

《非银行支付机构网络支付业务管理办法》条款释义

条款	释义
第一章 总 则	
<p>第一条 为规范非银行支付机构（以下简称支付机构）网络支付业务，防范支付风险，保护当事人合法权益，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》（中国人民银行令〔2010〕第2号发布）等规定，制定本办法。</p>	<p>制定本办法的目的和依据。</p>
<p>第二条 支付机构从事网络支付业务，适用本办法。</p> <p>本办法所称支付机构是指依法取得《支付业务许可证》，获准办理互联网支付、移动电话支付、固定电话支付、数字电视支付等网络支付业务的非银行机构。</p> <p>本办法所称网络支付业务，是指收款人或付款人通过计算机、移动终端等电子设备，依托公共网络信息系统远程发起支付指令，且付款人电子设备不与收款人特定专属设备交互，由支付机构为收付款人提供货币资金转移服务的活动。</p> <p>本办法所称收款人特定专属设备，是指专门用于交易收款，在交易过程中与支付机构业务系统交互并参与生成、传输、处理支付指令的电子设备。</p>	<p>一、本办法的适用范围。</p> <p>二、本办法所称支付机构的含义。</p> <p>三、本办法规范的网络支付业务，应同时具备四个基本特征：</p> <p>（一）为收付款人提供资金转移服务的主体是支付机构；</p> <p>（二）支付指令的发起借助于计算机、移动终端等电子设备；</p> <p>（三）电子设备经由公共网络信息系统与相关后台系统交互并传递支付指令。因此，支付指令发起过程中，电子设备不需与后台系统交互的支付业务不属于本办法规范范畴（例如基于手机 NFC 功能的电子现金脱机消费业务等）；</p> <p>（四）支付指令发起过程中，付款人的电子设备不与“收款人特定专属设备”交互。</p> <p>四、“收款人特定专属设备”是专门用于交易收款的电子设备，其在交易过程中</p>

条款	释义
	<p>与支付机构业务系统交互，并参与完成支付指令的生成、传输及处理。此类设备通常布放在收款人经营场所，付款人需亲临该经营场所完成支付。</p> <p>“收款人特定专属设备”具体包括POS等传统受理终端，以及可生成、读取、识别条码（二维码）、声波、光线等信息传输介质并发起交易的新型受理设备。</p> <p>五、付款人电子设备需要与前述新型受理设备进行交互的业务，目前仍处于研究和探索阶段，相关配套技术和安全标准有待根据业务实践持续检验和完善。本办法暂不将此类支付方式纳入规范范畴，以便为其留出探索和创新发展空间。人民银行将密切关注相关新型支付方式的探索和发展情况，并适时制定配套管理措施。</p>
<p>第三条 支付机构应当遵循主要服务电子商务发展和为社会提供小额、快捷、便民小微支付服务的宗旨，基于客户的银行账户或者按照本办法规定为客户开立支付账户提供网络支付服务。</p> <p>本办法所称支付账户，是指获得互联网支付业务许可的支付机构，根据客户的真实意愿为其开立的，用于记录预付交易资金余额、客户凭以发起支付指令、反映交易明细信息的电子簿记。</p> <p>支付账户不得透支，不得出借、出租、出售，不得利用支付账户从事或者协助他人从事非法活动。</p>	<p>一、支付机构应遵循《关于促进互联网金融健康发展的指导意见》（银发〔2015〕221号）所明确的网络支付服务宗旨。</p> <p>二、支付机构可以基于银行账户（例如银行网关支付、银行卡快捷支付等模式）或者支付账户提供网络支付服务。</p> <p>三、需要特别说明的是，实践中，部分支付机构开立的在途资金账户（亦称内部过渡账户、内部记账账户、中间账户等）不属于本办法所称支付账户，一般具有下列特征：</p> <p>（一）记录的余额是支付指令发起之后、执行完毕之前，客户待收或待付的在途资金金额，而不是客户的预付交易资金余额；</p> <p>（二）最多具有查询功能，客户不能凭以发起支付指令。</p> <p>四、支付账户的使用原则。</p>
<p>第四条 支付机构基于银行卡为客户</p>	<p>支付机构应当遵守的相关规定。</p>

条款	释义
<p>提供网络支付服务的，应当执行银行卡业务相关监管规定和银行卡行业规范。</p> <p>支付机构对特约商户的拓展与管理、业务与风险管理应当执行《银行卡收单业务管理办法》（中国人民银行公告〔2013〕第9号公布）等相关规定。</p> <p>支付机构网络支付服务涉及跨境人民币结算和外汇支付的，应当执行中国人民银行、国家外汇管理局相关规定。</p> <p>支付机构应当依法维护当事人合法权益，遵守反洗钱和反恐怖融资相关规定，履行反洗钱和反恐怖融资义务。</p>	
<p>第五条 支付机构依照中国人民银行有关规定接受分类评价，并执行相应的分类监管措施。</p>	<p>支付机构接受分类监管的原则性规定。本办法第五章明确了具体分类监管措施。</p>
<p>第二章 客户管理</p>	
<p>第六条 支付机构应当遵循“了解你的客户”原则，建立健全客户身份识别机制。支付机构为客户开立支付账户的，应当对客户实行实名制管理，登记并采取有效措施验证客户身份基本信息，按规定核对有效身份证件并留存有效身份证件复印件或者影印件，建立客户唯一识别编码，并在与客户业务关系存续期间采取持续的身份识别措施，确保有效核实客户身份及其真实意愿，不得开立匿名、假名支付账户。</p>	<p>一、无论基于银行账户还是支付账户提供网络支付服务，支付机构都应遵循“了解你的客户”原则，建立健全客户身份识别机制。</p> <p>二、本条款明确支付账户应实行实名制管理，并提出核实客户身份的相关要求。</p>
<p>第七条 支付机构应当与客户签订服务协议，约定双方责任、权利和义务，至少明确业务规则（包括但不限于业务功能和流程、身份识别和交易验证方式、资金结算方式等），收费项目和标准，查询、差错争议及投诉等服务流程和规则，业务风险和非法活动防范及处置措施，客户损失责任划分和赔付规则等内容。</p> <p>支付机构为客户开立支付账户的，还</p>	<p>一、本条款对服务协议所包含的内容明确具体要求，特别强调支付机构应确保客户在充分知晓并清晰理解相关权利、责任、义务的前提下自愿接受服务协议。</p> <p>二、支付账户所反映余额的本质是预付价值，类似于预付费卡中的余额，与客户的银行存款不同。该余额资金虽然所有权归属于客户，却未以客户本人名义存放在银行，而是支付机构以其自身名义存放</p>

