

## 《金融科技创新应用声明书》

创新应用 基本信息	创新应用编号	91310000132257510M-2022-0001		
	创新应用名称	基于支付标记化的企业移动支付服务		
	创新应用类型	金融服务		
	机构信息	统一社会信用代码	91310000132257510M	
		全球法人识别编码	300300C1091231000098	
		机构名称	上海银行股份有限公司	
		持有金融牌照信息	牌照名称：中华人民共和国金融许可证 机构编码：B0139H231000001 发证机关：中国银行业监督管理委员会 上海监管局	
	拟正式运营时间	2022年05月05日		
	技术应用	1. 运用支付标记化技术，按照标记编码规则对中小微企业对公结算账户进行标记化处理，生成与对公结算账户对应的支付标记，并为支付标记设置交易类型、支付渠道等域控属性，限定支付标记的使用范围，防范敏感信息泄露风险。 2. 运用大数据技术，在获得客户授权的前提下，将行外金融制裁黑名单等数据与行内历史交易数据进行分析挖掘与处理，构建支付风控模型，提高银行对于企业交易风险的识别能力。 3. 运用光学字符识别（OCR）技术，在获得客户授权的前提下，识别提取客户身份证件中的姓名、证件号码等信息，提升业务办理效率和录入准确度。		
	功能服务	本应用综合运用支付标记化、大数据等技术，为中小微企业提供企业账户移动支付服务。一是实现对公结算账户的支付标记申请、生成、授权、领用等功能，基于企业授权审批，为企业员工在差旅支出、小额采购、面对面扫码支付等线上线下消费场景中提供授权资金支付服务，纾解传统模式下企业纸质报销流程繁琐问题，降低企业运营成本，提升企业数字化管理水平；二是基于支付风控模型，对企业资金交易进行风险识别和预警，提升上海银行交易风控水平和效率。 本应用由上海银行股份有限公司独立研发及运营，并提供金融应用场景，此外没有其它第三方机构参与。		

	创新性说明	<p>1. 在数据安全方面，用支付标记代替原有交易过程中的账户信息，与传统基于账号的交易传递过程相比，降低敏感信息泄露风险，保证了企业数据在使用上的安全性。</p> <p>2. 在交易安全方面，通过限定支付标记使用的交易场景，降低支付标记被攻击或泄漏时影响的范围，有效防范欺诈交易风险，保障中小微企业合法权益。</p> <p>3. 在风险控制方面，运用大数据技术构建支付风控模型，多维度评估中小微企业资金使用风险，加强交易真实性管控，有效提升银行风险识别和防范能力。</p>
	预期效果	<p>1. 降低企业移动支付中信息泄露和欺诈交易风险，提高移动支付安全性。</p> <p>2. 优化中小微企业经营采购和资金结算流程，提高中小微企业经营效率，促进企业数字化转型发展。</p>
	预期规模	按照风险可控原则合理确定用户范围和服务规模，预计年服务中小微企业约 500 家。
创新应用 服务信息	服务渠道	线上渠道
	服务时间	7×24 小时
	服务用户	中小微企业及企业授权使用的个人
	服务协议书	《服务协议书-基于支付标记化的企业移动支付服务》（见附件 1-1）
合法合规 性评估	评估机构	上海银行股份有限公司
	评估时间	2022 年 01 月 05 日
	有效期限	3 年
	评估结论	<p>本应用严格按照《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国消费者权益保护法》《中华人民共和国反洗钱法》《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》（中国人民银行 中国银行业监督管理委员会 中国证券监督管理委员会 中国保险监督管理委员会令（2007）第 2 号发布）、《中国人民银行金融消费者权益保护实施办法》（中国人民银行令〔2020〕第 5 号发布）、《人民币银行结算账户管理办法》（中国人民银行令〔2003〕第 5 号发布）、《金融机构大额交易和可疑交易报告管理办法》（中国人民银行令〔2016〕第 3 号发布）、《金融机构反洗钱和反恐怖融资监督管理办法》（中国人民银行令〔2021〕第 3 号发布）等国家法律法规及金融行业相关政策文件要求</p>

