

支付机构互联网支付业务管理办法

(征求意见稿)

第一章 总则

第一条 为规范和促进互联网支付业务发展,防范支付风险,保护当事人的合法权益,根据《中华人民共和国中国人民银行法》、《非金融机构支付服务管理办法》等法律制度,制定本办法。

第二条 支付机构提供互联网支付服务,适用本办法。

本办法所称支付机构是指依据中国人民银行《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。

本办法所称互联网支付是指客户为购买特定商品或服务,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。

第三条 按照支付机构提供的支付服务方式不同,互联网支付分为银行账户模式和支付账户模式。

银行账户模式是指付款人通过支付机构向开户银行提交支付指令,直接将银行账户内的货币资金转入收款人指定账户的支付方式。

支付账户模式是指付款人直接向支付机构提交支付指令,将支付账户内的货币资金转入收款人指定账户的支付方式。

第四条 支付机构开展互联网支付业务,应拥有并运营独立、安全、可靠的支付业务处理系统,该系统及其备份系统的服

务器应设置在中华人民共和国境内。

第五条 支付机构应当遵循“了解你的客户”原则，建立健全和执行客户身份识别制度。

第六条 支付机构不得为客户提供账户透支、现金存取和融资服务。

第七条 支付机构应按照中国人民银行相关规定，履行反洗钱和反恐怖融资义务。

第八条 支付机构应遵循安全、效率、诚信和公平竞争的原则，为客户提供可靠、便捷的互联网支付服务，对提供互联网支付服务中获取的客户身份信息和交易信息予以保密。

第九条 支付机构开展互联网支付业务，应建立有效的业务管理制度、内部控制制度和风险管理制度。

第十条 支付机构开展互联网支付业务，应遵守相关法律制度，不得损害国家利益、社会公共利益和客户合法权益。

第二章 支付账户管理

第十一条 支付账户是指支付机构根据客户申请，为客户开立的具有记录客户资金交易和资金余额功能的电子账簿。

根据账户开立主体不同，支付账户分为单位支付账户和个人支付账户。

单位支付账户是指客户凭机关、团体、部队、企业、事业单位、其他组织等组织资质以单位名称开立的支付账户；个人支付账户是指客户凭个人身份证件以自然人名称开立的支付账户。

个体工商户凭营业执照以字号或经营者姓名开立的支付账户纳入单位支付账户管理。

第十二条 支付机构应根据审慎性原则，确定开立支付账户客户的资质。

第十三条 支付账户的开立实行实名制。支付机构对客户身份信息的真实性负责。支付机构不得为客户开立匿名、假名支付账户。

第十四条 个人客户申请开立支付账户时，支付机构应登记客户的姓名、性别、国籍、职业、住址、联系方式以及客户有效身份证件的种类、号码和有效期限等身份信息，并对客户姓名、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审核。

个人支付账户单笔收付金额超过1万元，个人客户开立的所有支付账户月收付金额累计超过5万元或资金余额连续10天超过5000元的，支付机构还应留存个人客户的有效身份证件的复印件或者影印件。

第十五条 客户申请开立单位支付账户时，支付机构应登记以下基本信息：

（一）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）；

（二）可证明该客户依法设立或者依法开展经营、社会活动的执照、证件或者文件的名称、号码和有效期限；

（三）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。

第十六条 支付机构为客户开立支付账户，应与客户签订书面协议。协议内容包括但不限于：

（一）支付账户的开立、使用、挂失、止付和撤销的条件；

(二) 身份验证和支付授权方式;

(三) 客户对支付机构核验其银行账户信息和身份信息真实性的授权;

(四) 支付账户使用规则, 以及违规使用的处置和责任;

(五) 支付账户资金变动通知方式;

(六) 发现支付账户被盗用后的通知和处置方式;

(七) 客户身份信息和交易信息的保密责任;

