风险发生的可能性分为几乎不可能、不大可能、比

较可能、很可能和极有可能。

风险的影响性分为几乎没有、很小、中等、较大和严重。

风险等级根据发生的可能性和影响性进行确定。

第二十三条、风险评估应当分别对固有风险和剩余风险进行评估。

第二十四条、固有风险评估：

（一）可能性评估。根据《风险识别与评估工作表》评估风险因素的可能性等级。

（二）影响性评估。根据《风险识别与评估工作表》评估风险因素的影响性等级。

（三）确定风险等级。根据可能性等级和影响性等级的乘积计算固有风险等级，并依据《风险识别与评估工作表》确定固有风险的等级。

第二十五条、剩余风险评估：

（一）现有控制描述。从流程内和流程外分别描述针对风险因素的现有控制措施。

（二）可能性评估。根据《风险影响性等级表》评估在现有控制措施下，风险因素的可能性等级。

（三）影响性评估。根据《风险影响性等级表》评估在现有控制措施下，风险因素的影响性等级。

（四）确定风险等级。根据可能性等级和影响性等级的乘积计算在现有控制措施下剩余风险等级，并依据《风险影响性等级表》确定剩余风险的等级。

第五章　风险控制

第二十六条、公司应当根据现有控制措施下评估的风险等级对现有控制措施的有效性进行评价：

（一）控制有效。

（二）控制基本有效。

（三）控制不足。

（四）控制过度。

第二十七条、风险管理部应依据评价结果，会同风险事项的关联部门对所有风险因素提出明确具体的控制目标。

第二十八条、对现有控制措施不能达到预期风险控制目标的，应由风险管理部会同风险事项的关联部门拟定新增控制措施，审批后实施。

若新增控制措施仍不能达到预期的控制目标的，应当重新拟订风险控制方案。

第二十九条、风险管理部应对风险控制方案的执行情况进行跟踪监测，并适时对控制措施的有效性、适宜性进行验证。

第三十条、风险控制改进方案的实施、监测和验证情况，应当按照风险的报告路线进行报告。