		进行设计开发，在数据收集和使用过程中采取措施保护个人金融信息和用户敏感信息安全，所提供金融服务符合相关法律法规的合规性和风险管控要求，可依法合规开展业务应用。		
	评估材料	《合法合规性评估报告-基于支付标记化的企业移动支付服务》（见附件1-2）		
技术安全性评估	评估机构	上海银行股份有限公司		
	评估时间	2022年01月05日		
	有效期限	3年		
	评估结论	本应用严格按照《中国金融移动支付 支付标记化技术规范》（JR/T 0149—2016）、《移动金融客户端应用软件安全管理规范》（JR/T 0092—2019）、《网上银行系统信息安全通用规范》（JR/T 0068—2020）、《个人金融信息保护技术规范》（JR/T 0171—2020）、《商业银行应用程序接口安全管理规范》（JR/T 0185—2020）、《金融科技创新安全通用规范》（JR/T 0199—2020）、《基于大数据的支付风险智能防控技术规范》（JR/T 0202—2020）、《金融业数据能力建设指引》（JR/T 0218—2021）、《人工智能算法金融应用评价规范》（JR/T 0221—2021）、《金融大数据 术语》（JR/T 0236—2021）、《金融大数据平台总体技术要求》（JR/T 0237—2021）等相关金融行业技术标准规范进行设计开发并进行安全评估。经评估，本应用符合现有相关金融行业标准要求。		
	评估材料	《技术安全性评估报告-基于支付标记化的企业移动支付服务》（见附件1-3）		
风险防控	风控措施	1	风险点	在数据采集、存储、传输、使用等过程，由于技术缺陷或业务管理漏洞可能会造成数据的泄露风险。
		1	防范措施	遵循“用户授权、最小够用、全程防护”原则，充分评估潜在风险，加强数据全生命周期安全管理，严防用户数据的泄露、篡改和滥用风险。数据采集时，通过隐私政策文件、个人信息授权书等方式明示用户数据采集和使用目的、方式以及范围，获取用户明确授权后方可采集。数据存储时，通过数据泛化等技术将原始信息进行脱敏，并与关联性较高的敏感信息进行安全隔离、分散存储，严控访问权限，降低数据泄露风险。数据传输时，采用加密通道进行数据传输。数据使用时，借助标记化等技术，

			在不归集、不共享原始数据前提下，仅向外提供脱敏后的计算结果。
	风险点	2	创新应用上线运行后，可能面临网络攻击、业务连续性中断等方面风险，亟需采取措施加强风险监控预警与处置。
	防范措施	2	在应用实施过程中，将按照《金融科技创新风险监控规范》（JR/T 0200—2020）建立健全风险防控机制，掌握创新应用风险态势，保障业务安全稳定运行，保护金融消费者合法权益。
	风险点	3	随着业务量的不断增加，可能存在企业资金违规使用风险。
	防范措施		事前通过设置交易白名单（包括商户和行业）等方式控制资金使用用途及场景；事中基于支付风控模型筛查可疑或风险交易，对可疑客户及时开展尽职调查，并设置专岗进行人工干预；事后复查可能存在的风险交易，对于确认为风险客户的及时采取终止合作、添加黑名单、上报可疑交易报告等措施控制风险。
	风险补偿机制	本应用按照风险补偿方案（见附件 1-4）建立健全风险补偿机制，明确风险责任认定方式、制定风险赔付机制、配套风险拨备金、保险计划等补偿措施，切实保障金融消费者合法权益。在金融消费者因使用金融服务而出现资金损失时，由上海银行按照风险补偿机制进行赔付。对于非客户自身责任导致的资金损失，提供全额补偿，充分保障消费者合法权益。	
	退出机制	本应用按照退出预案（见附件 1-5），在保障用户资金和信息安全的前提下进行系统平稳退出。 在业务方面，按照退出方案终止有关服务，及时告知客户并与客户解除协议。如遇法律纠纷，按照服务协议约定进行仲裁、诉讼。涉及资金的，按照服务协议约定退还客户，对客户造成资金损失的通过风险补偿机制进行赔偿。 在技术方面，对系统进行下线。涉及数据的，按照国家及金融行业相关规范要求做好数据清理、隐私保护等工作。	
	应急预案	本应用按照应急处置预案（见附件 1-6）妥善处理突发安全事件，切实保障业务稳定运行和用户合法权益。在系统上线前进行全链路压测、容灾演练，对相关操作人员进行应急处置培训；在系统上线后定期开展突发事件处置演练，确保应急预案的全面性、合理性和可操作性。建立日常生产运行监控机制，7×24 小时实时监控系统运行状况，第一时间对核	

