条码支付业务规范（试行）

第一章 总　　则

第一条 为规范条码（二维码）支付（以下简称条码支付）业务，保护消费者合法权益，促进条码支付业务健康发展，根据《电子支付指引(第一号)》（中国人民银行公告〔2005〕第23号公布）、《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）、《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）、《非银行支付机构网络支付业务管理办法》（中国人民银行公告〔2015〕第43号公布）等规定，制定本规范。

第二条 本规范所称条码支付业务是指银行业金融机构（以下简称银行）、非银行支付机构（以下简称支付机构）应用条码技术，实现收付款人之间货币资金转移的业务活动。

条码支付业务包括付款扫码和收款扫码。付款扫码是指付款人通过移动终端识读收款人展示的条码完成支付的行为。收款扫码是指收款人通过识读付款人移动终端展示的条码完成支付的行为。

第三条 银行、支付机构开展条码支付业务应遵循本规范。

第四条 支付机构开展条码支付业务，应按规定取得相应的业务许可，并按相应管理办法规范开展业务。

第五条 支付机构不得基于条码技术，从事或变相从事证券、保险、信贷、融资、理财、担保、信托、货币兑换、现金存取等业务。

第六条 银行、支付机构开展条码支付业务应遵守客户实名制管理规定；遵守反洗钱法律法规要求，履行反洗钱和反恐怖融资义务；依法维护客户及相关主体的合法权益。

第七条 银行、支付机构应自觉遵守商业道德，不得以任何形式诋毁其他市场主体的商业信誉，不得采用不正当竞争手段排挤竞争对手、损害其他市场主体利益，破坏市场公平竞争秩序。

第八条 银行、支付机构应遵守中国人民银行发布的相关技术标准与规范要求，保证条码支付业务的交易安全和信息安全。

第二章 条码生成和受理

第九条 银行、支付机构开展条码支付业务，应将客户用于生成条码的银行账户或支付账户、身份证件号码、手机号码进行关联管理。

第十条 银行、支付机构开展条码支付业务,可以组合选用下列三种要素，对客户条码支付交易进行验证：

（一）仅客户本人知悉的要素，如静态密码等；

（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；

（三）客户本人生物特征要素，如指纹等。

银行、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。

第十一条 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相关规定，应确保数字证书的唯一性、完整性及交易的不可抵赖性。

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。

采用客户本人生物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。

第十二条 银行、支付机构应根据《条码支付安全技术规范（试行）》（银办发〔2017〕242 号）关于风险防范能力的分级，对个人客户的条码支付业务进行限额管理：

（一）风险防范能力达到 A 级，即采用包括数字证书或电子签名在内的两类（含）以上有效要素对交易进行验证的，可与客户通过协议自主约定单日累计限额；

（二）风险防范能力达到 B 级，即采用不包括数字证书、电子签名在内的两类（含）以上有效要素对交易进行验证的,同一客户单个银行账户或所有支付账户单日累计交易金额应不超过 5000 元；

（三）风险防范能力达到 C 级，即采用不足两类要素对交易进行验证的，同一客户单个银行账户或所有支付账户单日累计交易金额应不超过 1000 元；

（四）风险防范能力达到 D 级，即使用静态条码的，同一客户单个银行账户或所有支付账户单日累计交易金额应不超过 500 元。

第十三条 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，同一客户全部银行账户合计日累计交易限额执行第十二条的规定。

第十四条 银行、支付机构提供付款扫码服务的，应具备差异化的风控措施和完善的客户权益受损解决机制，在条码生成、识读、支付等核心业务流程中明确提示客户支付风险，切实防范不法分子通过在条码中植入木马、病毒等方式造成客户信息泄露和资金损失。

第十五条 银行、支付机构提供收款扫码服务的，应使用动态条码，设置条码有效期、使用次数等方式，防止条码被重复使用导致重复扣款，确保条码真实有效。

第十六条 银行、支付机构开展条码支付业务所涉及的业务系统、客户端软件、受理终端(网络支付接口)等，应当持续符合监管部门及行业标准要求，确保条码生成和识读过程的安全性、真实性和完整性。

第十七条 银行、支付机构应按照中国人民银行相关规定强化支付敏感信息内控管理和安全防护，强化交易密码保护机制；通过支付标记化技术应用等手段，从源头控制信息泄露和欺诈交易风险。