(八) 双方的其他权利和义务。

第十七条 同一客户在同一支付机构开立多个支付账户的, 支付机构应采取有效措施确保多个支付账户为同名账户, 且多个支付账户中登记的客户基本身份信息一致。

支付机构应为同一客户建立唯一的客户身份识别号, 对该客户开立的所有支付账户进行统一管理。

第十八条 客户在同一支付机构开立的所有支付账户须关联本客户银行账户, 支付账户的名称应与该客户所关联的银行账户名称一致。

支付机构应通过有效方式, 对支付账户所关联的银行账户信息和客户身份信息进行核验。

个人客户向在同一支付机构开立的所有支付账户月累计充值金额合计小于 1000 元的, 可不关联银行账户。未关联银行账户的支付账户可用于付款、接受交易退款, 但不得用于收款。

第十九条 支付机构通过合理、有效方式确认客户真实身份并履行通知义务后, 支付账户方可生效。按规定应关联银行账户的支付账户, 支付机构应在采取有效方式验证该支付账户与银行账户为同一客户持有并至少完成一个银行账户关联后方可生效。

第二十条 客户应通过关联银行账户为支付账户充值。未关

联银行账户的，可通过非关联银行账户或经中国人民银行批准的“仅限线上实名支付账户充值”的同一支付机构预付卡为支付账户充值。

通过非关联银行账户或同一支付机构预付卡充值的，同一客户的充值金额月累计不得超过 1000 元。通过同一支付机构预付卡充值的资金仅限用于互联网支付，不得赎回。

客户不得利用信用卡透支为支付账户充值。

第二十一条 支付机构可提供银行账户模式和支付账户模式服务。

(一) 银行账户模式下，付款人银行账户向收款人银行账户或支付账户转出；

(二) 支付账户模式下，付款人支付账户向收款人银行账户或支付账户转出。

第二十二条 同一客户在同一支付机构开立多个支付账户的，支付账户内的资金可互相划转。

不同支付机构的支付账户内的资金不得互相划转。

第二十三条 客户办理充值资金退回业务时，应将支付账户内的充值未用资金按照后充先退原则，原路退回至银行账户。

第二十四条 除电子商务交易付款、公用事业缴费、信用卡还款、购买特定金融产品及交易退款外，客户支付账户内的资金应通过划转关联银行账户的方式实现资金转出支付机构。

第二十五条 支付机构应提醒客户将支付账户的资金余额保持在合理水平，不得以任何形式引导、鼓励客户在支付账户存放资金。

个人客户在同一支付机构开立的所有支付账户日终资金合计余额连续 10 天超过 5000 元、单位客户在同一支付机构开立的

所有支付账户日终资金合计余额连续 10 天超过 5 万元的，支付机构应及时提醒客户降低支付账户资金余额。

第二十六条 支付机构不得为任何单位或个人查询支付账户信息资料，不得随意冻结、扣划支付账户内的资金。国家法律法规另有规定或与客户另有约定的除外。

第二十七条 客户申请支付账户查询、挂失、止付、撤销的，应由本人向支付机构提出申请。支付机构应在确认客户身份后予以及时办理。

客户申请撤销支付账户的，应确认该支付账户项下所有款项均已结清。

第二十八条 客户的基本身份信息发生变更的，应及时通知支付机构，支付机构应在核实客户身份后予以更新。客户身份证件逾有效期的，支付机构应要求客户重新提供有效的身份证件信息，支付机构应予以核验，并按本办法规定留存有效身份证件的复印件或影印件。

第二十九条 客户或支付机构发现支付账户被盗用的，应按双方约定的方式和程序及时通知对方，并按约定进行处理。

第三十条 客户未遵守支付账户管理规定的，支付机构应按双方协议对支付账户的使用采取限制措施。

第三十一条 支付账户只能由本人使用，不得出租、出借支付账户。

第三章 业务管理

第三十二条 支付机构为客户提供银行账户模式服务，单笔资金金额在人民币 1 万元以上的，应在提供服务前要求客户登记本人的姓名、有效身份证件种类、号码和有效期限，并通过合理手段核对客户有效身份证件信息的真实性。

第三十三条 支付机构应为支付账户提供安全可靠的密码、密钥或电子签名等身份验证和支付授权方式。客户挂失或重置密码、密钥或数字证书，支付机构应在确认客户身份后予以及时办理。