		<p>心链路、接口、功能模块、硬件资源等的异常情况进行告警。一旦发生突发事件，根据其影响范围和危害程度，及时采取针对性措施进行分级分类处理，视需要及时关闭增量业务，妥善处置受影响的存量业务，切实保障用户资金和信息安全。</p>	
投诉响应机制	机构投诉	投诉渠道	<p>1. 营业网点 向上海银行各营业网点负责人反映问题。</p> <p>2. 客服电话 致电上海银行客服热线（95594），选择企业客户联系客服。</p> <p>3. 门户网站 通过门户网站（www.bosc.cn），联系在线客服。</p> <p>4. 投诉邮箱 将您的投诉内容编辑成电子邮件，发送至“webmaster@bosc.cn”。</p> <p>5. 传真号码 通过传真号码（021-68476111）发送投诉传真文件。</p>
		投诉受理与处理机制	<p>受理部门：上海银行总行客服中心 受理时间：9:00-17:00 处理流程：在接到投诉事件后，客服人员负责对事件进行了解和分析，在确认投诉原因和相关问题后，协调相关技术部门或业务部门进行处理解决。 处理时限：7个工作日</p>
	自律投诉	投诉渠道	<p>受理单位：中国支付清算协会 投诉网站：<a href="http://cfp.pcac.org.cn/">http://cfp.pcac.org.cn/</a> 投诉电话：010-66001918 投诉邮箱：<a href="mailto:fintechts@pcac.org.cn">fintechts@pcac.org.cn</a></p>
		投诉受理与处理机制	<p>中国支付清算协会是经国务院同意、民政部批准成立的全国性非营利社会团体法人。为保护金融消费者合法权益，营造遵守国家宪法、法律、法规和社会道德风尚的良好金融科技创新监管环境，推动金融科技行业健康可持续发展，按金融管理部门工作要求，协会以</p>

		<p>调解的形式，独立公正地受理、调查以及处理金融科技创新监管工具实施过程中出现的投诉举报等相关事宜。</p> <p>对于涉及相关地区的金融科技创新应用的投诉举报事项，中国支付清算协会将依照规定的程序进行调解，由协会举报中心对投诉情况进行沟通、记录后，相关业务部门负责进行调查处理。</p> <p>对外办公时间：周一至周五 上午 08:30-11:30，下午 13:30-17:00</p>
备注	无	
承诺声明	<p>本机构承诺所提交的材料真实有效，严格遵守相关金融管理要求，并做出以下声明：</p> <ol style="list-style-type: none"> <li>1. 守正创新。忠实履行金融天职和使命，着力解决实体经济痛点难点，确保科技创新不偏离正确的发展方向，严防技术滥用，切实通过技术创新满足人民群众对美好生活的期待与向往。</li> <li>2. 以人为本。始终坚持以人民为中心的发展思想，坚持金融科技创新行为从人民群众实际需求出发，以增进社会共同福祉为目标，尊重并维护人民群众尊严和利益，致力促进社会和谐与文明进步。</li> <li>3. 诚实守信。恪守社会主义核心价值观，将求真务实作为金融科技从业人员的基本素养，将履约践诺作为从事金融科技活动的基本要求，强化诚信道德自律，积极倡导诚实守信的良好社会风尚。</li> <li>4. 公开透明。使用简明清晰、通俗易懂的方式，及时、真实、准确、完整地主动对外披露金融科技创新的功能实质和潜在风险，不隐瞒不利信息、不“劝诱”销售产品，让社会公众看得到、读得懂、能监督。</li> <li>5. 权益保护。充分尊重和保障人民群众隐私权、自主选择权、依法求偿权等合法权益，严格履行适当性义务，严防过度采集、违规使用、非法交易和泄露用户隐私数据行为，采取风险拨备资金、保险计划等补偿机制，切实保护用户资金和信息安全。</li> <li>6. 安全合规。把遵守法律法规和维护金融稳定作为开展金融科技创新活动的前提条件，已通过业务合规性和技术安全性评估审计等措施保障新技术应用风险可控，避免新技术应用带来的数据泄露、算法黑箱、信息茧房等问题，切实防范技术和数据滥用可能导致的人民群众信息与资金失窃风险。</li> <li>7. 公平普惠。应用新一代信息技术优化金融服务供给结构，持续增强金融服务的普适性、可得性和满意度。重点关注特殊人群、弱势群体需求，努力消除因使用成本、文化程度、地域限制等造成的“数字鸿沟”，不断提升人民群众的获得感、幸福感、安全感。</li> </ol>	