第十八条 银行、支付机构应指定专人操作与维护条码生成相关系统。条码信息仅限包含当次支付相关信息，不应包含任何与客户及其账户相关的支付敏感信息。

特约商户展示的条码，仅限包含与当次支付有关的特约商户、商品（服务）或商品（服务）订单等信息。

移动终端展示的条码，不得包含未经加密处理的客户本人账户信息。

第十九条 银行、支付机构应确保条码支付交易经客户确认或授权后发起，支付指令应真实、完整、有效。

移动终端完成条码扫描后，应正确、完整显示扫码内容，供客户确认。

特约商户受理终端完成条码扫描后，应仅显示扫码结果并提示下一步操作，不得显示付款人的支付敏感信息。

第二十条 银行、支付机构应根据条码支付的真实场景，按规定正确选用交易类型，准确标识交易信息并完整发送，确保交易信息的完整性、真实性和可追溯性。

交易信息至少应包括：直接提供商品或服务的特约商户名称、类别和代码，受理终端（网络支付接口）类型和代码，交易时间和地点（网络特约商户的网络地址），交易金额，交易类型和渠道，交易发起方式等。网络特约商户的交易信息还应当包括订单号和网络交易平台名称。

银行、支付机构应在支付交易报文中通过特定域标识该交易为条码支付交易，以供报文接收方正确识别并进行授权处理。

第二十一条 支付交易完成后，特约商户受理终端和移动终端应显示支付结果；支付失败的，特约商户受理终端和移动终端还应显示失败原因。

第三章 特约商户管理

第二十二条　银行、支付机构拓展条码支付特约商户，应遵循“了解你的客户”原则，确保所拓展的是依法设立、合法经营的特约商户。

第二十三条　中国支付清算协会、清算机构应将条码支付特约商户纳入特约商户信息管理系统及黑名单管理机制。银行、支付机构拓展特约商户时，应进行查询确认，如商户及其法定代表人或负责人在特约商户信息管理系统中存在不良信息记录的，应谨慎为该商户提供条码支付服务；不得将已纳入黑名单的单位和个人，以及由纳入黑名单个人担任法定代表人或者负责人的单位拓展为特约商户，已经拓展为特约商户的，应当自该特约商户被列入黑名单之日起 10 日内予以清退。

第二十四条 银行、支付机构拓展特约商户应落实实名制规定，严格审核特约商户的营业执照等证明文件，以及法定代表人或负责人的有效身份证件等申请材料，确认申请材料的真实性、完整性、有效性，并留存申请材料的影印件或复印件。

对依据法律法规和相关监管规定免于办理工商注册登记的实体特约商户（小微商户），收单机构在遵循“了解你的客户”原则的前提下，可以通过审核商户主要负责人身份证明文件和辅助证明材料为其提供条码支付收单服务。辅助证明材料包括但不限于营业场所租赁协议或者产权证明、集中经营场所管理方出具的证明文件等能够反映小微商户真实、合法从事商品或服务交易活动的材料。

以同一个身份证件在同一家收单机构办理的全部小微商户基于信用卡的条码支付收款金额日累计不超过 1000 元、月累计不超过 1 万元。银行、支付机构应当结合小微商户风险等级动态调整交易卡种、交易限额、结算周期等，强化对小微商户的交易监测。

第二十五条 银行、支付机构应与特约商户签订条码支付受理协议，就银行结算账户的设置和变更、资金结算周期、结算手续费标准、差错和争议处理等条码支付服务相关事项进行约定，明确双方的权利、义务和违约责任。

第二十六条　银行、支付机构在条码支付受理协议中，应要求特约商户基于真实的商品或服务交易背景受理条码支付；按规定使用受理终端或网络支付接口、银行结算账户，不得利用其从事或协助他人从事非法活动；妥善处理交易数据信息、保存交易凭证，保障交易信息安全；不得向客户收取或变相收取附加费用，或降低服务水平。

第二十七条 银行、支付机构应建立特约商户信息管理系统，记录特约商户名称和经营地址、特约商户身份资料信息、特约商户类别、结算手续费标准、银行结算账户信息、开通的交易类型和开通时间、受理终端（网络交易接口）类型和安装地址等信息，并及时进行更新。

银行、支付机构应按规定向中国支付清算协会和清算机构特约商户信息管理系统报送特约商户基本信息。

第二十八条 银行、支付机构应建立特约商户检查制度，明确检查频率、检查内容、检查记录等管理要求，落实检查责任。

第二十九条 银行、支付机构应当对实体特约商户条码收单业务进行本地化经营和管理，通过在特约商户及其分支机构所在省（区、市）辖内的收单机构或其分支机构提供收单服务，不得跨省（区、市）开展条码收单业务。

