中国人民银行《支付机构网络支付业务管理办法》征求意见稿全文

第一章总则

为规范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》等规定，制定本办法。支付机构从事网络支付业务，适用本办法。

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、固定电话支付和数字电视支付等网络支付业务的非金融机构。

本办法所称网络支付业务是指客户通过计算机、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，由支付机构为付款人和网络特约商户的电子商务交易实现货币资金转移的活动。

支付机构不得为付款人和实体特约商户的交易提供网络支付服务。

支付机构应当依法维护当事人的合法权益，保障信息安全和交易安全。

支付机构应遵守反洗钱法律法规要求，履行反洗钱和反恐怖融资义务，不得为国家法律法规禁止和限制买卖的物品或服务、虚假交易提供网络支付服务。

支付机构开展网络支付业务，涉及跨境人民币结算和外汇支付业务的，应按照中国人民银行、国家外汇管理局相关规定执行。

第二章 业务开通与客户管理

支付机构办理网络支付业务，应当遵循“了解你的客户”原则，采取有效措施核实并依法留存客户身份基本信息。

支付机构应为客户建立唯一的客户识别编码，并根据客户特征、交易类型、交易金额等，与客户约定安全可靠的身份认证方式。

支付机构采用电子签名方式进行客户身份认证和交易授权的，应当优先由合法的第三方认证机构提供认证服务。

支付机构提供网络支付服务，应当向客户公示信息、提供章程或与客户签订协议。

公示信息、章程或协议应当包括但不限于以下内容：

(一)支付机构名称、营业地址、网址和联系方式;

(二)所提供的网络支付业务交易类型、交易规则、身份验证和交易授权方式;

(三)客户资金结算的时限要求，及支付机构为此提供相关支付便利的义务;

(四)具体收费项目和收费标准;

(五)差错及纠纷处理规则和程序;

(六)客户身份信息、账户信息和交易信息的保护责任;

(七)客户身份信息变更后的通知义务和方式;

(八)客户服务及投诉的方式和渠道，以及客户权益保障条款。

支付机构应基于客户银行账户提供网络支付服务。

支付机构向客户银行发送支付指令，扣划客户银行账户资金的，支付机构、客户及银行应事先或在首笔交易时，签订三方协议或两两协议，按照以下规则明确相关授权并依照执行：

(一)支付机构应取得客户及银行的协议授权，同意其向客户的银行账户发起支付指令扣划资金;

(二)银行应依法履行客户身份识别义务，并已事先或在首笔交易时取得客户的协议授权，明确支付机构发起支付指令扣划客户银行账户资金时，银行对其客户的身份识别和交易验证方式;但客户首笔业务的身份识别和交易验证应由银行完成，支付机构不得代为识别与验证;后续交易的验证主体、验证手段和渠道，由客户、银行与支付机构通过协议进行授权及约定;

(三)支付机构应当为客户提供后续交易验证由银行完成的优先选择权，不得人为设置障碍;支付机构应当配合客户及银行为控制交易风险而采取的必要措施和手段。

(四)确因业务需要，客户自愿授权并与支付机构和开户银行约定后续交易由支付机构代为验证的，支付机构应确保验证手段和渠道的安全性，设置单笔、日累计交易限额，并承担由此所导致的客户信息泄露和资金被盗用风险。

根据客户意愿，获得互联网支付业务资质的支付机构，可以为客户开立记录客户支付交易和资金余额信息的支付账户。

支付机构不得为金融机构以及从事融资、理财、担保、货币兑换等金融业务的其他机构开立支付账户。

支付机构不得为客户办理或变相办理支付账户的透支和现金存取，以及融资、担保业务。

支付机构开立支付账户应当遵守实名制管理规定，识别客户身份，核实有效身份证件，登记身份基本信息，并按规定留存有效身份证件复印件或者影印件。

支付机构应确保支付账户名称与客户有效身份证件或者身份证明文件上记载的姓名或名称一致，不得为客户开立匿名、假名支付账户。

支付机构要求客户提供有关资料信息时，应告知客户使用目的和范围、客户信息保护措施，以及客户未准确提供或提供虚假资料信息的后果;支付机构承担未妥善保管和使用客户信息导致信息被盗用的后果和责任。