8. 社会责任。贯彻落实国家战略部署，围绕新时代经济社会发展的战略目标、战略重点，始终把社会效益放在首位，坚持社会效益和经济效益相统一，开展“负责任的创新”，打造“值得信赖的技术”，切实服务经济社会健康可持续发展。

本声明书正文与附件表述不一致的，以正文为准。

以上承诺如有违反，愿承担相应责任与后果。

法定代表人或其授权人（签字）

2022年7月28日（盖章）



## 附件 1-1

# 企业移动支付服务协议书

本协议由上海银行股份有限公司（以下简称“甲方”）与上海银行股份有限公司企业客户（以下简称“乙方”）就企业移动支付服务（以下简称“本服务”）的相关事项所订立的有效合约，具有合同法律效力。

在使用企业移动支付服务前，乙方应当认真阅读并遵守本协议、《上海银行企业电子银行服务协议》，双方确认《上海银行企业电子银行服务协议》是本协议不可分割的一部分，具有同等法律效力，与本协议相冲突的，以本协议为准。

请乙方务必审慎阅读并充分理解各条款内容，特别是免除或者限制责任的条款、争议解决和法律适用条款。免除或者限制责任的条款可能以加粗字体显示，乙方应重点阅读。除非乙方已阅读并接受本协议所有条款，否则无权使用本服务。乙方通过点击确认或以其他方式选择接受本协议，即表示同意接受本协议的全部约定内容，确认承担由此产生的一切责任。

### 第一条 定义

（一）“上海银行”客户端：指由甲方开发并运营的手机银行 APP、小程序、H5 等电子渠道。以下亦称“甲方客户端”。

（二）企业移动支付服务：指甲方基于乙方的申请及授权，为乙方提供的基于乙方单位结算账户的，可在甲方客户端或其他线上渠道使用的移动化支付服务。

（三）账户：特指基于乙方的申请及授权，开通企业移动支付服务的乙方单位结算账户。

（四）操作员：指乙方在甲方企业网上银行端指定的对本企业移动支付服务具有操作权限的人员，包括复核操作员和制单操作员。

（五）数字证书：指用于存放乙方身份标识，并对乙方发送的交易指令进行数字签名认证，并用于识别乙方身份和权限的电子文件。

(六) 被授权人：指经过乙方授权的使用甲方移动支付服务的乙方员工或其相关人员。乙方需在被授权人信息授权的情况下，在甲方企业网上银行提交其身份信息，被授权人在甲方客户端注册并完成身份认证后，方可使用本移动支付服务。

(七) 支付标记：基于乙方的授权，甲方为乙方被授权人生成的与乙方单位结算账户相关联的支付结算工具，支持乙方被授权人在甲方客户端或其他线上渠道使用支付标记进行支付。

(八) 企业移动支付交易指令（以下或简称“交易指令”）：指乙方通过甲方企业网上银行向甲方发起的服务开通、预授权、查证等交易或乙方被授权人通过甲方客户端发起的支付标记领取、支付标记支付、查证或经由其他线上渠道发起的支付标记支付等交易的指示或要求。针对涉及服务开通及支付标记领取、支付等交易指令，甲方将采用数字证书、交易密码、动态密码、人脸识别等方式进行组合验证。

## **第二条 服务内容**

(一) **服务内容及范围**：乙方通过甲方企业网上银行完成签约申请并勾选确认本协议后即可开通服务，甲方提供的具体服务包括但不限于以下内容：

1. 预授权：指乙方在开通企业移动支付服务后，操作员在甲方企业网上银行上为被授权人进行本服务的使用授权、使用授权的终止，即支付标记的申请、支付标记的停用，以及支付标记的设置，包括限额、有效期、交易类型等。

2. 支付标记领取：由被授权人在甲方客户端发起支付标记领取申请，甲方完成对被授权人身份核验后，被授权人领取支付标记并有权使用本服务。

3. 支付标记使用：被授权人领取支付标记后，可在支付标记设置范围内，使用乙方单位结算账户的资金。

4. 查证交易：包括服务开通状态查询、交易明细查询等。服务开通状态查询及交易记录及交易结果（包括预授权交易、支付标记领取交易、支付标记使用）查询可由乙方操作员在甲方企业网上银行上自行查询或使用；被授权人可在甲方客户端查询其支付标记信息，使用本服务的交易记录及交易结果。