条款	释义
<p>应在服务协议中以显著方式告知客户，并采取有效方式确认客户充分知晓并清晰理解下列内容：“支付账户所记录的资金余额不同于客户本人的银行存款，不受《存款保险条例》保护，其实质为客户委托支付机构保管的、所有权归属于客户的预付价值。该预付价值对应的货币资金虽然属于客户，但不以客户本人名义存放在银行，而是以支付机构名义存放在银行，并且由支付机构向银行发起资金调拨指令。”</p> <p>支付机构应当确保协议内容清晰、易懂，并以显著方式提示客户注意与其有重大利害关系的事项。</p>	<p>在银行，并实际由支付机构支配与控制。同时，该余额仅代表支付机构的企业信用，法律保障机制上远低于《人民银行法》、《商业银行法》及《存款保险条例》保障下的央行货币与商业银行货币。一旦支付机构出现经营风险或信用风险，将可能导致支付账户余额无法使用，不能回提为银行存款，使客户遭受财产损失。</p> <p>本条款规定支付机构应充分提示支付账户余额的本质属性和相关风险。在此前提下，由客户本着“自愿开立、自担风险”的原则申请开立支付账户。</p>
<p>第八条 获得互联网支付业务许可的支付机构，经客户主动提出申请，可为其开立支付账户；仅获得移动电话支付、固定电话支付、数字电视支付业务许可的支付机构，不得为客户开立支付账户。</p> <p>支付机构不得为金融机构，以及从事信贷、融资、理财、担保、信托、货币兑换等金融业务的其他机构开立支付账户。</p>	<p>一、未获得互联网支付业务许可的支付机构，不可为客户开立支付账户；获得互联网支付业务许可的支付机构，如客户未主动提出申请，不可为其开立支付账户。</p> <p>二、本条款基于审慎性原则，规定支付机构为金融机构和从事网络借贷、股权众筹融资、互联网基金销售、互联网保险、互联网信托和互联网消费金融等业务的机构提供网络支付服务时，不可开立支付账户，各项资金收付均应基于其银行账户办理，以对相关机构进一步明晰资金流向、加强资金监管，有效隔离跨市场风险。</p>
第三章 业务管理	
<p>第九条 支付机构不得经营或者变相经营证券、保险、信贷、融资、理财、担保、信托、货币兑换、现金存取等业务。</p>	<p>基于支付机构业务许可范围、业务专营性和审慎监管原则，本条款对支付机构的业务范围提出禁止性规定。</p>
<p>第十条 支付机构向客户开户银行发送支付指令，扣划客户银行账户资金的，支付机构和银行应当执行下列要求：</p> <p>（一）支付机构应当事先或在首笔交易时自主识别客户身份并分别取得客户和银行的协议授权，同意其向客户的银行账</p>	<p>一、“银行卡快捷支付”及类似业务，涉及客户、支付机构及银行三方，权责关系相对复杂，应以清晰、完整的业务授权为前提：一是支付机构要获得客户和银行的授权；二是银行要通过与客户直接签订协议的方式，直接获取客户授权。</p>