第三十四条 支付机构只能为电子商务交易、公用事业缴费、信用卡还款、购买特定金融产品或经中国人民银行批准的其他业务提供互联网支付服务。

第三十五条 支付机构要求客户提供有关资料信息时，应告知客户所提供信息的使用目的和范围、安全保护措施、以及客户未提供信息或提供虚假信息的后果。

第三十六条 支付机构提供互联网支付服务，应与客户签订书面协议。协议内容包括但不限于：

- （一）互联网支付业务的类型和基本规则；
- （二）身份验证方式和支付授权方式；
- （三）资金结算时间和方式；
- （四）向客户提供交易记录的时间和方式；
- （五）收费项目和标准；
- （六）争议及差错处理和损害赔偿 responsibility；
- （七）服务终止的情形；
- （八）双方的其他权利和义务。

第三十七条 互联网支付指令应记载下列事项：

- （一）付款人名称，银行账户账号或支付账户账号；
- （二）收款人名称，银行账户账号或支付账户账号；
- （三）确定的金额；
- （四）付款人与支付机构约定的身份验证和支付授权信息；
- （五）支付指令的发起时间；

- (六) 业务类型;
- (七) 付款人的开户银行名称或开户支付机构名称;
- (八) 收款人的开户银行名称或开户支付机构名称;
- (九) 客户有效身份证件种类和号码。

欠缺记载上述前五事项之一的，支付指令无效。

第三十八条 在支付账户模式下，支付机构应采取有效措施，在客户发出支付指令前，提示客户对支付指令的准确性进行确认。

第三十九条 客户发出的支付指令经支付机构确认后产生支付效力。

第四十条 在银行账户模式下，支付机构应及时传递、记录支付指令信息，并将结果及时通知客户。

在支付账户模式下，支付机构应在确认客户真实身份和该支付指令真实后，借记客户支付账户，记录支付指令信息，并及时将结果通知客户。

第四十一条 支付机构应建立确保支付指令被正确传递和执行的支付业务处理系统，保证支付指令的完整性、一致性和不可抵赖性。

第四十二条 由于超时、无响应或系统故障等原因无法正常处理支付指令的，支付机构应及时向客户发出提示。

第四十三条 客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，应在协议约定的时间内，按照约定程序和方式通知支付机构。支付机构应积极调查并告知客户调查结果。

支付机构发现因客户原因造成支付指令未执行、未适当执行、延迟执行的，应主动通知客户改正或配合客户采取补救措施。

第四十四条 支付机构应按照据实、准确和及时的原则处理差错交易，指定相应部门和人员负责互联网支付业务差错处理，并明确相关人员的操作权限和职责。

第四十五条 客户根据有关业务规则办理退款的，支付机构应将相应款项划回原发出支付指令的付款人账户。因付款人销户等原因而无法退回原账户的，可根据有关规定退回到付款人的同名银行账户或付款人在同一支付机构的同名支付账户。