### **第三条 甲方的权利与义务**

（一）为确保乙方开通企业移动支付服务意愿的真实性，甲方有权要求乙方按照甲方要求，线上申请开通本服务，并签署本协议，方可使用企业移动支付服务。

（二）甲方负责保障甲方客户端、企业网银及企业移动支付系统的建设、运行和管理，并尽商业合理努力确保该系统的安全性。

（三）甲方通过甲方企业网银为乙方提供企业移动支付服务功能管理及交易查询服务。

（四）甲方依据乙方设置的被授权人信息及授权权限提供服务，乙方需确保授权信息及授权范围的真实有效，被授权人在授权范围内使用本服务产生的资金支付转移交易均视为乙方行为，被授权人发出的交易指令均视为乙方发出的交易指令，因乙方、乙方被授权人原因导致的交易错误或资金损失等，甲方不承担责任。

（五）甲方仅根据乙方的交易指令为乙方提供资金转移服务，乙方、被授权人与其他主体之间的交易纠纷由乙方自行负责处理，与甲方无关。

（六）甲方将尽商业合理努力保障乙方交易指令的传输稳定与安全，但由于互联网的性质及甲方控制范围以外的网络可能出现非控制的传输问题或其他因素的影响而导致的事故除外。甲方有权随时对其系统进行保养、升级、测试或改造。乙方不得有意诋毁、损害甲方声誉或恶意攻击甲方系统。

（七）乙方存在未按时支付有关费用、不遵守甲方有关业务规定或存在恶意操作、诋毁、损害甲方声誉等情况的，甲方有权单方面终止对乙方提供的本服务，并保留追究乙方责任的权利。乙方利用甲方提供的本服务从事违反国家法律法规活动的，甲方有权按照相关部门的要求停止为其办理业务。

### **第四条 乙方的权利与义务**

（一）乙方自愿申请开通甲方移动支付服务，若乙方有多个企业网上银行及多个账户需要开通服务，则每个企业网上银行编号及账户需单独开通本服务。服务开通完成后，乙方有权根据本协议目的，使用甲方的移动支付服务，并保证遵守本协议约定及相关申请功能。

(二) 乙方确认对于企业移动支付服务的网络、电讯有效性和安全性以及电子交易风险有充分的认识,因乙方的差错、遗漏或者重复发送任何交易指令所造成的任何风险和损失由乙方自行承担。

(三) 乙方获取被授权人身份信息(包括姓名、证件类型、证件号码、联系方式等)需取得被授权人的同意,乙方需确保被授权人授权同意乙方将上述身份信息传输至甲方,乙方及其被授权人须妥善保管身份信息及身份认证方式(包括数字证书、人脸识别、动态密码、交易密码等),不得公开、告知或转交他人。因乙方或乙方被授权人原因导致的身份信息、身份认证方式泄露或遗失造成的损失由乙方承担。

(四) 乙方授权甲方在接收乙方被授权人的交易指令并校验通过后,直接从乙方开通企业移动支付服务的指定账户进行扣款,用于支付乙方被授权人请求付款的金额。乙方应确保其支付行为合法、有效,未侵犯任何各方合法权益;否则因此造成任何各方损失的,乙方应负责赔偿并承担全部法律责任。

(五) 乙方应在其付款账户中保留足够余额或额度,保证甲方能够按照本协议和交易指令及时准确扣款。

(六) 甲方对于乙方、乙方被授权人与其他主体之间就付款金额、商品/服务交易产生的纠纷不承担责任。同时因通过本服务而产生的一切关于购买的商品、服务质量及款项扣收等争议均由乙方、乙方被授权人与其他主体自行协商解决,与甲方无关。

(七) 乙方及乙方被授权人应妥善保管被授权人的身份信息、身份认证方式、企业相关有效证件、绑定手机号码的手机、在其他线上渠道的身份信息及身份认证方式等信息,凡使用乙方被授权人的身份信息及身份认证方式登陆甲方客户端进行的企业移动支付操作以及乙方被授权人通过其他线上渠道向甲方发起的通过甲方校验的交易指令,视为乙方的真实意思表示,发生的任何损失均由乙方自行承担。