条款	释义
<p>户发起支付指令扣划资金;</p> <p>(二) 银行应当事先或在首笔交易时自主识别客户身份并与客户直接签订授权协议, 明确约定扣款适用范围和交易验证方式, 设立与客户风险承受能力相匹配的单笔和单日累计交易限额, 承诺无条件全额承担此类交易的风险损失先行赔付责任;</p> <p>(三) 除单笔金额不超过 200 元的小额支付业务, 公共事业缴费、税费缴纳、信用卡还款等收款人固定并且定期发生的支付业务, 以及符合第三十七条规定的情形以外, 支付机构不得代替银行进行交易验证。</p>	<p>二、银行作为客户资金安全的管理责任主体, 事先或首笔交易时应自主识别客户身份并与客户直接签订授权协议, 后续交易扣款时原则上应自主完成交易验证。银行“自主识别客户身份”、“与客户直接签订授权协议”、“自主完成交易验证”, 并不意味着客户必须跳转到银行的网页或通过银行开发的手机软件完成签约授权或者交易付款。支付机构和银行可以采用安全、有效的技术手段, 以便在银行落实上述责任的同时, 确保客户操作体验流畅和便捷。</p> <p>三、本办法允许符合条件的支付机构与银行自主约定由支付机构代替验证的具体情形, 在坚持银行承担资金管理责任、保障客户权益的基础上, 适度提高监管措施的灵活性(详见第三十七条)。</p>
<p>第十一条 支付机构应根据客户身份对同一客户在本机构开立的所有支付账户进行关联管理, 并按照下列要求对个人支付账户进行分类管理:</p> <p>(一) 对于以非面对面方式通过至少一个合法安全的外部渠道进行身份基本信息验证, 且为首次在本机构开立支付账户的个人客户, 支付机构可以为其开立 I 类支付账户, 账户余额仅可用于消费和转账, 余额付款交易自账户开立起累计不超过 1000 元(包括支付账户向客户本人同名银行账户转账);</p> <p>(二) 对于支付机构自主或委托合作机构以面对面方式核实身份的个人客户, 或以非面对面方式通过至少三个合法安全的外部渠道进行身份基本信息多重交叉验证的个人客户, 支付机构可以为其开立 II 类支付账户, 账户余额仅可用于消费和转账, 其所有支付账户的余额付款交易年累</p>	<p>一、个人支付账户分为三类。其中, I 类账户的开立仅需通过一个外部渠道验证客户身份(例如联网核查客户的身份证信息), 开户过程最为便捷。客户如果只需要进行小额、临时支付, 或者可用的网上验证身份手段较少, 可以快速开立 I 类账户并完成支付。</p> <p>二、鉴于网络支付主要服务电子商务发展和为社会提供小额、快捷、便民小微支付服务的宗旨, 本条款对支付账户“余额”付款规定了交易限额。客户使用银行账户付款(例如银行网关支付、银行卡快捷支付等)不属于本条款规范范畴, 也不受本条款的功能和限额约束。</p> <p>为兼顾便捷性和安全性, I 类账户的交易限额相对较低, 但支付机构可以通过强化客户身份验证, 将 I 类账户升级为 II 类或 III 类账户, 提高交易限额。支付机构所提供的交易数据表明, II 类、III 类账户</p>

条款	释义
<p>计不超过10万元(不包括支付账户向客户本人同名银行账户转账);</p> <p>(三)对于支付机构自主或委托合作机构以面对面方式核实身份的个人客户,或以非面对面方式通过至少五个合法安全的外部渠道进行身份基本信息多重交叉验证的个人客户,支付机构可以为其开立Ⅲ类支付账户,账户余额可以用于消费、转账以及购买投资理财等金融类产品,其所有支付账户的余额付款交易年累计不超过20万元(不包括支付账户向客户本人同名银行账户转账)。</p> <p>客户身份基本信息外部验证渠道包括但不限于政府部门数据库、商业银行信息系统、商业化数据库等。其中,通过商业银行验证个人客户身份基本信息的,应为Ⅰ类银行账户或信用卡。</p>	<p>的交易限额可以有效满足大部分客户使用“余额”付款的日常需求。</p> <p>三、客户身份信息验证渠道包括但不限于公安、社保、民政、住建、交通、工商、教育、财税等管理部门,以及商业银行、保险公司、证券公司、征信机构、移动运营商、铁路公司、航空公司、电力公司、自来水公司、燃气公司等单位所运营的,能够切实有效验证客户身份基本信息的数据库或系统。</p> <p>客户一般只需要按照支付机构的要求在网上填写并上传身份信息,由支付机构负责与相关外部数据库或系统进行连接并验证身份信息的真实性,应采用必要技术手段确保客户操作流程简便、客户体验便捷。</p> <p>四、本办法允许符合条件的支付机构运用各种安全、合法的技术手段灵活制定其他有效的身份核实方法,经人民银行评估认可后予以采用,以兼顾监管原则性和灵活性(详见第三十三条)。</p>
<p>第十二条 支付机构办理银行账户与支付账户之间转账业务的,相关银行账户与支付账户应属于同一客户。</p> <p>支付机构应按照与客户的约定及时办理支付账户向客户本人银行账户转账业务,不得对Ⅱ类、Ⅲ类支付账户向客户本人银行账户转账设置限额。</p>	<p>一、原则上,支付账户与非同名的银行账户之间不可以相互转账。但符合条件的支付机构除外(即支付账户充值和余额回提交易,既可以发生在支付账户与同名的银行账户之间,也可以发生在支付账户与非同名的银行账户之间),以便提高监管灵活性,并进一步满足客户支付需求(详见第三十五条)。</p> <p>二、客户要求将支付账户余额回提为本人银行存款时,支付机构应按照客户意愿及时、足额办理。</p>
<p>第十三条 支付机构为客户办理本机构发行的预付卡向支付账户转账的,应当按照《支付机构预付卡业务管理办法》(中</p>	<p>本条款明确支付机构基于预付卡办理网络支付业务的相关要求,对利用支付账户进行预付卡资金套现作出禁止性规定。</p>