第四十六条 支付机构应免费为客户提供上溯一年的支付信息查询服务。

第四十七条 支付机构调整互联网支付服务的收费项目、收费标准时，应通过有效方式提前 30 天通知客户。

第四十八条 支付机构提供互联网支付服务，应向客户公开披露以下信息：

（一）支付机构名称、营业地址和联系方式；

（二）所提供的互联网支付业务类型、操作规程、收费项目和收费标准；

（三）办理互联网支付业务可能产生的风险，提醒客户妥善保管密码、密钥、数字证书等警示性信息；

（四）退款规则及处理流程；

（五）争议及差错处理方法；

（六）中国人民银行规定的其他需要公开披露的信息。

第四十九条 支付机构对客户的基本信息和支付指令信息应按会计档案要求，以纸质或电子方式妥善保存，并便于调阅。

第四章 特约商户管理

第五十条 支付机构只能发展互联网特约商户。

互联网特约商户（以下简称特约商户）是指基于互联网信息

系统直接向消费者销售商品或提供服务，并接受支付机构互联网支付服务完成资金结算的法人、其他组织或自然人。

第五十一条 支付机构负责发展特约商户、发放支付插件、处理相关交易并承担相关支付风险。

第五十二条 支付机构应在付款人确认付款的当日至迟下一工作日将相应资金转入特约商户的银行账户或支付账户。

支付机构与特约商户另行约定结算时间的，从其约定。

第五十三条 支付机构不得发展以下特约商户：

（一）非法设立的；

（二）从事非法经营活动的；

（三）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。

第五十四条 支付机构应制定特约商户审批流程和审批制度，明确审批权限，指定专人负责特约商户审批工作。特约商户审批岗位不得与特约商户拓展等相关岗位兼岗。

第五十五条 支付机构发展特约商户要落实实名制，要严格审核特约商户申请材料的真实性、完整性、有效性，并留存特约商户有效身份证件影印件或复印件。对于申请材料虚假、缺失、要素不全或不合规的，不得审批通过。

对企业单位及个体工商户应至少核验营业执照、税务登记证、单位银行结算账户开户许可证、法定代表人或负责人有效身份证件。无税务登记证的企业单位及个体工商户，应出示无需办理税务登记证的证明文件或经营期间的完税证明材料。

行政事业单位和社会团体，应至少核验组织机构代码证或事业单位法人证书、法定代表人或负责人有效身份证件。

月累计销售金额高于5万元的个人商户，支付机构应予以重

点关注，必要时应采取实地调查、核验个人有效身份证件原件等更严格的风险管理措施。

第五十六条 支付机构应与特约商户直接签订收款服务协议，并将款项直接结算至双方在收款服务协议中约定的账户。支付机构和特约商户不得委托他人代理签约、代理结算。

第五十七条 支付机构应测试特约商户网店网络统一资源定位符（URL）及网络通讯地址（IP 地址）的有效性和安全性，检查站点提供的商品及服务内容、服务条款是否符合国家相关法律法规规定。

第五十八条 支付机构应尊重特约商户对支付机构的自由选择权，不得干涉或变相干涉特约商户与其他支付机构的合作。

第五十九条 支付机构应按照《金融零售业务商户类别代码》（GB/T 20548-2006）正确设置商户类别码。对同时销售多种商品和服务的特约商户，支付机构应区分经营业务的类别分别设置商户类别码。对经营业务类别相互不独立、无法严格区分的特约商户，应按照其主营业务设置特约商户类别码。不同特约商户不得共用同一商户编码。

在银行账户模式下，支付机构应在客户通过其向银行机构发出的支付指令后，准确附上标识特约商户的商户名称、商户类别码（MCC）、商户编码等特约商户基本信息。

第六十条 除自然人外的特约商户应使用单位账户作为收款账户。对使用个人支付账户和个人银行结算账户作为收款账户的特约商户，信用卡交易受理、额度和使用频率等由发卡行与支付机构根据审慎原则确定。

第六十一条 支付机构应按照收款服务协议约定为特约商户提供资金结算及对账服务，妥善、及时处理互联网支付业务产

生的差错和争议，保障客户资金安全。

支付机构应将交易的差错、退货资金，退回至原支付账户或银行账户，不得截留或退至其他账户。原账户已销户时，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本人账户。

第六十二条 支付机构应建立特约商户风险评级制度，划分商户风险等级。对风险等级较高的商户，应通过设置特约商户单笔或当日交易限额、强化交易监测、建立商户风险准备金、延迟清算等风险管理措施，防范交易风险。

第六十三条 支付机构应建立特约商户检查、评估制度。根据特约商户的风险等级，制定不同的检查、评估频率和方式，并保留相关记录。

第六十四条 支付机构不得以任何形式存储客户银行卡卡片验证码、个人标识代码（PIN）、卡片有效期以及银行交易密码，并应采取有效措施防止特约商户和外包服务机构存储银行卡卡片验证码、个人标识代码（PIN）及卡片有效期等交易验证信息。