(八) 乙方如发现任何人未经授权使用乙方被授权人的身份信息及身份认证方式或其他可能导致乙方被授权人身份信息及身份认证方式被他人盗用的情形,应立即通知甲方,并授权甲方对乙方被授权人采取限制或禁止使用本服务等相关措施直至乙方确认恢复被授权人的正常使用。乙方知晓并理解甲方对乙方的请求采取行动需要合理时间,甲方对在采取行动前已经产生的后果(包括但不限于乙方的任何损失)不承担任何责任。

(九) 甲方未按照协议内容进行付款并造成乙方损失的,甲方应承担相应责任。但因以下情况造成付款请求未能支付,所造成的经济损失及相应责任由乙方承担:

- (1) 甲方接收到的交易指令信息不明确或不完整;
- (2) 乙方账户可用余额或信用额度不足;
- (3) 支付金额高于甲方或乙方设置的限额;
- (4) 乙方的账户状态不正常,包括但不限于账户挂失、冻结、止付等;
- (5) 有权机关依法对账户执行冻结或扣划等措施;
- (6) 乙方的行为出于欺诈或其他非法目的;
- (7) 在甲方公告的非正常交易时间内提交的交易指令;

(8) 由于不可抗力因素、计算机黑客袭击、系统故障、通讯故障、网络拥堵、供电系统故障、电脑病毒、恶意程序攻击及其他不可归因于甲方的非人为因素造成系统无法受理的情况;

(9) 法律、法规或监管部门规定的其他情况。

(十) 如因不可抗力因素、通讯故障、网络拥堵等不可归因于甲方的非人为因素造成乙方不当得利的,乙方同意甲方有权从其账户中扣划乙方的不当得利所得。当乙方账户余额不足时,乙方应在接到甲方通知后及时补缴不当得利所得。对于拒绝补缴的,甲方有权根据需要暂停乙方对应账户的相关服务。

(十一) 乙方不得利用本服务进行虚假交易、洗钱等行为,且有义务配合甲方进行相关调查,一旦乙方拒绝配合进行相关调查或由甲方认定存在或涉嫌虚假交易、洗钱、或任何其他非法活动、欺诈或违反诚信原则的行为,甲方有权暂停或终止提供本协议项下服务。

(十二) 乙方有权解除本协议,但应由乙方通过甲方营业网点、或通过甲方企业网上银行进行协议解除。乙方在协议终止前发出的所有指令仍为有效指令,由乙方承担相应责任。

## **第五条 信息保密与使用**

(一) 甲方在法律允许的前提下,为业务和管理需要,可收集、处理、传递及应用乙方在甲方企业网上银行上提交的乙方信息。

(二) 甲方收集乙方信息的目的：依法合规地为乙方提供优质的产品（或服务），该信息对于充分履行甲乙双方之间的合约很有必要，并使得甲方能够遵守相关法律，具体可能包括：

- 1) 为保护乙方的账户安全，对乙方的身份进行识别、验证等；
- 2) 为评估乙方的履约能力及履约状况，用于业务准入和风险控制；
- 3) 为乙方提供产品（或服务）所必须（包括但不限于企业移动支付服务等）；
- 4) 为保护乙方的资金安全；
- 5) 为履行法定义务（如反洗钱义务等）；
- 6) 经乙方许可的其他用途。

(三) 甲方收集乙方信息的方式：

- 1) 甲方为乙方提供金融服务时，乙方主动向甲方提供的身份信息；
- 2) 甲方为乙方提供金融服务过程中形成的与服务相关的信息；
- 3) 经乙方授权，向合法留存乙方信息的自然人、法人以及其他组织、电信运营商收集的，与甲方为乙方提供的金融服务相关的必要信息；
- 4) 经乙方许可的其他方式和信息。

(四) 甲方收集乙方信息的内容和范围：

甲方通过乙方提供的企业名称、组织机构代码、对公结算账户、法人姓名、法人联系方式，为乙方开通本服务；

(五) 甲方会依法使用乙方所授权的信息，并对相关的信息保密。但由于技术水平局限以及可能存在的恶意攻击，有可能出现甲方无法合理预见、防范、避免、控制的意外情况。互联网并非绝对安全的环境，乙方需要妥善保管身份信息，协助甲方保证乙方的信息安全。

(六) 如发生信息安全事件，甲方将按照法律法规要求，及时将事件相关情况以邮件或信函或电话或推送通知等方式告知乙方，或采取合理、有效的方式发布公告。同时，甲方还将依据监管规定，主动上报信息安全事件处置情况。