第三十一条、当发生重大损失、险情或不符合时，风险管理部应对风险识别评估的方法、过程以及结果进行必要的评审和改进。

第三十二条、同业发生风险管理案件时，公司应当对该案件进行分析和评估，检查本单位相关事项的控制措施是否有效，并及时予以

完善和改进。

第六章　附则

第三十三条、相关部门应当收集整理风险识别与评估过程中形成的各类表单、记录等资料，并妥善保管备查。

第三十四条、风险识别与评估过程中发现的风险点、存在的内部控制不当环节和改进建议，均属公司内部机密，相关人员应严格履行保密义务。

第三十五条、公司风险管理部可以根据工作实际，对本办法所列附件内容组织统一修订和完善。

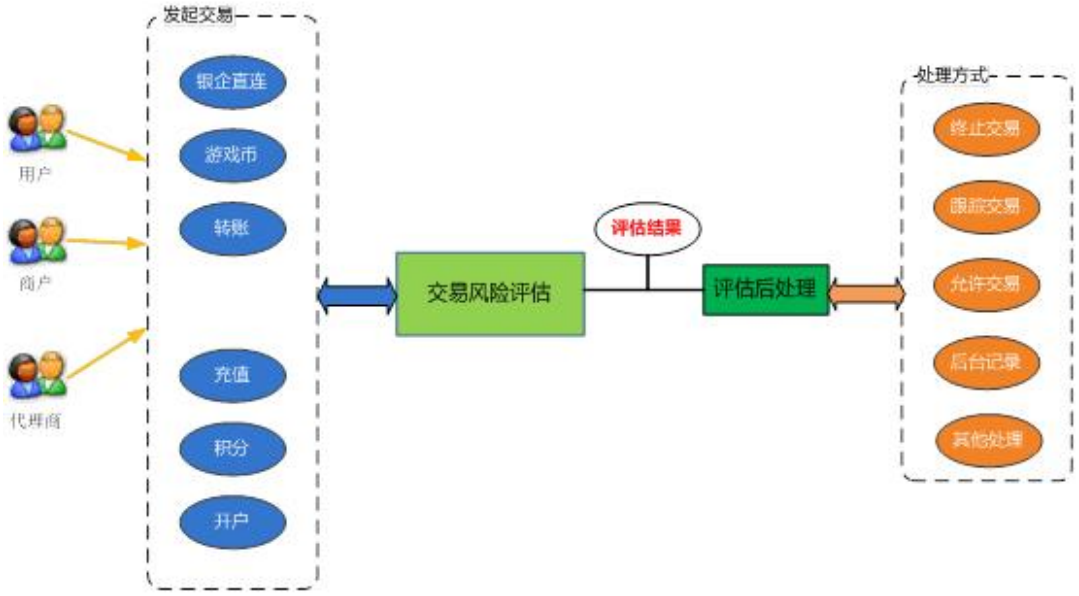
第三十六条、本办法由公司风险管理部负责解释和修订。

第三十七条、本办法自下发之日起施行。

（三）可疑交易处理及管理办法

1.风险控制流程说明

（1）总体风险处理流程：



（2）险预警流程说明：

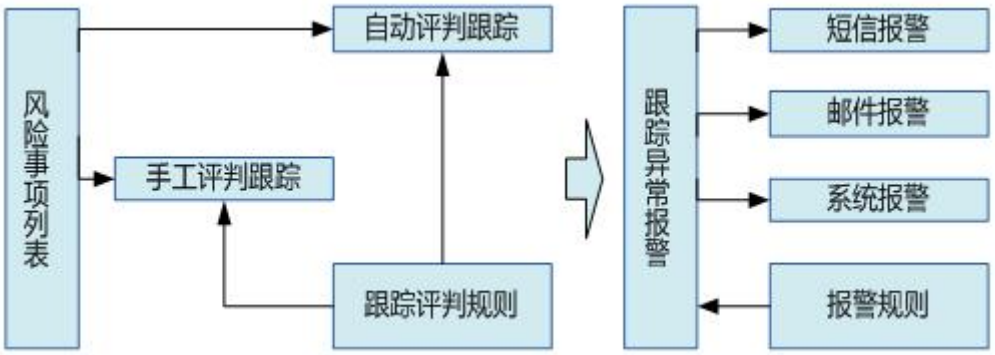
A、 通过风险事项查询规则，对符合风险事项的客户可以进行手工或自动评判是否启动跟踪；

B、 系统按跟踪评判规则，在预定义的时间间隔扫描被跟踪的客户行为数据；

C、 对于达到跟踪报警阀值的客户，根据报警规则及时发出报警信息；

D. 系统报警指系统可以通过接口将报警信息传输到其他系统，已使其他系统对该客户采取规避风险措施；

如下图所示：

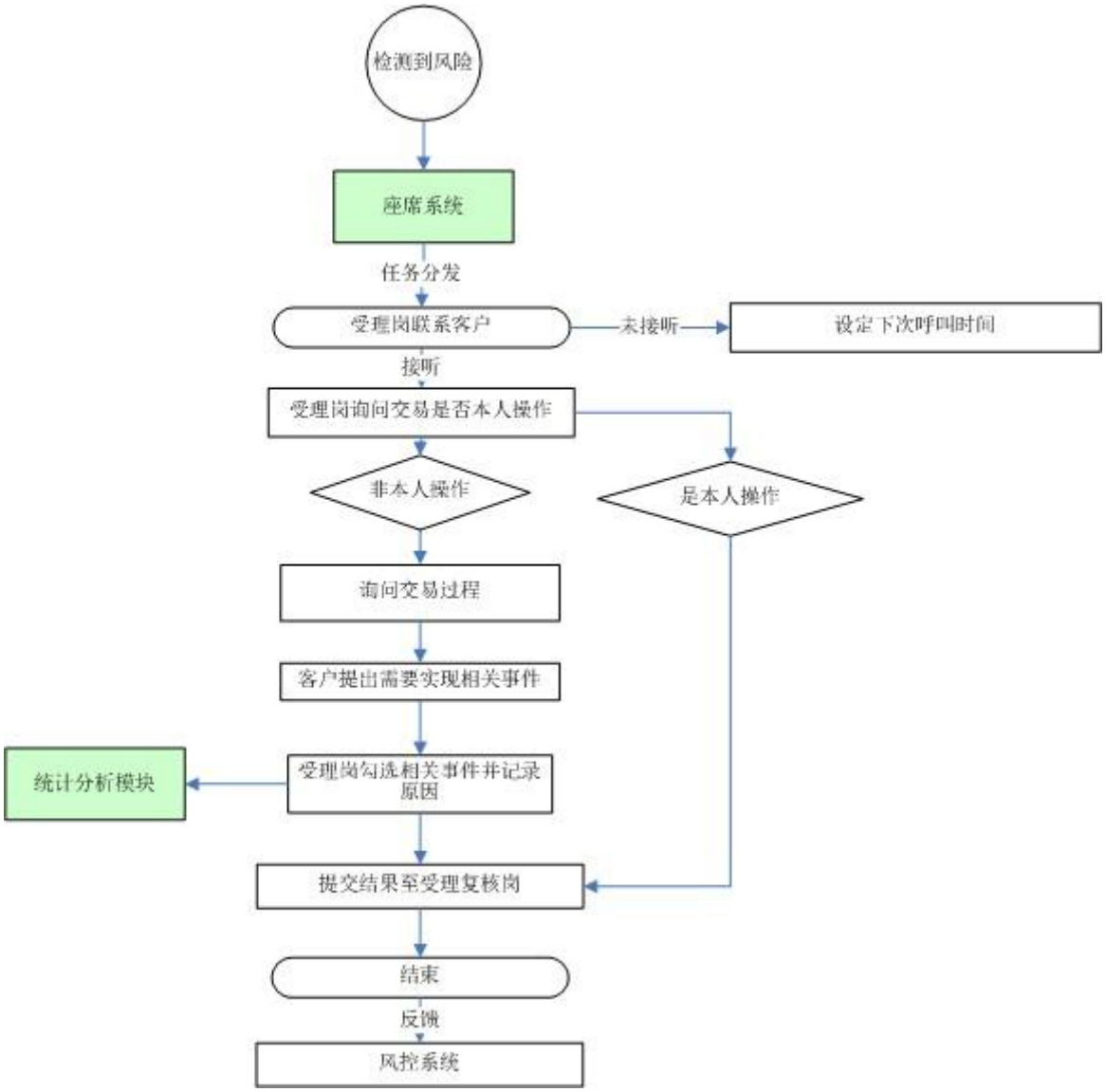


对于列表中的风险事项，根据跟踪评判规则确定是自动评判跟踪，还是由手工进行评判跟踪。在跟踪中检测到异常情况，根据设置的报警规则所检测到的不同类型进行预警，分为短信报警、邮件报警、系统报警等。