第六十五条 支付机构为公用事业缴费、信用卡还款业务、购买特定金融产品提供货币资金代收服务的，适用本章对特约商户的管理。

第五章 风险管理

第六十六条 支付机构开展互联网支付业务采用的信息安全标准、技术标准等应符合中国人民银行关于信息安全和技術标准的有关规定。

第六十七条 支付机构为客户开立支付账户接受的备付金的存放、划转和监督，应符合《支付机构客户备付金存管暂行办法》的规定。

第六十八条 支付机构应制定全面的互联网支付风险管理

制度，设立风险管理部门或岗位，明确职责分工，建立规范、有效的风险管理体系。

第六十九条 支付机构应制定有效的应急计划、业务连续性计划和风险处理预案，并定期进行演练。

第七十条 支付机构应建立内部审计机制，定期对互联网支付业务及相关系统进行审计。

第七十一条 支付机构应采取有效安全措施保护支付指令及所附信息的安全传输，防止客户信息泄露、支付指令被篡改。

第七十二条 支付机构应采取必要措施确保支付信息的完整性和可靠性：

（一）制定相应的风险控制策略，防止支付业务处理系统发生危害支付交易数据完整性和可靠性的变化；

（二）防止支付信息在传送、处理、存储、使用中非法篡改，且任何非法篡改的行为都能被及时发现并记录。

第七十三条 支付机构对客户身份信息和支付信息等信息的使用，不得超出法律许可和客户授权的范围，并应采取必要措施为客户信息保密：

（一）客户信息须以安全方式保存和传输，并防止其被擅自查看或非法截取；

（二）对客户信息的访问应经合法授权和确认，并须登记且确保该登记不被篡改。

第七十四条 除法律法规另有规定或客户书面同意外，支付机构不得向其他机构和个人提供客户信息。

第七十五条 支付机构应确保对互联网支付业务处理系统的操作人员、管理人员以及系统服务商有合理的授权控制：

（一）确保进入账户系统等核心系统所需的认证数据免遭篡

改和破坏。对此类篡改都应是可侦测的，而且审计监督应能恰当地反映出这些篡改行为；

（二）对认证数据进行的任何查询、添加、删除或更改都应得到必要授权，并具有不可篡改的日志记录。日志记录按会计档案的管理要求进行保存。

第七十六条 支付机构采用电子签名方式进行客户身份认证和支付交易授权的，应由合法的第三方认证机构提供认证服务。

第七十七条 支付机构可根据有关规定将互联网支付业务的账户管理和业务处理等核心业务以外的业务外包给合法的专业化服务机构，但其对客户的义务及相应责任不因外包关系的确立而转移。

支付机构应与开展互联网支付外包业务的专业化服务机构签订协议，并确立一套综合性、持续性的程序，以管理其外包关系。

支付机构应确保与其签约的专业化服务机构不得从事或变相从事支付业务，但该机构取得相应支付业务许可的除外。

第七十八条 客户提供的身份信息和银行账户信息经多次验证仍未通过的，支付机构应予以重点关注，并暂停相关业务处理；支付机构发现银行账户信息或支付账户信息被盗取、欺诈、洗钱等风险事件的，应对客户采取暂停交易、限制账户使用等相关措施；对于涉嫌犯罪的，应立即向当地公安机关报案，同时向所在地中国人民银行分支机构报告。

第六章 监督管理

第七十九条 中国人民银行依法对支付机构互联网支付业务活动、内部控制、信息安全、风险状况等进行定期或不定期现

场检查和非现场检查。

第八十条 支付机构应协助配合中国人民银行及其分支机构开展现场检查及非现场检查，定期报送互联网支付业务统计报表和相关信息。

第八十一条 互联网支付业务自律组织应制定业务自律规范，通过现场检查和非现场检查等手段，督促支付机构遵守自律规范，维护市场秩序、促进公平竞争。

第八十二条 支付机构应提前 15 日向所在地中国人民银行分支机构报告如下事项：

- （一）向客户提供新的互联网支付业务产品和服务；
- （二）新增、变更收费项目、收费标准；
- （三）对客户服务规则的变更；
- （四）互联网支付业务系统停运、升级换代；
- （五）其他可能对客户、互联网支付市场产生重要影响的事项。