(七) 甲方应依法为乙方在甲方开通的企业移动支付服务的各种信息保密。未经乙方许可, 甲方不得向任何第三人提供或许可第三人使用乙方信息; 但依照法律、法规规定应向有权机关(包括但不限于向征信机构)披露, 或银行为完善服务, 必须向相关外包服务提供商提供, 或乙方违反本协议及业务规则, 甲方需将平台用户信息、违约信息向有关第三方公开披露的除外。

(八) 乙方理解并同意, 为提高甲方企业移动支付服务的安全性, 更好地预防钓鱼网站、欺诈、网络漏洞、计算机病毒、网络攻击、网络侵入等安全风险, 更准确地识别违反法律法规或本平台协议及相关规则的情况, 甲方可能使用或整合乙方的注册信息、交易信息、设备信息、有关网络日志以及关联公司、合作伙伴取得乙方授权或依据法律共享的信息, 来综合判断乙方交易风险、进行身份验证、检测及防范安全事件, 并依法采取必要的记录、审计、分析、处置措施。

(九) 乙方理解并同意, 乙方主动向甲方提供数据信息、授权甲方主动获取或收集乙方在使用甲方本服务过程中留存于甲方的数据信息, 甲方为优化、提高对乙方的服务水平及质量, 将会对前述数据进行分析、整合, 经甲方分析、整合后的数据所有权归甲方享有。

## **第六条 收费**

(一) 乙方授权甲方根据中国人民银行、中国银行保险监督管理委员会等有权机关及甲方的相关规定, 向乙方在甲方办理的企业移动支付收取服务相关的费用。甲方应通过官方网站公示费用标准。

(二) 在乙方存续期间, 甲方可以在符合法律法规和有关政策的前提下决定调整与本服务相关的收费事项, 包括但不限于调整收费项目、收费标准、收费对象、收费时间或收费方式等, 但甲方应在上述调整生效前 10 个工作日通过甲方的官方网站公告相关事项。如乙方不同意调整后的费用标准的, 可向甲方申请关闭本服务, 本协议即行终止, 如乙方继续使用本服务的, 则视为乙方同意调整后的费用标准。

## **第七条 责任免除**

(一) 本协议如与国家新颁布的法律、法规、监管规定等相抵触, 以国家新颁布的法律、法规、监管规定为准。在本协议生效期间, 因法律、法规或监管规定的变化而致使本协议无法履行的, 双方均有权终止本协议的履行, 并互不承担违约责任。

(二) 因下列状况导致甲方无法正常运作, 使乙方无法正常使用本服务时, 甲方不承担损害赔偿责任, 但甲方有义务及时采取措施, 尽快排除故障、处置紧急事件, 恢复正常的服务秩序。该状况包括但不限于:

(三) 甲方预先通知乙方后进行系统维护所引起的, 包括维修、升级和模拟故障演练等原因造成的本平台服务中断或延迟。因台风、地震、海啸、洪水、停电、战争、恐怖袭击等不可抗力之因素, 造成甲方系统故障不能执行业务的。由于计算机病毒、黑客攻击或其他恶意程序的破坏等原因而造成的甲方数据丢失、泄漏。由于网站升级、电信部门技术调整或故障、第三方服务机构系统的问题等原因而造成的甲方提供的本服务中断、延迟。

## **第八条 其他**

(一) 本协议自乙方在企业网银本服务的签约界面上确认或以其他方式选择接受后生效, 至乙方关闭本服务后终止。

(二) 甲方如变更本协议, 应通过甲方营业网点、企业网银等方式公告变更内容。相关公告发布即视为乙方已收到。在公告发布后乙方继续办理本服务的, 视同接受本协议的变更, 如乙方不同意本协议的变更, 应停止使用本服务, 且按照本协议约定的方式解除协议。

(三) 甲乙双方在履行本协议的过程中如发生争议, 可协商解决; 协商不成的, 任何一方应向甲方所在地的人民法院提出诉讼。

(四) 本协议未尽事宜, 应按照中国人民银行、中国银行保险监督管理委员会等监管机构的要求、相关法律法规及乙方的相关规章制度执行。监管机构的要求和相关法律法规的规定与本协议约定内容有冲突的, 以监管机构的要求和相关法律法规的规定为准。

### **重要提示:**

乙方已仔细阅读上述条款, 并全面、准确地理解条款内容, 乙方对本协议条款内容均无疑义, 并对双方权利义务和责任限制、免除责任条款的法律含义有准确无误的理解。

(以下无正文)