2.可疑交易处理

（1）风控人工处理流程

监控到风险后通知座席系统，后者进行任务分发，受理岗联系客户，如果未接听则设定下次外呼时间，如果接听则询问是否本人操作，如果是本人操作则提交结果至复核岗，否则询问交易过程，并记录相关原因，反馈结果。如下图所示：



（2）风险审核

风险分析员通过对风险识别出的可疑风险事件相关数据的分析，如账户属性，交易明细，风险事件关联性等， 对风险事件进行认定，并提出合理的处理意见。风险认定的结果会通过工单流转到下一个流程　风险审核。

风险审核员负责对风险认定的结果进行复核，如果复核不通过，

风险事件将被发还到风险分析人员进行再次认定。如果复核通过，风险认定的分析结果将被记录如风险管理系统数据库。

业务人员可以对风险事件进行整理分析，归纳总结出典型案例。业务人员也可以补录入从其他途径获取的相关案例，如同业典型案例。在案例生成时，业务人员需要确定案例中的典型要素，并提供业务解决方案。业务人员也可以通过分析对现有的案例提出修改/删减意见。

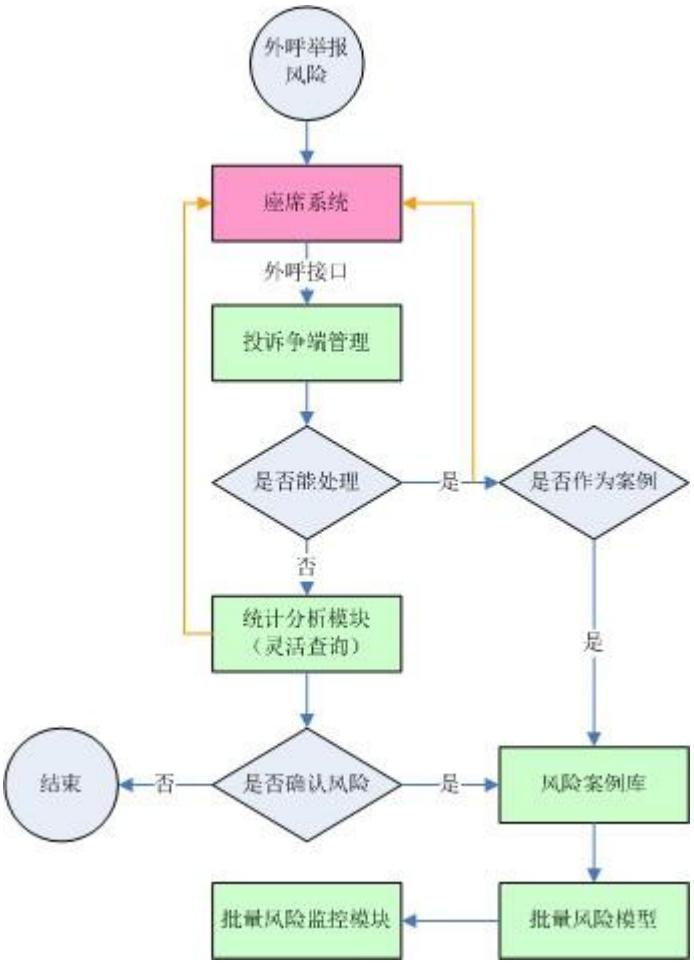
案例审核人员对案例分析中提出的案例增加，修改，删除等进行复核。

业务人员可以根据风险类型，案例名称，交易类型，规则，风险等级等对案例进行查找。

所有的案例数据信息将被存储在案例库中。业务人员可以根据权限对案例进行查询，添加，补录，修改，删除。

（3）用户投诉交易处理流程：

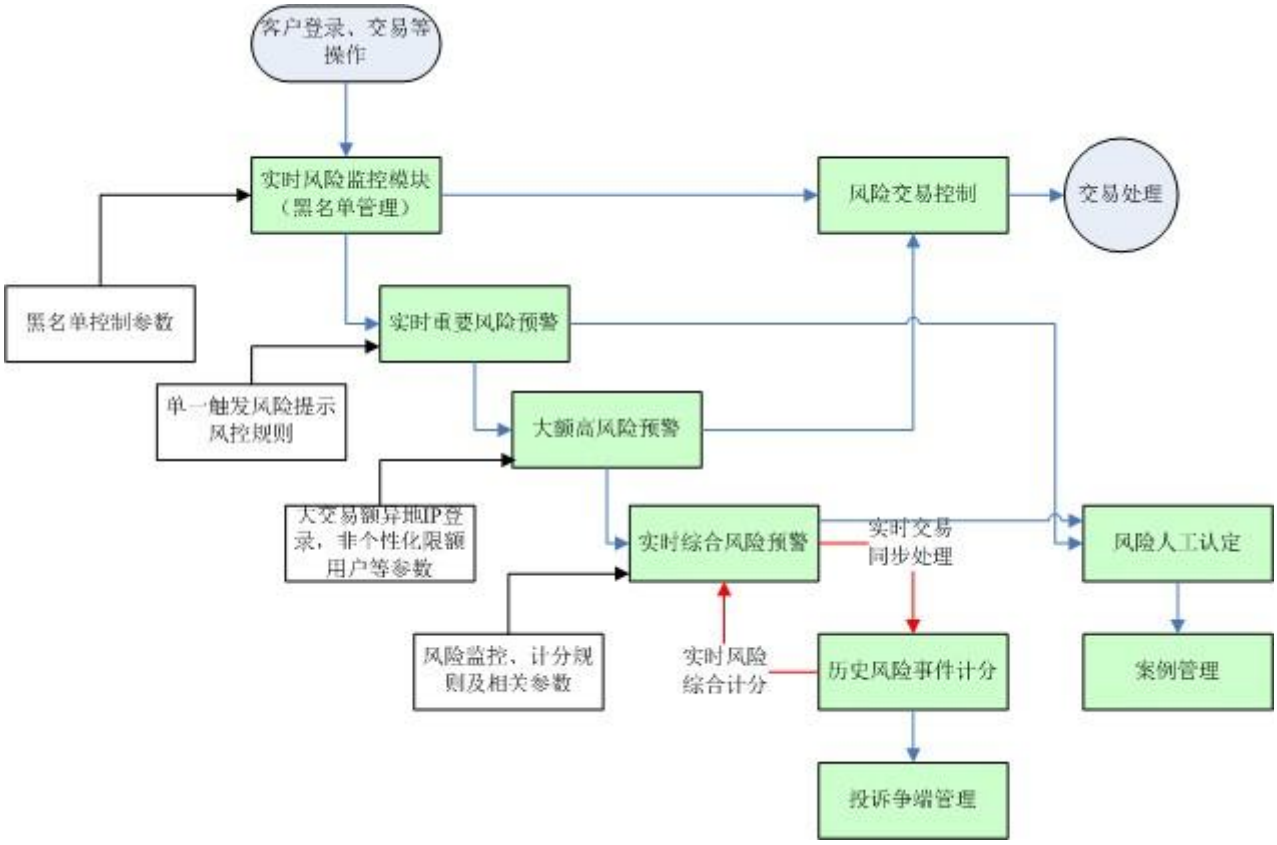
当客户通过外呼进行风险投诉或举报时，座席系统通过外呼接口进入投诉争端管理模块，给出能否处理的判断，如果能够处理，判断是否将举报的风险作为案例，从而进入到案例库，如果投诉争端管理模块不足以处理，则进入统计分析模块，通过灵活查询等功能识别是否确实存在争端或者是风险，如果确认没有风险，则对该次风险举报结束，如果确认风险，则进入风险案例库，通过对案例的分析提炼出批量风控模型， 并将其作为风险监控模块的输入的结果根据实际情况进入案例管理模块共后续批量分析。如下图所示：



（4）风控模型内部处理流程：