第八十三条 支付机构应建立互联网支付业务运作重大事项报告制度，及时向所在地中国人民银行分支机构报告业务经营过程中发生的风险事件。重大事项包括但不限于：

- （一）发现业务系统安全存在重大隐患或发现互联网支付业务系统被恶意攻击并出现 10 户（含）以上客户损失；
- （二）发生因支付机构原因导致客户或交易信息泄露等信息安全事件的，涉及客户数量在 20 户（含）以上；
- （三）发现客户利用互联网支付进行洗钱、套现且涉嫌金额较大、客户较多或已移交司法机关的；
- （四）因突发事件导致业务中止超过 1 小时的；
- （五）产生司法纠纷或舆论风波可能影响声誉的。

重大事项报告不得超出案件和事件发生后 48 小时。

第八十四条 支付机构应建立自我评估制度，定期对本机构的互联网支付业务开展、支付业务处理系统运营、风险管理、业务外包等情况进行全面评估，并每年向所在地中国人民银行分支机构提交评估报告。

第八十五条 支付机构因机构解散、依法被撤销、被宣告破产，或经中国人民银行批准终止业务的，应自解散、被撤销、被宣告破产或被批准终止业务之日起，在大众媒体、支付机构营业场所及其网站显著位置至少公告 30 日以下事项：

- （一）互联网支付业务终止原因；
- （二）互联网支付业务终止时间；
- （三）客户债权债务清算事项；
- （四）中国人民银行要求公告的其他事项。

第七章 纪律与责任

第八十六条 任何单位和个人不得使用虚假资料开立支付账户，不得利用互联网支付业务从事洗钱、信用卡套现等违法犯罪活动。

第八十七条 客户应妥善保管和正确使用支付账户及其密码、密钥或数字证书。

第八十八条 支付机构应及时为客户办理互联网支付业务，不得延压客户资金。

第八十九条 支付机构未尽审核责任，为其客户开立非实名账户，并由此造成付款人损失的，由支付机构承担相应赔偿责任。

第九十条 客户有下列情形之一的，支付机构应当停止为其提供互联网支付服务：

- (一) 使用虚假资料开立支付账户的；
- (二) 利用互联网支付从事违法犯罪活动的；
- (三) 中国人民银行规定的其他违规情况。

第九十一条 支付机构有下列情形之一的，由中国人民银行分支机构依据《非金融机构支付服务管理办法》第四十二条予以处罚：

- (一) 未建立有效的业务管理制度、内部控制制度和风险管理制度的；
- (二) 未制定有效的应急计划、风险处理预案和内部审计机制的；
- (三) 未公开披露相关信息的；
- (四) 未及时向中国人民银行及其分支机构报送信息资料的。

第九十二条 支付机构有下列情形之一的，由中国人民银行及其分支机构依据《非金融机构支付服务管理办法》第四十三条予以处罚：

- (一) 未按本办法规定使用、止付、撤销支付账户或为支付账户关联非本人银行账户的；
- (二) 未经客户授权擅自将客户信息发送银行验证的；
- (三) 运营的支付业务处理系统及其备份系统的服务器未按规定设置在中华人民共和国境内的；
- (四) 未按本办法规定记录、保存、使用客户身份信息和支付信息的；
- (五) 未按本办法规定处理互联网支付业务差错的；
- (六) 违反本办法的其他行为。

第九十三条 支付机构未按实名制原则为客户开立支付账

户和发展特约商户的，由中国人民银行及其分支机构依据《非金融机构支付服务管理办法》第四十四条予以处罚。

未取得互联网支付相关业务资质，擅自或变相开展互联网支付业务的，由中国人民银行及其分支机构责令终止其互联网支付业务；涉嫌犯罪的，依法移送公安机关立案侦查；构成犯罪的，依法追究刑事责任。

第八章 附则

第九十四条 本办法由中国人民银行负责解释和修订。

第九十五条 本办法自发布之日起实施。