第三十条 银行、支付机构应按照《中国人民银行关于加强银行卡收单业务外包管理的通知》（银发〔2015〕199 号）相关要求审慎选择外包服务机构，严格规范与外包服务机构的业务合作，强化收单外包业务的风险管理责任。银行、支付机构作为条码支付收单业务主体的管理责任和风险承担责任不因外包关系而转移。

银行、支付机构不得将特约商户资质审核、受理协议签订、资金结算、交易处理、风险监测、受理终端主密钥生成和管理、网络支付接口管理、差错和争议处理工作交由外包服务机构办理。银行、支付机构与外包服务机构系统对接开展业务的，应确保外包服务机构无法获取或者接触支付敏感信息、不得从事或者变相从事特约商户资金结算。

第三十一条 银行、支付机构应尊重特约商户的自主选择权，不得干涉或变相干涉特约商户与其他机构的合作。

第三十二条 银行、支付机构开展条码支付业务应参照银行卡刷卡手续费定价标准科学合理定价，不得采用交叉补贴、低于成本价格倾销等不正当手段排挤竞争对手，扰乱市场秩序。

第四章 风险管理

第三十三条 银行、支付机构应建立全面风险管理体系和内部控制机制，提升风险识别能力，采取有效措施防范风险，及时发现、处理可疑交易信息及风险事件。

第三十四条 银行、支付机构开展条码支付业务，应当评估业务相关的洗钱和恐怖融资风险，采取与风险水平相适应的管控措施。

第三十五条 银行、支付机构应建立特约商户风险评级制度，综合考虑特约商户的区域和行业特征、经营规模、财务和资信状况等因素，对特约商户进行风险评级。

第三十六条 银行、支付机构应结合特约商户风险等级及交易类型等因素，设置或与其约定单笔及日累计交易限额。

第三十七条 银行、支付机构对风险等级较高的特约商户，应通过强化交易监测、建立特约商户风险准备金、延迟清算等风险管理措施，防范交易风险。

第三十八条 银行、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。

第三十九条 银行、支付机构应制定突发事件应急预案，建立灾难备份系统，确保条码支付业务的连续性和业务系统安全运行。

第四十条 银行、支付机构应能够有效识别本机构发行的客户端程序和特约商户受理终端，能够确保条码生成和识读过程的安全性。

第四十一条 银行、支付机构应确保客户身份或账户信息安全，防止泄露，并根据收付款不同业务场景设置条码有效性和使用次数。

第四十二条 银行、支付机构应建立条码支付交易风险监测体系，及时发现可疑交易，并采取阻断交易、联系客户核实交易等方式防范交易风险。

第四十三条 银行、支付机构发现特约商户发生疑似套现、洗钱、恐怖融资、欺诈、留存或泄露账户信息等风险事件的，应对特约商户采取延迟资金结算、暂停交易、冻结账户等措施，并承担因未采取措施导致的风险损失责任；发现涉嫌违法犯罪活动的，应及时向公安机关报案。

第四十四条 银行、支付机构应持续完善客户服务体系，及时受理和解决条码支付业务中的客户咨询、查询和投诉等问题，自觉维护客户的合法权益。

第四十五条 银行、支付机构应充分披露条码支付业务产品类型、办理流程、操作规程、收费标准等信息，明确业务风险点及相关责任承担机制、风险损失赔付方式及操作方式。

第四十六条 银行、支付机构应开展对客户的条码支付安全教育，提升其风险防范意识和应对能力。

第四十七条 银行、支付机构应向中国支付清算协会、清算机构风险信息管理系统报送其条码支付特约商户风险信息。

银行、支付机构或其外包服务机构、条码支付特约商户发生涉嫌重大支付违法犯罪案件或重大风险事件的，应当于 2 个工作日内向中国人民银行或其分支机构报告。

第五章 附 则

第四十八条 采取自定义符号、图形、图像等作为信息载体传递交易信息用于支付服务的，参照本规范进行管理。

第四十九条 本规范相关用语含义如下：

移动终端，指客户使用的、具有移动通讯功能，用于展示或识读条码，完成支付的终端设备。如手机、平板电脑等。

特约商户受理终端，指具有条码展示或识读等功能，参与条码支付完成销售收款的特约商户端专用设备。包括具有条码展示功能的显码设备；识读条码并且向后台系统发起支付指令的专用设备，包括但不限于带扫码装置的收银系统、销售点终端（POS）、自助终端等。

支付敏感信息，是指一旦遭到泄露或修改，会对标识的信息主体的信息安全和资金安全造成危害的信息。包括但不限于支付密码、银行卡密码、验证码、卡片有效期、生物特征以及未获客户授权的金融信息。

第五十条 本规范自 2018 年 4 月 1 日起实施。