当客户远程登录并交易时，实时风险监控模块根据黑名单控制参数进行处理，如果发生问题，则通过风险交易控制进行处理；根据单一触发风险提示风控模型进行实时重要风险预警，传到风险人工认定进行处理；根据大交易额异地 IP登录，非个性化限额用户等参数进行大额高风险预警，如果符合规则，通过风险交易控制进行处理；根据风险监控、计分规则及相关参数进行实时综合风险预警，与历史风险事件计分进行交互，根据风险判断结果进入风险人工认定。历史风

险事件计分可以用于处理投诉争端管理，如根据不同的计分分配到不同级别的座席。风险人工认定的结果根据实际情况进入案例管理模块共后续批量分析。



（四）对合规风险的管理

为了保证非金融机构支付业务的健康、快速发展，中国人民银行逐步出台各类政策法规规范行业发展。在互联网业务发展过程中，需要不断加大对支付行业的研究力度，遵守各项法律法规，规避政策风险，以依法运营为基本原则，以部门及人员建设为基石，以完善风险

管理体系为可持续发展方向，稳步开展支付服务工作。

严格按照《非金融机构支付服务管理办法》及其他企业法的相关规定，在法律规定范围内实施开展工作。如按办法规定存放使用客户备付金、在核准业务范围内经营、及时报送相关资料等。同时精心研究办法的相关规定，在制定各种决策前首先参考相关法律法规。

成立公司专业的风险部，下设有内控与反洗钱管理和法务管理，主要对公司法律风险进行管控，包括决策的合法性分析、合同管理、人员培训、合规性监控、监督公司在反腐倡廉及代理诉讼、仲裁、复议、调解等；

从公司发展的战略性和全局性着眼，有计划、有步骤地进行法律风险管理体系建设和完善。以国家政策为导向，合法合规及预防为主、动态调整和综合治理为原则，不断提高公司法律风险管理的核心竞争力，为公司实现新的目标保驾护航。

互联网业务除了面临各项政策风险的监管外，还需要受到《中华人民共和国反洗钱法》、《中华人民共和国刑法》等法律的监管。互联网业务主要面临的法规风险包括洗钱与恐怖融资风险和套现风险、客户权益保障合规风险。

1.洗钱与恐怖融资风险

在当前经济全球化、资本流动国际化的情况下，洗钱活动对国际金融体系的安全、对国际政治经济秩序的危害极大。在国内，网上支付越来越普遍，犯罪分子利用金融系统进行洗钱交易将越来越容易，而对此类违法行为的监控和发现也越来越难。因此，增加非金融机构洗钱风险的相关防范已成当务之急。根据《中华人民共和国反洗钱法》中对反洗钱的规定、刑法第一百九十六条关于信用卡透支的规定及