条款	释义
<p>国人民银行公告〔2012〕第12号公布)相关规定对预付卡转账至支付账户的余额单独管理,仅限其用于消费,不得通过转账、购买投资理财等金融类产品等形式进行套现或者变相套现。</p>	
<p>第十四条 支付机构应当确保交易信息的真实性、完整性、可追溯性以及支付全流程中的一致性,不得篡改或者隐匿交易信息。交易信息包括但不限于下列内容:</p> <p>(一)交易渠道、交易终端或接口类型、交易类型、交易金额、交易时间,以及直接向客户提供商品或者服务的特约商户名称、编码和按照国家与金融行业标准设置的商户类别码;</p> <p>(二)收付款客户名称,收付款支付账户账号或者银行账户的开户银行名称及账号;</p> <p>(三)付款客户的身份验证和交易授权信息;</p> <p>(四)有效追溯交易的标识;</p> <p>(五)单位客户单笔超过5万元的转账业务的付款用途和事由。</p>	<p>交易信息的真实性、完整性、可追溯性及一致性是有效识别客户支付行为、开展风险防控、保障交易安全及维护客户权益的重要基础。本条款要求支付机构真实反映和详尽记载交易信息,并在基于银行卡的支付业务中向相关银行真实、完整、准确提供交易信息,这与《银行卡收单业务管理办法》、《中国人民银行关于加强银行卡业务管理的通知》(银发〔2014〕5号)有关规定是一脉相承的。</p>
<p>第十五条 因交易取消(撤销)、退货、交易不成功或者投资理财等金融类产品赎回等原因需划回资金的,相应款项应当划回原扣款账户。</p>	<p>交易资金的“原路返回”规定。特别地,客户购买投资理财产品需要赎回本金和收益时,支付机构应当将资金划回原扣款账户,而不可默认划至支付账户,以保证交易的可追溯性。</p>
<p>第十六条 对于客户的网络支付业务操作行为,支付机构应当在确认客户身份及真实意愿后及时办理,并在操作生效之日起至少五年内,真实、完整保存操作记录。</p> <p>客户操作行为包括但不限于登录和注销登录、身份识别和交易验证、变更身份</p>	<p>支付机构记录并保存客户各项操作的要求。</p>

条款	释义
<p>信息和联系方式、调整业务功能、调整交易限额、变更资金收付方式，以及变更或挂失密码、数字证书、电子签名等。</p>	
<p>第四章 风险管理与客户权益保护</p>	
<p>第十七条 支付机构应当综合客户类型、身份核实方式、交易行为特征、资信状况等因素，建立客户风险评级管理制度和机制，并动态调整客户风险评级及相关风险控制措施。</p> <p>支付机构应当根据客户风险评级、交易验证方式、交易渠道、交易终端或接口类型、交易类型、交易金额、交易时间、商户类别等因素，建立交易风险管理制度和交易监测系统，对疑似欺诈、套现、洗钱、非法融资、恐怖融资等交易，及时采取调查核实、延迟结算、终止服务等措施。</p>	<p>支付机构实施客户风险评级管理，以及建立交易风险管理制度和交易监测系统的要求。</p>
<p>第十八条 支付机构应当向客户充分提示网络支付业务的潜在风险，及时揭示不法分子新型作案手段，对客户进行必要的安全教育，并对高风险业务在操作前、操作中进行风险警示。</p> <p>支付机构为客户购买合作机构的金融类产品提供网络支付服务的，应当确保合作机构为取得相应经营资质并依法开展业务的机构，并在首次购买时向客户展示合作机构信息和产品信息，充分提示相关责任、权利、义务及潜在风险，协助客户与合作机构完成协议签订。</p>	<p>一、支付机构向客户及时提示风险、作好安全教育的义务。</p> <p>二、支付机构与其他机构合作开展金融类产品销售前，必须充分了解合作机构的经营资质和产品信息，并本着对客户负责的态度充分提示潜在风险。</p>
<p>第十九条 支付机构应当建立健全风险准备金制度和交易赔付制度，并对不能有效证明因客户原因导致的资金损失及时先行全额赔付，保障客户合法权益。</p> <p>支付机构应于每年1月31日前，将前一年度发生的风险事件、客户风险损失发生和赔付等情况在网站对外公告。支付机</p>	<p>一、方便、快捷的支付服务必须以保护客户权益为前提，以完善的风险准备金制度和交易赔付制度为保障。为防范支付机构盲目追求“便捷”而忽视“安全”，本条款规定了支付机构对客户资金损失的先行赔付责任。</p> <p>二、为增加支付机构信息透明度，加</p>

条款	释义
<p>构应在年度监管报告中如实反映上述内容和风险准备金计提、使用及结余等情况。</p>	<p>强社会公众和舆论监督，本条款要求支付机构定期公开披露风险信息。</p>
<p>第二十条 支付机构应当依照中国人民银行有关客户信息保护的规定，制定有效的客户信息保护措施和风险控制机制，履行客户信息保护责任。</p> <p>支付机构不得存储客户银行卡的磁道信息或芯片信息、验证码、密码等敏感信息，原则上不得存储银行卡有效期。因特殊业务需要，支付机构确需存储客户银行卡有效期的，应当取得客户和开户银行的授权，以加密形式存储。</p> <p>支付机构应当以“最小化”原则采集、使用、存储和传输客户信息，并告知客户相关信息的使用目的和范围。支付机构不得向其他机构或个人提供客户信息，法律法规另有规定，以及经客户本人逐项确认并授权的除外。</p>	<p>一、支付机构应参照《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》（银发〔2011〕17号）等规定，切实做好客户信息安全保护工作。</p> <p>二、除银行卡有效期之外的其他敏感信息，支付机构在任何情况下都不得存储；支付机构确因业务需要而存储银行卡有效期的，必须同时获得客户本人和银行的授权。</p>
<p>第二十一条 支付机构应当通过协议约定禁止特约商户存储客户银行卡的磁道信息或芯片信息、验证码、有效期、密码等敏感信息，并采取定期检查、技术监测等必要监督措施。</p> <p>特约商户违反协议约定存储上述敏感信息的，支付机构应当立即暂停或者终止为其提供网络支付服务，采取有效措施删除敏感信息、防止信息泄露，并依法承担因相关信息泄露造成的损失和责任。</p>	<p>在《银行卡收单业务管理办法》的基础上，本条款进一步明确商户不得存储客户敏感信息。特别强调支付机构应对商户采取有效措施进行检查和监督，切实防范因商户违规存储敏感信息而导致客户信息泄露或资金损失。</p>
<p>第二十二条 支付机构可以组合选用下列三类要素，对客户使用支付账户余额付款的交易进行验证：</p> <p>（一）仅客户本人知悉的要素，如静态密码等；</p> <p>（二）仅客户本人持有并特有的，不可复制或者不可重复利用的要素，如经过</p>	<p>为降低业务风险、保障客户资金安全，支付机构可以选择采用“静态密码+数字证书”、“一次性密码+指纹”、“静态密码+指纹”等多种验证要素组合方式，对支付账户余额付款交易进行验证。</p>