客户基本身份信息发生变更的，应当及时通知支付机构，支付机构在核实客户身份后予以更新。

支付机构为客户开立支付账户，应当与客户签订协议。协议内容包括但不限于：

(一)支付账户开立、挂失、止付、注销的规则;

(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的授权;

(四)支付账户使用和管理的责任、权利和义务;

(五)支付账户违规使用的处置和责任;

(六)支付账户资金变动的通知方式;

(七)支付账户异常交易的通知、处置方式和责任划分。

支付账户只能用于电子商务交易付款和符合规定的个人客户支付账户(以下简称个人支付账户)间转账，不得用于电子商务交易收款。

支付机构应按协议约定及时将电子商务交易收款资金结算至网络特约商户指定的同名银行账户，资金结算时限应为付款客户确认可直接向网络特约商户付款的支付指令生效之日起 1 至 3 个工作日，因涉嫌违规违法等风险交易延迟结算的除外。

支付机构应按照客户识别编码，对同一客户开立的所有支付账户统一管理。

支付账户只能由本人使用，不得出借、出租、出售。任何单位和个人不得利用支付账户从事或协助他人从事非法活动。

客户挂失或重置密码、密钥或数字证书，更改预留手机号码等验证信息，或办理支付账户止付、注销业务的，支付机构应在确认客户身份及真实意愿后及时办理。

支付机构应严格规范客户身份信息、交易验证方式更改流程，针对不同业务处理类型和修改渠道完善客户身份验证措施。

第三章 业务管理

支付机构提供的网络支付业务的交易类型包括充值、消费、转账等。

充值，是指客户将本人同名银行借记账户或同一支付机构发行的预付卡中资金转入本人同名支付账户。支付账户未用充值资金退回时，应转回原银行账户或原预付卡。

消费，是指客户因商品或服务购买、税费缴纳、信用卡还款、购买特定金融产品等电子商务交易活动，将付款客户的银行账户或支付账户资金划转至网络特约商户的银行账户。因交易取消(撤销)、退货、交易不成功等原因需退款的，相应款项应转回原银行账户或支付账户。

转账，是指个人支付账户之间无电子商务交易背景的小额资金划转。单位客户的支付账户(以下简称单位支付账户)不得办理无电子商务交易背景的资金转账业务。

单位支付账户的资金来源仅限于其同名人民币银行账户，资金只能用于消费;个人支付账户的资金来源仅限于本人同名人民币银行借记账户、本支付机构按规定发行的预付卡充值和个人支付账户转账转入，资金只能用于消费和转账转出。

个人支付账户转账单笔金额不得超过 1000 元，同一客户所有支付账户转账年累计金额不得超过 1 万元。

支付机构应对转账转入资金进行单独管理，转入资金只能用于消费和转账转出，不得向银行账户回提。

个人支付账户单笔消费金额不得超过5000元,同一个人客户所有支付账户消费月累计金额不得超过1万元。超过限额的，应通过客户的银行账户办理。

网络特约商户应指定一个同名银行账户，用于交易资金结算。

支付机构应建立网络特约商户用于资金结算的银行账户设置和变更审核制度，严格审核设置和变更申请材料的真实性、有效性。

支付机构应确保交易信息的真实性、完整性、可追溯性。交易信息包括但不限于下列事项：

(一)交易渠道、受理终端类型、交易类型、网络特约商户类别码及唯一性编码、交易金额、交易时间;

(二)收付款客户名称，收付款银行账户的开户银行名称及账号、支付账户账号;

(三)付款客户的身份验证和交易授权信息;