《非金融机构支付服务管理办法》中对非金融机构从事支付服务的相关规定，在反洗钱风险防范方面主要工作重点如下：

（1）成立合规与反洗钱委员会

（2）建立反洗钱内部控制制度

（3） 未来将建设反洗钱实时监控系统

2.套现风险

信用卡违规套现一直是第三方支付关注的热点。正常的取现一般情况下并无危害也不会违反相关法律法规，但如果套现后不及时还款，或者借用别人的身份证办理信用卡，恶意刷卡消费和套现，就会触犯法律，而且可能为洗钱等不法行为提供便利条件。套现的社会危害范围广，影响大：一、严重扰乱金融秩序；二、增加银行信用卡业务的风险；三、存在合规风险隐患；四、存在客户信息资料被盗风险，而且可能影响个人信用记录。为此互联网业务在防套现方面采取以下几项防范措施：

（1）控制提现及信用卡消费限额

（2）增强对相关可疑套现行为的系统监控

（3）收取一定手续费、加大套现成本

客户权益保障合规风险

加强预付资金管理，维护用户合法权益，是防范金融风险的重要手段，必须引起足够重视，用于未来支付需要的预付资金，不属于发卡人的自有财产，互联网支付公司不得挪用、挤占。有如下防范措施：

（1）在商业银行开立备付金专用存款账户存放预付资金，并与银行签订存管协议，接受银行对备付金使用情况的监督。

（2）健全商业互联网收费、投诉、保密、赎回、清退等业务管理制度，全面维护用户合法权益。

对操作风险的管理

操作风险是由于内控制度建设不完善、各种主观违规、操作失误、操作程序遗漏或忽略、业务流程设计不合理、开发战略不合理、业务中断、系统失灵、交割及流程管理不完善等原因引起的。随着非金融机构支付业务进程的加快，互联网业务规模的不断扩大，及支付范围的拓展和支付产品的日趋复杂，操作风险管理将越显重要。为了规避、防范和减少操作风险事故的发生，建立科学合理的操作风险管理监管体系、以及根据不同类型的操作风险，制定相应的规避措施已成为当务之急。

根据《巴塞尔协议》、《商业银行操作风险管理指引》和《非金融机构支付服务管理办法》，并结合互联网业务在操作风险管理中的现实问题，操作风险防范主要从人员因素、内部流程、系统运行、外部事件四方面着手。

人员风险

操作风险管理中因人员因素引发的风险，主要包括内部欺诈、失职违规、知识/技能匮乏、操作失误、违反用工法律等。为了防范上述情况的发生，采取如下防范措施：

（1）建立健全公司内部控制管理制度及内部审计制度

（2）建设良好的操作风险文化环境

（3）提高员工职业道德修养，强化风险意识

（4）建立操作审批、权限分级及双重复核机制

流程风险

操作风险管理中因内部流程引发的风险，主要包括内部流程不健全、流程执行失败、控制和报告不力、产品设计缺陷、错误监控/报告等。为了防范上述情况的发生，采取如下防范措施：

（1）制定和健全操作风险流程，提高流程执行力

（2）通过操作系统固化流程，各流程按序执行

（3）建立风险事件上报机制，保证流程的更新完善

系统风险

操作风险管理中因系统缺陷引发的风险，主要包括数据/信息质量、违反系统安全规定、系统设计/稳定性运行的风险等。随着互联网业务不断发展，服务用户的不断增加及产品的多样性，并发服务不断扩充，存储数据不断增长等的影响，给互联网业务的技术运营带来更大的挑战。为了规避各种系统风险，互联网业务建设了一整套技术措施：

（1）建设、维护基础设施及硬件系统

（2）建立完善的操作风险系统，包括损失数据库、关键风险指标等

（3）建设先进完善的规避操作风险的技术措施

a) 应用系统稳定：通过系统自动进行应用系统运行状态的监控及网络安全的监控以保证应用系统稳定。同时依照《非金融机构支付服务管理办法实施细则》的要求，建立同城应用级备份设施，以提高灾难恢复处理能力。

b) 系统运行安全：主要从防钓鱼（充值防钓鱼、支付防钓鱼、系统内部防钓鱼）、账户安全（密码错误次数限制及锁定机制、

双重密码因子控制、账户资金变动短信通知机制)、病毒和恶意攻击方面的防范入手。

c) 网络安全：计算机系统安全性方面主要措施为网络连通性监控、网络负载监控等；通信设备和通信线路安全主要通过防火墙、 iGuard防篡改等进行防范；

d) 信息（传播）安全采用备份机制，主要从防篡改、防泄漏，保护完整性、数据的不可否认性等方面重点把控；

（4） 培养与储备业务与技术兼备的高级人才

外部事件风险

外部事件方面的风险主要包括因外部欺诈、自然灾害、外围系统等原因引发的风险。随着互联网业务的迅速发展，欺诈手段的高科技化，外部欺诈已成为对业务影响较大的外部风险。采取如下防范措施：

（1） 建立自然灾害预警体系、应急处理预案及演练计划

（2） 加强外部监管，构建统一的欺诈风险管理平台

（3） 完善平台系统的安全运行

对声誉风险的管理

第三方支付公司的可持续发展离不开良好的声誉，声誉是其发展的生命线。支付行业具有独特的声誉依赖性。 立誉难、毁誉易 ，只有具备良好的声誉和杰出的服务才能有忠实的客户和优秀的人才，才能形成业务发展的良性循环。为企业赢得良好的声誉，不仅需要高层领导的重视，公司规章制度的要求，更需声誉风险管理文化的培养。互联网业务主要通过行业自律、维权、协调及宣传等方式维护公司的良好声誉。