条款	释义
<p>安全认证的数字证书、电子签名，以及通过安全渠道生成和传输的一次性密码等；</p> <p>（三）客户本人生理特征要素，如指纹等。</p> <p>支付机构应当确保采用的要素相互独立，部分要素的损坏或者泄露不应导致其他要素损坏或者泄露。</p>	
<p>第二十三条 支付机构采用数字证书、电子签名作为验证要素的，数字证书及生成电子签名的过程应符合《中华人民共和国电子签名法》、《金融电子认证规范》（JR/T 0118-2015）等有关规定，确保数字证书的唯一性、完整性及交易的不可抵赖性。</p> <p>支付机构采用一次性密码作为验证要素的，应当切实防范一次性密码获取端与支付指令发起端为相同物理设备而带来的风险，并将一次性密码有效期严格限制在最短的必要时间内。</p> <p>支付机构采用客户本人生理特征作为验证要素的，应当符合国家、金融行业标准和相关信息安全管理要求，防止被非法存储、复制或重放。</p>	<p>一、支付机构采用的数字证书、电子签名应符合相关法律法规和技术标准。</p> <p>二、部分支付场景下，一次性密码（例如短信动态验证码）和支付指令通过同一个物理设备（例如同一部手机）处理。在设备被植入恶意程序或被盗用情况下，易造成一次性密码和支付指令同时被拦截、窃取、伪造或篡改，大大增加了交易风险。支付机构应采取有效措施对此类风险予以防范，保障客户资金安全。</p> <p>三、客户的指纹等生理特征一般相对固定，基本不发生变化，因此存在被非法窃取、存储、复制或重放的风险。支付机构采用生理特征验证交易时，应符合有关技术安全标准和要求，切实防范相关风险。</p>
<p>第二十四条 支付机构应根据交易验证方式的安全级别，按照下列要求对个人客户使用支付账户余额付款的交易进行限额管理：</p> <p>（一）支付机构采用包括数字证书或电子签名在内的两类（含）以上有效要素进行验证的交易，单日累计限额由支付机构与客户通过协议自主约定；</p> <p>（二）支付机构采用不包括数字证书、电子签名在内的两类（含）以上有效要素进行验证的交易，单个客户所有支付账户单日累计金额应不超过5000元（不包括支</p>	<p>一、为引导支付机构提高交易验证方式的安全性，加强客户资金安全保护，本条款规定，对于安全级别较高的支付账户“余额”付款交易，支付机构可以与客户自主约定限额；但对于安全级别不足的支付账户“余额”付款交易，本条款规定了单日累计限额。支付机构所提供的交易数据表明，本条款规定限额可以满足大部分客户使用“余额”付款的日常需求。</p> <p>客户使用银行账户付款（例如银行网关支付、银行卡快捷支付等）不属于本条款规范范畴，也不受本条款的限额约束。</p>

条款	释义
<p>付账户向客户本人同名银行账户转账);</p> <p>(三)支付机构采用不足两类有效要素进行验证的交易,单个客户所有支付账户单日累计金额应不超过1000元(不包括支付账户向客户本人同名银行账户转账),且支付机构应当承诺无条件全额承担此类交易的风险损失赔付责任。</p>	<p>二、本办法允许符合条件的支付机构在本条款规定的基础上适度提高交易限额,以进一步提高监管灵活性,兼顾便捷性和安全性(详见第三十六条)。</p>
<p>第二十五条 支付机构网络支付业务相关系统设施和技术,应当持续符合国家、金融行业标准和相关信息安全管理要求。如未符合相关标准和要求,或者尚未形成国家、金融行业标准,支付机构应当无条件全额承担客户直接风险损失的先行赔付责任。</p>	<p>网络支付业务依托公共网络作为信息传输通道,不可避免地面临网络病毒、信息窃取和篡改、网络钓鱼、网络异常中断等各种安全隐患。为保障客户信息安全和资金安全,本条款从技术和安全标准符合性角度对支付机构提出要求。</p>
<p>第二十六条 支付机构应当在境内拥有安全、规范的网络支付业务处理系统及其备份系统,制定突发事件应急预案,保障系统安全性和业务连续性。</p> <p>支付机构为境内交易提供服务的,应当通过境内业务处理系统完成交易处理,并在境内完成资金结算。</p>	<p>支付机构业务系统相关规定。</p>
<p>第二十七条 支付机构应当采取有效措施,确保客户在执行支付指令前可对收付款客户名称和账号、交易金额等交易信息进行确认,并在支付指令完成后及时将结果通知客户。</p> <p>因交易超时、无响应或者系统故障导致支付指令无法正常处理的,支付机构应当及时提示客户;因客户原因造成支付指令未执行、未适当执行、延迟执行的,支付机构应当主动通知客户更改或者协助客户采取补救措施。</p>	<p>本条款要求支付机构在支付指令执行之前的相关交易环节,通过向客户清晰展示交易信息、获取客户有效确认等方式,避免因收付款客户名称和账号、交易金额等信息错误而导致客户资金损失或引发争议纠纷。</p>
<p>第二十八条 支付机构应当通过具有合法独立域名的网站和统一的服务电话等渠道,为客户免费提供至少最近一年以内</p>	<p>一、本条款明确了支付机构为客户提供交易信息查询服务的最低标准,以及健全差错争议和纠纷投诉处理制度的要求。</p>