(四)直接向客户提供商品或服务的特约商户名称及按照《金融零售业务商户类别代码》(GB/T 20548-2006)设置的商户类别码;

(五)有效追溯交易的标识。

支付机构对网络特约商户的拓展与管理、客户使用银行账户支付的交易处理，以及相关风险控制措施，应当按照《银行卡收单业务管理办法》的相关规定执行。

支付机构开展网络支付业务，应拥有并运营独立、安全、规范的业务处理系统，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。

第四章 风险管理与客户权益保护

支付机构网络支付业务应符合国家和金融行业技术标准和相关信息安全管理要求。

支付机构业务处理系统应对客户发起支付指令的计算机、移动电话、固定电话等不同终端进行有效识别，并针对不同终端发起交易的风险程度，实施充分的、有效的验证方式，采取有效的风险控制措施。

支付机构应综合客户实名认证、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。 对风险评级较高的客户，支付机构应对其开通的交易类型、交易金额进行限制，并采取强化交易监测、账户止付、延迟结算等风险管理措施。

支付机构应健全网络支付业务风险管理制度，建立交易监测系统，对疑似套现、洗钱、非法融资、欺诈或泄漏客户信息等可疑交易及时核查，采取有效的风险防控措施，并承担因未采取措施导致的风险损失责任;发现涉嫌违法犯罪的，应及时向公安机关报案，同时向中国人民银行及其分支机构报告。

支付机构应至少每年对内部控制制度、业务处理系统、交易监测系统、信息安全管理等风险防控机制开展一次全面的风险评估，并完善支付安全措施。

支付机构应限制客户尝试登陆或身份验证的次数，制定客户访问超时规则，设置身份验证时限。使用一次性密码进行身份验证时，支付机构应将该密码有效期严格限制在最短的必要时间内。

支付机构对业务办理过程中采集和处理的客户信息，应制定有效的风险控制措施，依法或按照客户授权使用，确保相关信息安全并承担相应的安全管理责任。

支付机构不得存储客户银行账户密码、银行卡卡片验证码及卡片有效期等敏感信息;确因业务需要存储客户银行卡卡号、卡片有效期的，应取得客户和客户开户银行授权，并以加密形式存储。

支付机构应制定突发事件应急预案，建立灾备系统，保障业务连续性和系统安全性。

支付机构应建立健全风险准备金制度和交易赔付制度，风险准备金应对非因客户原因发生的风险损失予以先行赔付，保障客户合法权益。

支付机构应向客户充分提示网络支付业务的潜在风险，对客户进行必要的认知教育和安全指导，并对高风险业务在操作前、操作中进行风险警示。

支付机构为客户特定金融产品购买、网络信贷等融资活动提供网络支付服务的，应确保产品或服务提供方为依法合规开展业务的机构，并充分向客户提示潜在风险。

支付机构应采取有效措施，在执行支付指令前提示客户对支付指令的准确性进行确认，并在支付指令完成后及时将结果通知客户。 因交易超时、无响应或系统故障导致支付指令无法正常处理的，支付机构应及时提示客户。

因客户原因造成支付指令未执行、未适当执行、延迟执行的，支付机构应主动通知客户更改或配合客户采取补救措施。

支付机构应建立健全网络支付业务差错处理制度，配备专业部门和人员，据实、准确、及时处理差错交易。

支付机构提高网络支付服务收费标准或新设收费项目的，应至少于执行日前 3 个月在网站公示。

支付机构提高对网络特约商户的收费标准，应通过合理有效方式提前 3 个月通知商户。

支付机构应在提高收费标准或新设收费项目后、客户首次办理相关业务前，确认客户知悉该服务收费标准并保证客户对该服务的选择权。

支付机构因系统升级、调试等原因，需暂停网络支付服务的，应至少提前 5 个工作日予以公告。

支付机构提供网络支付服务，应开设具有合法独立域名的网站，设立统一的客户服务电话和查询投诉渠道。

支付机构应为客户免费提供最近一年以内交易信息查询服务。

支付机构对客户的身份资料、账户信息和交易信息，应妥善保存，身份资料、账户信息自业务关系结束之日起至少保存 5 年，交易信息自交易记账之日起至少保存 5 年。

第五章 监督管理

中国人民银行及其分支机构依法对支付机构的网络支付业务活动进行监督和管理。

中国人民银行及其分支机构可采取如下措施，对支付机构进行现场检查：

(一)进入与网络支付业务相关的经营场所进行检查;