风控规则管理

序号	筛选逻辑	参数	风险描述
1	连续 3个月中有 2个月，且每月累计充值额 >=上限 * 天数 *80%的账户	连续 60天 累计风险充值额 >20000元 (可配置）	充值额异常
2	连续 3个月中有 2个月，且每月累计充值笔数 >=上限 *天数 *80%笔数的账户	连续 60天 累计风险充值笔数 >8笔 (可配置）	充值笔数异常
3	7个自然日内进行 5笔（含）以上且单笔充值额 >=账户额度 *80%的交易	连续 3天 (1<=N<=7) 累计连续充值金额 >2000元 (可配置）	连续大额交易
4	7个自然日内进行 5笔（含）以上且单笔消费额 >=账户额度 *80%的交易	连续 3天 (1<=N<=7) 累计连续消费金额 >2000元 (可配置）	连续大额交易
5	>=5张银行卡向同一个账户充值	连续 3天 (1<=N<=7) (可配置）	多充一账户
6	1小时内 同账户发生充值交易 笔数 >=2 且 IP显示为异地	时间 1<=小时（可配置） 笔数 >=2（可配置）	异地检测

风险等级	触发条件	措施	备注
初	击中逻辑序号 1、2、3、4、5、6 中任意 1个逻辑	安全通知（安全邮箱 / 绑定手机）	
中	击中逻辑序号 1、2、3、4、5、6 中任意 2 4个逻辑	临时冻结 加入黑名单	
高	击中逻辑序号 1、2、3、4、5、6 中任意 5个（含）以上逻辑	永久冻结 加入黑名单	
拒绝交易类型	行为	措施	备注
金额	单笔充值 /消费 >=5000元（可配置）	系统自动拒绝	
	单日累计充值 /消	系统自动拒绝	

	费 >=10000元 （可配置）		
	当月累计消费 >=100000元（可配置）	系统自动拒绝	
频率	单日累计消费次数 >=6次（可配置）	系统自动拒绝	

黑名单管理	永久冻结	临时冻结	备注
恢复条件	击中上述逻辑中任意 5个（含）以上的账户，永不从黑名单中删除	击中逻辑序号 1、2、3、4、5、6 中任意 2 4个逻辑，且后续连续 6个月未击中黑名单筛选逻辑的账户，从黑名单中剔除	

（五）商户管理制度

第一章 总则

第一条、 为规范公司商户管理工作，实现公司制度化和规范化，根据《中华人民共和国民法通则》、《中华人民共和国合同法》、《电子支付指引 (第一号)》及其他相关法律和法规，结合公司实际情况，制定本制度。

第二条、 本制度所称商户是指与我司签约的企事业单位、个人或其他组织。

商户管理工作是指公司对签约商户在签约、接入、交易监控管理等活动中进行的工作。通过系统化、规范化的方法，防范风险，促进公司治理，帮助公司实际各项既定目标。

第三条、 商户管理工作的组织机构

公司商户管理工作由公司风险委员会负责，由风险合规部负责具体工作，依照国家法律、法规和有关政策、公司规章制度，协调公司各部门配合执行。

第二章 商户签约

第四条、 支付账户实行实名制，签约主体必须为行政事业单位、企业、个人，签约时需提供相应资质复印件。

我司将对商户提供的居民身份证及各项企业资质进行校验审核，未通过校验审核的用户不能享受我司提供的各项服务，审核结果将记录在《商户非现场检查表》中。

同一身份证号码签约注册多个支付账户的，其第一次签约注册成功的支付账户为其主账户，后续其他账户自动关联至主账户下；

第五条、 商户签约时应认真填写各项甲方信息，且需要设置一个银行结算账户作为该商户账户的关联账户，银行结算账户名需与有效身份证件或其它有效注册证明文件上记载的名称一致。

第六条、 商户签署《支付服务协议》时，企事业单位商户应由加盖公章，并由法定代表人签字，如委托他人代签，该单位需同时提供授权委托书；个人商户应签字。

第七条、 电子协议商户在网站注册并上传资质，由风险部负责审

核商户填写的各项注册信息、资质、网站经营内容等，并回复商户是否予以开通服务。

第三章　商户管理

第八条、 我司在商户接入前对商户网站经营内容及相关资质进行审查，确保商户业务合规；

1、审查协议中的甲方信息及甲方网站经营内容，存在下列情况将不予接入：

a商户网站不能正常访问的，不予接入；

b商户经营内容涉嫌违法违规的，不予接入；

c商户经营内容为色情、赌博、私服等业务的，不予接入；

d商户网站需注册才能访问的，需商户提供测试账户，不能提供测试账户的，不予接入。

2、审查商户在协议及商户管理后台中预留的联系方式，如联系方式虚假，则暂停接入，联系销售经理重新提供有效联系方式后再接入。

3、商户提供的资质不符合《商户签约资质要求》的，不予接入。

4、对于资质不全的商户，只开通测试服务，不提供结算、转账、提现等业务，商户自开通测试服务之日 2周内不能补齐所需资质的，到期关闭测试服务。

第九条、 商户需要在正式合作前对我司服务进行测试的，可申请开通商户测试服务，但不可做结算、转账和提现。

第十条、 我司向商户提供数字证书及手机动态验证服务，确保交易已获得充分授权，商户可自由选择使用上述服务。

第十一条、 我司将严格履行对商户的各项注册信息及交易信息的保密义务，未经法律或商户授权，我司将拒绝向任何人透露商户信息，商户所提交的注册信息及交易信息仅用于我司对商户的服务。