条款	释义
<p>交易信息查询服务，并建立健全差错争议和纠纷投诉处理制度，配备专业部门和人员据实、准确、及时处理交易差错和客户投诉。支付机构应当告知客户相关服务的正确获取途径，指导客户有效辨识服务渠道的真实性。</p> <p>支付机构应当于每年1月31日前，将前一年度发生的客户投诉数量和类型、处理完毕的投诉占比、投诉处理速度等情况在网站对外公告。</p>	<p>二、为防范不法分子通过仿冒支付机构网站、客服热线等手段骗取客户身份或账户信息，导致客户信息泄露或资金损失，本条款要求支付机构采取有效措施指导客户辨识服务渠道的真实性。</p> <p>三、为增加支付机构信息透明度，加强社会公众和舆论监督，本条款要求支付机构定期公开披露客户投诉相关信息。</p>
<p>第二十九条 支付机构应当充分尊重客户自主选择权，不得强迫客户使用本机构提供的支付服务，不得阻碍客户使用其他机构提供的支付服务。</p> <p>支付机构应当公平展示客户可选用的各种资金收付方式，不得以任何形式诱导、强迫客户开立支付账户或者通过支付账户办理资金收付，不得附加不合理条件。</p>	<p>支付机构不应以任何形式侵害客户的自主选择权。例如强迫客户使用甚至仅使用本机构的支付服务，阻碍客户选用其他机构提供的支付服务，诱导客户选用某种支付方式而故意隐藏其他可选支付方式，诱导或强迫客户开立或使用支付账户等。</p>
<p>第三十条 支付机构因系统升级、调试等原因，需暂停网络支付服务的，应当至少提前5个工作日予以公告。</p> <p>支付机构变更协议条款、提高服务收费标准或者新设收费项目的，应当于实施之前在网站等服务渠道以显著方式连续公示30日，并于客户首次办理相关业务前确认客户知悉且接受拟调整的全部详细内容。</p>	<p>支付机构保护客户知情权、自主选择权的义务。</p>
第五章 监督管理	
<p>第三十一条 支付机构提供网络支付创新产品或者服务、停止提供产品或者服务、与境外机构合作在境内开展网络支付业务的，应当至少提前30日向法人所在地中国人民银行分支机构报告。</p> <p>支付机构发生重大风险事件的，应当及时向法人所在地中国人民银行分支机构</p>	<p>支付机构的报告义务。</p>

条款	释义
报告；发现涉嫌违法犯罪的，同时报告公安机关。	
<p>第三十二条 中国人民银行可以结合支付机构的企业资质、风险管控特别是客户备付金管理等因素，确立支付机构分类监管指标体系，建立持续分类评价工作机制，并对支付机构实施动态分类管理。具体办法由中国人民银行另行制定。</p>	<p>本条款明确人民银行对支付机构实施分类监管。对于综合评级较高的机构，人民银行从多个方面制定弹性和灵活性更高的监管措施，为创新预留更多空间；对于综合评级较低的机构，人民银行提出更加严格的监管措施，以加强风险防范和客户权益保护。</p>
<p>第三十三条 评定为“A”类且Ⅱ类、Ⅲ类支付账户实名比例超过95%的支付机构，可以采用能够切实落实实名制要求的其他客户身份核实方法，经法人所在地中国人民银行分支机构评估认可并向中国人民银行备案后实施。</p>	<p>本条款在第十一条的基础上，适度提升了支付账户实名验证方式的灵活性。符合条件的支付机构在开立Ⅱ类、Ⅲ类支付账户时，既可以按照“三个”、“五个”外部渠道的方式进行客户身份核实，也可以运用各种安全、合法的技术手段灵活制定其他有效的身份核实方法，经评估认可后予以采用。</p>
<p>第三十四条 评定为“A”类且Ⅱ类、Ⅲ类支付账户实名比例超过95%的支付机构，可以对从事电子商务经营活动、不具备工商登记注册条件且相关法律法规允许不进行工商登记注册的个人客户（以下简称个人卖家）参照单位客户管理，但应建立持续监测电子商务经营活动、对个人卖家实施动态管理的有效机制，并向法人所在地中国人民银行分支机构备案。</p> <p>支付机构参照单位客户管理的个人卖家，应至少符合下列条件：</p> <p>（一）相关电子商务交易平台已依照相关法律法规对其真实身份信息进行审查和登记，与其签订登记协议，建立登记档案并定期核实更新，核发证明个人身份信息真实合法的标记，加载在其从事电子商务经营活动的主页面醒目位置；</p> <p>（二）支付机构已按照开立Ⅲ类个人</p>	<p>一、为进一步促进电子商务发展，为从事电子商务经营活动的个人卖家提供便利，本条款适度提升了个人卖家管理方式的灵活性，符合条件的支付机构可以参照单位客户对个人卖家进行管理。</p> <p>二、为兼顾便捷性和安全性，防止不法分子通过虚构电子商务交易伪装经营者身份，规避个人支付账户相关管理措施，增加欺诈、套现、洗钱等风险，本条款对支付机构提出了相应管理要求：</p> <p>一是建立有效机制，确保能够识别和控制虚构交易行为，能够鉴别个人卖家是否真实从事电子商务经营活动，并对个人卖家持续进行动态管理；</p> <p>二是科学把握适用范围，仅对于长期具有大额支付需求，且Ⅲ类支付账户无法满足经营需要的个人卖家，支付机构可以参照单位客户管理。对于Ⅱ类、Ⅲ类支付</p>