(二)查阅、复制与检查事项有关的文件、资料;

(三)询问有关工作人员，要求对有关事项进行说明;

(四)检查有关系统和设施，复制有关数据资料。

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和非现场检查，按时报送网络支付业务统计信息和管理信息。

支付机构提供网络支付创新产品或服务、决定停止提供产品或服务、调高服务收费标准或新增收费项目等，应至少提前 30 日向中国人民银行及其分支机构备案。

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。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，向中国人民银行备案后组织实施。

支付机构发生涉嫌违法犯罪案件或重大风险事件的，应及时向中国人民银行及其分支机构报告。

第六章 罚则

支付机构从事网络支付业务有下列情形之一的，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》第四十二条的规定责令其限期改正，并予以警告或处 1 万元以上 3 万元以下罚款：

(一)未按规定建立并落实客户实名制、客户风险评级管理、风险准备金与交易赔付、交易和信息安全管理、年度风险评估、应急管理等制度的;

(二)未按规定向客户提供相关业务优先选择权的;

(三)未按规定进行风险提示或公开披露相关信息的;

(四)未按规定处理客户身份信息、账户信息、交易信息及提供有关信息查询服务的;

(五)未按规定向中国人民银行及其分支机构报送信息或办理相关备案手续的。

支付机构从事网络支付业务有下列情形之一的，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》第四十三条的规定责令其限期改正，并处 3 万元罚款;情节严重的，中国人民银行注销其《支付业务许可证》;涉嫌犯罪的，依法移送公安机关：

(一)网络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;

(二)不符合国家和金融行业技术标准和相关信息安全管理要求的;

(三)未按规定建立交易监测系统，发现客户疑似或涉嫌违法违规行为未采取有效措施的;

(四)未按规定开立、使用和管理支付账户，或为实体特约商户提供网络支付服务，以及为客户提供或变相提供现金存取、融资和担保等本办法规定的禁止性支付服务的;

(五)未准确反映网络支付交易信息，未按规定进行网络支付业务处理及相关交易限额管理、交易验证、资金划转与资金结算的;

(六)发生客户身份信息、账户信息、交易信息泄露，或未尊重客户意愿，侵害相关当事人合法权益的;

(七)为非法交易、虚假交易提供支付服务的。

支付机构未按本办法要求识别客户身份、履行反洗钱义务的，由中国人民银行及其分支机构依据国家有关反洗钱法律法规等进行处罚。

未取得网络支付业务相关资质，擅自或变相开展网络支付业务的，由中国人民银行及其分支机构终止其网络支付业务;涉嫌犯罪的，依法移送公安机关;构成犯罪的，依法追究刑事责任。

第七章附则

本办法相关用语含义如下：

个人有效身份证件，是指居民身份证、港澳台居民通行证、外国公民护照等;

单位有效身份证件，是指营业执照、有关政府部门的批文、登记证书或其他能证实其合法真实身份的证明等。

网络特约商户，是指基于公共网络信息系统提供商品或服务的特约商户;

实体特约商户，是指通过实体经营场所提供商品或服务的特约商户。

单位客户，是指接受支付机构支付服务的企事业单位、个体工商户或其他组织，以及按照国家工商行政管理机关有关规定，开展网络商品交易等经营活动的自然人;

个人客户，是指接受支付机构的支付服务，但未开展网络交易等经营活动的自然人。

本办法由中国人民银行负责解释和修订。