第十二条、 商户发现自身未按规定操作，或由于自身其他原因造成支付指令未执行、未适当执行、延迟执行的，应在 1日内通知我司，我司将积极调查并告知客户调查结果。

第十三条、 我司发现因商户原因造成支付指令未执行、未适当执行、延迟执行的，将主动通知商户改正或配合客户采取补救措施。

第十四条、 我司定期人工核查可疑交易，商户发生违法违规业务的，我司将立即暂停提供支付服务，将可疑交易信息报送中国人民银行，并要求商户在 3日内提供合法有效的交易证明材料；交易证明材料通过审核的，我司将继续提供支付服务。

第十五条、 我司发现商户真实交易网址与签约网址不符的，由销售经理通知商户进行网址变更，商户自通知之日起 7日内未完成变更的，我司将暂停提供支付服务。

第十六条、 我司发现商户交易金额与实际业务类型不匹配，存在较大风险的，将列为关注类商户，持续关注达到 15日的，将转交公司反洗钱部门进行处理。

第十七条、 我司发现商户交易金额短时间内发生大幅放大的，列为关注类商户，持续关注达到 15日的，将转交公司反洗钱相关部门进行处理。

第十八条、 我司发现发现商户经营色情、赌博、私服业务的，立即关闭商户支付服务，终止协议，发送商户关闭通知书，涉嫌洗钱的将转交公司反洗钱部门进行处理。

第十九条、 我司发现发现商户交易中包含信用卡套现交易时，我司将立即向商户发送整改通知书，警告商户守法经营，并冻结套现资金 60天；若 60天内该商户仍发生套现交易，则关闭支付服务，终止协议，发送商户关闭通知书。

第二十条、 当发生国内信用卡持卡人对交易提出拒付时，我司将配合银行要求商户提供真实交易材料，商户未能按时提供或提供材料未获得银行及持卡人认可时，该笔交易的损失由商户全额承担。

第二十一条、 商户在 90日内发生两起以上（不含两起）拒付交易时，我司将立即向商户发送整改通知书；若 60天内该商户仍发生拒付交易，则停止提供支付服务，终止协议，向商户发送关闭通知书。

第二十二条、 商户账户的资金来源仅限于本人自关联的银行账户转入及通过交易产生的款项；商户账户的账存资金可向商户设定的结算银行卡转出，并可向其他账户转出。

第二十三条、 风险合规部每月定期维护网址黑名单列表，系统实现黑名单内网址拒绝提供支付服务。

第四章 商户信息变更

第二十四条、 商户签约主体不允许进行变更，但企业名称变更或企业合并分立的情况除外（需提供工商局颁发的企业名称变更准许书或新营业执照）。

第二十五条、 商户账户的登录名、显示名称、联系方式、接入网址、结算周期等信息可由商户自行登入商户管理后台进行修改。

第二十六条、 商户银行账户名不允许变更，但企业名称变更或企业合并分立（需提供工商局颁发的企业名称变更准许书或新营业执照）的情况除外。商户变更开户行、账号信息的，可由商户自行登入商户管理后台进行修改。

第二十七条、 风险预存期的变更审批由产品线、财务部、风险合规部审批，交易平台类商户风险预存期不做调低。

第二十八条、 商户登陆名称、密码遗失或需要重置的，商户可通过找回或重置；商户账户被盗或因其他原因需要挂失账户或暂停账户

支付服务的，应由商户本人向我司提出书面申请，我司在收到书面申请并确认商户身份后，实时办理。

第二十九条、 商户需要注销账户的，应由商户本人向我司提出书面申请，我司收到申请并核实后，对商户账户内的剩余资金做清算，清算资金仅可转入商户关联的银行账户，清算完成后将立即注销商户的支付账户，注销后账户不可恢复。