条款	释义
<p>支付账户的标准对其完成身份核实；</p> <p>(三)持续从事电子商务经营活动满6个月，且期间使用支付账户收取的经营收入累计超过20万元。</p>	<p>账户可以满足需要的个人卖家，支付机构应严格按照个人客户管理。</p>
<p>第三十五条 评定为“A”类且Ⅱ类、Ⅲ类支付账户实名比例超过95%的支付机构，对于已经实名确认、达到实名制管理要求的支付账户，在办理第十二条第一款所述转账业务时，相关银行账户与支付账户可以不属于同一客户。但支付机构应在交易中向银行准确、完整发送交易渠道、交易终端或接口类型、交易类型、收付款客户名称和账号等交易信息。</p>	<p>一、本条款在第十二条的基础上，适度扩充了支付账户的转账交易功能。符合条件的支付机构可以同时办理支付账户与同名银行账户之间、支付账户与非同名银行账户之间的转账业务。</p> <p>二、支付账户转账交易功能的扩充以交易信息的透明度为前提。如支付机构未向银行准确、完整发送交易信息，则应严格执行第十二条规定。</p>
<p>第三十六条 评定为“A”类且Ⅱ类、Ⅲ类支付账户实名比例超过95%的支付机构，可以将达到实名制管理要求的Ⅱ类、Ⅲ类支付账户的余额付款单日累计限额，提高至第二十四条规定的2倍。</p> <p>评定为“B”类及以上，且Ⅱ类、Ⅲ类支付账户实名比例超过90%的支付机构，可以将达到实名制管理要求的Ⅱ类、Ⅲ类支付账户的余额付款单日累计限额，提高至第二十四条规定的1.5倍。</p>	<p>一、本条款在第二十四条的基础上，适度提升了支付账户余额付款的单日累计交易限额。</p> <p>二、对于安全性较高的余额付款交易（采用了数字证书或电子签名进行验证），本条款仍然不规定单日累计限额，支付机构可以与客户自主约定限额。</p> <p>三、客户使用银行账户付款（例如银行网关支付、银行卡快捷支付等）不属于本条款规范范畴，也不受本条款的限额约束。</p>
<p>第三十七条 评定为“A”类的支付机构按照第十条规定办理相关业务时，可以与银行根据业务需要，通过协议自主约定由支付机构代替进行交易验证的情形，但支付机构应在交易中向银行完整、准确发送交易渠道、交易终端或接口类型、交易类型、商户名称、商户编码、商户类别码、收付款客户名称和账号等交易信息；银行应核实支付机构验证手段或渠道的安全性，且对客户资金安全的管理责任不因支付机构代替验证而转移。</p>	<p>一、本条款在第十条的基础上，适度提升了银行卡快捷支付交易验证方式的灵活性。符合条件的支付机构可以与银行自主约定由支付机构代替进行交易验证的具体情形。</p> <p>二、支付机构与银行自主约定交易验证主体，应以交易信息的透明度为前提。如支付机构未向银行准确、完整发送交易信息，则应严格执行第十条规定。</p> <p>三、无论银行自主进行交易验证还是支付机构代替验证，银行都应在事先或首笔交易时自主识别客户身份并与客户直接</p>