第五章 商户合同管理

第三十条、 商户合同管理工作由风险合规部合同小组负责，设置专职合同管理员，商户合同保存在合同室，除合同管理员外其他人员不得进入合同室。

第三十一条、 合同管理员负责将每日签署的商户合同登记台账，并归档。

第三十二条、 合同管理员应遵守保密制度，不得向无关人员泄露合同档案内容。

第三十三条、 借阅合同档案材料要履行借阅手续，双方当面交点清楚，归还时要注意检查并注销，合同原件不外借。

第三十四条、 公司员工借阅合同的，需提出书面申请，由其部门主管及合同管理部门主管签字同意后，方可到合同管理员处办理借阅手续。

第三十五条、 商户合同及资质保存期限为五年，纸质协议商户以纸质形式保存，电子协议商户以电子信息形式保存。

第六章 附则

第三十六条、 本制度自颁布之日起实行。

第三十七条、 本制度由风险合规部负责解释与修订。

（六）商户准入签约制度及流程

第一条　签约商户范围

1、互联网支付业务应用范围为实名制的行政事业单位、企业、个人；

2、对于无卡支付业务，签约商户的范围是实名制企事业单位，并且商户应符合下列条件：

（1）3C行业及金融服务类商户在与商户合作前，需由销售总监进行审批，并与风险部门一同进行评估后视情况开放；

（2）签约商户必须需正常营业 2年以上，同时，注册资金在 500万以上，如有特殊商户需由销售总监批复是否可开通；

（3）无行业资质的企业必须由销售总监实地拜访，拍摄三张营业场所照片，销售总监可批复是否开通，再由风险部门批复；

（4）严禁杜绝商户使用他人公司资质办理开通境内银行卡收单业务，销售总监监督执行。

第二条　签约商户提供的资质

1、个人商户须提供签约本人身份证复印件（正反面并由其本人签名）

2、企事业单位商户须提供：

（1）企业营业执照副本复印件（已办理年检，并加盖企业公章）；

（2）法定代表人身份证复印件（正反面并由其本人签名）；

3、对于无卡支付业务，签约商户除提供第二条第 2款中的资质外，还须提供：

（1）企业税务登记证；

（2）企业组织机构代码证；

（3）根据商户经营范围的不同类别，应提供下列行业资质：

a. 电信类行业、汽车租赁、医疗健康、移民留学、火车票、金融服务、教育等行业需要提供相应的行业资质；

b. 3C行业提供 3C认证；

c. 航空公司及代理提供代理人资质；

d. 旅行社 /酒店提供旅行社经营许可证 /特种行业许可证。

4、成功签约后，商户每年需在国家规定的证照年检截止后 30日内向公司递交经过国家年检的新证件副本复印件一份。

第三条　签署协议

1、商户填写《支付服务协议》中甲方信息中的相关内容；

2、协议应由商户盖章（仅限公章）及法定代表人签字，如是委托人代签的，需同时提供授权委托书及受委托人身份证复印件。

第四条 流程

1、收到相关材料后，我司将对商户提供的居民身份证及各项企业资质进行校验审核，未通过校验审核的用户不能享受我司提供的各项服务，审核结果将记录在我司《商户非现场检查表》中。对于商户信息真实合法、资质及协议齐全的商户予以接入，开通支付服务。协议经我司签字盖章后一份存档，一份回寄给商户。

2. 审核中发现商户联系方式有误或虚假的，暂停接入，并要求商户提供真实有效的联系方式后予以接入。

3. 电子协议商户在我司网站注册并上传资质，由风险合规部负责审核商户填写的各项注册信息、资质、网站经营内容等，并回复商户是否予以开通服务。

4. 对于资质不全的商户，只开通测试服务，不提供结算、转账、提现等业务，商户自开通测试服务之日 2周内不能补齐所需资质的，到期关闭测试服务。但电话支付、委托结算、无卡支付、提现、转账等业务不开通测试服务。

（七）商户违规整改制度及流程

第一条、 商户应遵守国家机关制定的银行卡相关法律、法规、规章以及银联规则，接受我司的业务监督和检查指导，若发现商户出现下列情形之一且情节比较轻微的，我司将给予商户书面警告通知，暂停对此商户提供支付服务，并责令其在 3个工作日内提供合法有效的交易证明材料或改正相关违规行为：

1、交易中存在过多交易纠纷及持卡人投诉；

2、进行虚假交易、套现等违法经营行为，情节比较轻微的；

3、超出约定的经营范围使用我司产品的；

4、真实交易网址与签约网址不符的；

5、交易金额与实际业务类型不匹配，存在较大风险的；

6、在 90日内发生两起以上（不含两起）拒付交易时；

7、未按约定的时间缴纳相关费用的；

8、采集、截取、盗用消费者或用户（即持卡人）的银行卡或非银行卡账号及密码等信息的；

9、代消费者、用户或任何第三方提交订单或发出任何指令的；

10、未按照约定的流程及方式受理业务的；

11、其他违反《服务协议》的行为，情节比较轻微的。

第二条、 对于提供合法有效的交易证明材料及整改成功的商户，我司将继续提供支付服务，并将此商户列为关注商户，对此商户的交

易进行重点关注与监测。

第三条、 商户未在规定的期限内改正或经我司两次通知后仍不改正的，我司有权关闭商户支付接口，单方解除与该商户的合作。

第四条、 商户违规行为涉嫌洗钱行为的，将转交公司反洗钱部门进行处理。

第五条、 商户违规行为被司法部门追溯的，我司配合司法部门对商户资金冻结并配合进行司法追究。

（八）商户强制解约制度及流程

第一条、 商户需要终止支付服务时，应由商户本人向我司提出注销我司户的书面申请，我司收到申请并核实后，对商户我司账户内的剩余资金做清算，清算完毕后注销商户的我司账户，注销完成后账户不可恢复。

第二条、 我司发现商户出现下列情形之一且情节严重的，我司有权单方面通知商户后关闭支付服务，终止合作，发送商户关闭通知书，并将此类商户列入网址黑名单列表中：

1、交易中存在过多交易纠纷或过大的交易风险，经与我司协商无法解决；

2、交易涉嫌从事诈骗、洗钱、赌博、私服、传播淫秽色情等违法犯罪活动的；

3、无理拒绝受理消费者、用户使用我司的支付产品进行支付的；

4、未通过网站提供真实有效的联系方式，或发生业务变更、终止等情况而未及时通知我司，我司在 7天之内也无法联系到商户；

5、银行、电信或行政、司法等部门出具了要求终止商户交易的书面通知；

6、被工商部门注销登记、吊销营业执照；由于违反国家法令、法规或相关行业管理规定，被有关机构查处；

7、经营不善，停业整顿、申请解散或申请破产以及停业或破产；

8. 未按照约定向我司相关费用，经我司催告后仍未支付的；

9. 因自身行为严重影响我司声誉或给我司造成重大经济损失；

10. 其他违法法律法规、监管规定及中国银联商户风险管理规定的情形。

第三条、 商户存在违法交易需要进行追溯时，我司将配合银行、司法等部门冻结商户的资金并对该商户进行追究查处。

第四条、 我司每月定期维护网址黑名单列表，系统实现黑名单内网址拒绝提供支付服务。

第五条、 商户不存在交易纠纷或司法追究的情况时，我司对商户我司账户内的剩余资金做清算，清算完毕后注销商户的我司账户，注销完成后账户不可恢复。