条款	释义
	签订授权协议，并始终承担客户资金安全的管理责任。
<p>第三十八条 对于评定为“C”类及以下、支付账户实名比例较低、对零售支付体系或社会公众非现金支付信心产生重大影响的支付机构，中国人民银行及其分支机构可以在第十九条、第二十八条等规定的基础上适度提高公开披露相关信息的要求，并加强非现场监管和现场检查。</p>	<p>对于综合评级较低、实名制落实较差、对零售支付体系或社会公众非现金支付信心产生重大影响的支付机构，人民银行将适度增加信息披露相关义务，并依法重点加强监管。</p>
<p>第三十九条 中国人民银行及其分支机构对照上述分类管理措施相应条件，动态确定支付机构适用的监管规定并持续监管。支付机构分类评定结果和支付账户实名比例不符合上述分类管理措施相应条件的，应严格按照第十条、第十一条、第十二条及第二十四条等相关规定执行。</p> <p>中国人民银行及其分支机构可以根据社会经济发展情况和支付机构分类管理需要，对支付机构网络支付业务范围、模式、功能、限额及业务创新等相关管理措施进行适时调整。</p>	<p>第三十三条至第三十八条是人民银行根据支付机构分类评定结果和实名制落实情况所制定的差别化管理措施，仅适用于符合相应条件的支付机构。不符合相应条件的其他支付机构，应当严格执行前几章中明确的监管规定。</p>
<p>第四十条 支付机构应当加入中国支付清算协会，接受行业自律组织管理。</p> <p>中国支付清算协会应当根据本办法制定网络支付业务行业自律规范，建立自律审查机制，向中国人民银行备案后组织实施。自律规范应包括支付机构与客户签订协议的范本，明确协议应记载和不得记载事项，还应包括支付机构披露有关信息的具体内容和标准格式。</p> <p>中国支付清算协会应当建立信用承诺制度，要求支付机构以标准格式向社会公开承诺依法合规开展网络支付业务、保障客户信息安全和资金安全、维护客户合法权益、如违法违规自愿接受约束和处罚。</p>	<p>一、本条款要求支付机构加入行业协会并接受自律管理，要求行业协会制定配套自律规范、建立自律审查机制。</p> <p>二、本办法部分条款对支付机构与客户之间的权利、责任、义务及协议内容提出了监管要求，行业协会应在此基础上制定协议范本并组织支付机构统一采用。</p> <p>三、本办法部分条款对支付机构提出了关于披露信息的监管要求，行业协会应在此基础上确定信息披露包括的具体内容及标准格式。</p> <p>四、本条款要求行业协会建立信用承诺制度，充分发挥社会监督作用。</p>

条款	释义
第六章 法律责任	
<p>第四十一条 支付机构从事网络支付业务有下列情形之一的，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》第四十二条的规定进行处理：</p> <p>（一）未按规定建立客户实名制管理、支付账户开立与使用、差错争议和纠纷投诉处理、风险准备金和交易赔付、应急预案等管理制度的；</p> <p>（二）未按规定建立客户风险评级管理、支付账户功能与限额管理、客户支付指令验证管理、交易和信息安全管理、交易监测系统等风险控制机制的，未按规定对支付业务采取有效风险控制措施的；</p> <p>（三）未按规定进行风险提示、公开披露相关信息的；</p> <p>（四）未按规定履行报告义务的。</p>	支付机构违反相关规定的处理措施。
<p>第四十二条 支付机构从事网络支付业务有下列情形之一的，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》第四十三条的规定进行处理；情节严重的，中国人民银行及其分支机构依据《中华人民共和国中国人民银行法》第四十六条的规定进行处理：</p> <p>（一）不符合支付机构支付业务系统设施有关要求的；</p> <p>（二）不符合国家、金融行业标准和相关信息安全管理要求的，采用数字证书、电子签名不符合《中华人民共和国电子签名法》、《金融电子认证规范》等规定的；</p> <p>（三）为非法交易、虚假交易提供支付服务，发现客户疑似或者涉嫌违法违规行为未按规定采取有效措施的；</p> <p>（四）未按规定采取客户支付指令验证措施的；</p>	支付机构违反相关规定的处理措施。

条款	释义
<p>(五) 未真实、完整、准确反映网络支付交易信息，篡改或者隐匿交易信息的；</p> <p>(六) 未按规定处理客户信息，或者未履行客户信息保密义务，造成信息泄露隐患或者导致信息泄露的；</p> <p>(七) 妨碍客户自主选择支付服务提供主体或资金收付方式的；</p> <p>(八) 公开披露虚假信息的；</p> <p>(九) 违规开立支付账户，或擅自经营金融业务活动的。</p>	
<p>第四十三条 支付机构违反反洗钱和反恐怖融资规定的，依据国家有关法律法规进行处理。</p>	<p>支付机构违反相关规定的处理措施。</p>
第七章 附 则	
<p>第四十四条 本办法相关用语含义如下：</p> <p>单位客户，是指接受支付机构支付服务的法人、其他组织或者个体工商户。</p> <p>个人客户，是指接受支付机构支付服务的自然人。</p> <p>单位客户的身份基本信息，包括客户的名称、地址、经营范围、统一社会信用代码或组织机构代码；可证明该客户依法设立或者可依法开展经营、社会活动的执照、证件或者文件的名称、号码和有效期限；法定代表人（负责人）或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。</p> <p>个人客户的身份基本信息，包括客户的姓名、国籍、性别、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。</p> <p>法人和其他组织客户的有效身份证件，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</p>	<p>本办法有关用语的含义。</p>

条款	释义
<p>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。</p> <p>个人客户的有效身份证件，包括：在中国境内已登记常住户口的中国公民为居民身份证，不满十六周岁的，为居民身份证或户口簿；香港、澳门特别行政区居民为港澳居民往来内地通行证；台湾地区居民为台湾居民来往大陆通行证；定居国外的中国公民为中国护照；外国公民为护照或者外国人永久居留证（外国边民，按照边贸结算的有关规定办理）；法律、行政法规规定的其他身份证明文件。</p> <p>客户本人，是指客户本单位（单位客户）或者本人（个人客户）。</p>	
<p>第四十五条 本办法由中国人民银行负责解释和修订。</p>	<p>本办法的解释和修订主体。</p>
<p>第四十六条 本办法自 2016 年 7 月 1 日起施行。</p>	<p>本办法的施行日期。</p>