## 附件 1-2

# 基于支付标记化的企业移动支付服务 合法合规性评估报告

本应用严格按照《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国消费者权益保护法》《中华人民共和国反洗钱法》《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》（中国人民银行 中国银行业监督管理委员会 中国证券监督管理委员会 中国保险监督管理委员会令〔2007〕第 2 号发布）、《中国人民银行金融消费者权益保护实施办法》（中国人民银行令〔2020〕第 5 号发布）、《人民币银行结算账户管理办法》（中国人民银行令〔2003〕第 5 号发布）、《金融机构大额交易和可疑交易报告管理办法》（中国人民银行令〔2016〕第 3 号发布）、《金融机构反洗钱和反恐怖融资监督管理办法》（中国人民银行令〔2021〕第 3 号发布）等国家法律法规及金融行业相关政策文件要求进行设计开发，在数据收集和使用过程中采取措施保护个人金融信息和用户敏感信息安全，所提供金融服务符合相关法律法规的合规性和风险管控要求，可依法合规开展业务应用。

上海银行股份有限公司

2022 年 01 月 05 日

## 附件 1-3

# 基于支付标记化的企业移动支付服务 技术安全性评估报告



本应用严格按照《中国金融移动支付支付标记化技术规范》（JR/T 0149—2016）、《移动金融客户端应用软件安全管理规范》（JR/T 0092—2019）、《网上银行系统信息安全通用规范》（JR/T 0068—2020）、《个人金融信息保护技术规范》（JR/T 0171—2020）、《商业银行应用程序接口安全管理规范》（JR/T 0185—2020）、《金融科技创新安全通用规范》（JR/T 0199—2020）、《基于大数据的支付风险智能防控技术规范》（JR/T 0202—2020）、《金融业数据能力建设指引》（JR/T 0218—2021）、《人工智能算法金融应用评价规范》（JR/T 0221—2021）、《金融大数据术语》（JR/T 0236—2021）、《金融大数据平台总体技术要求》（JR/T 0237—2021）等相关金融行业技术标准规范进行设计开发并进行安全评估。经评估，本应用符合现有相关金融行业标准要求。

上海银行股份有限公司

2022年01月05日

## 基于支付标记化的企业移动支付服务 风险补偿机制

本应用按照风险补偿方案建立健全风险补偿机制，明确风险责任认定方式、制定风险赔付机制、配套风险拨备金、保险计划等补偿措施，切实保障金融消费者合法权益。在金融消费者因使用金融服务而出现资金损失时，由上海银行按照风险补偿机制进行赔付。对于非客户自身责任导致的资金损失，提供全额补偿，充分保障消费者合法权益。

风险补偿原则：坚守银行社会责任，遵从公平交易原则，依法维护银行业消费者的合法权益。

具体措施：

1、确保风险补偿受理渠道通畅。客户可通过客服电话95594提出投诉意见和赔付要求；

2、明确责任承担，制定赔付机制。因产品或技术等原因致使客户权益遭受损害的，由上海银行依据相关法律法规或双方约定对客户进行赔付；

3、配套风险补偿资金池。对于业务试点开展过程中因各类风险事件导致的客户损失进行赔偿。

## 基于支付标记化的企业移动支付服务 退出机制

本应用按照退出预案，在保障用户资金和信息安全的前提下进行系统平稳退出。

在业务方面，按照退出方案终止有关服务，及时告知客户并与客户解除协议。如遇法律纠纷，按照服务协议约定进行仲裁、诉讼。涉及资金的，按照服务协议约定退还客户，对客户造成资金损失的通过风险补偿机制进行赔偿。

在技术方面，对系统进行下线。涉及数据的，按照国家及金融行业相关规范要求做好数据清理、隐私保护等工作。

具体机制如下：

### 一、退出条件

因法律法规、监管意见等合规管理要求，或在产品设计、产品试点运行过程中遇到存在重大缺陷且无法解决的问题，致使产品无法继续提供服务的，启动本产品退出处理预案。

### 二、退出安排

1、业务：停止新增业务，及时告知客户并解除协议，稳妥处置存量业务并逐步退出；

2、系统：回退至正常版本，下线试点业务内容；

3、数据：按照国家及金融行业相关规范要求做好业务数据备份、用户数据清理、隐私保护等工作；



如遇法律纠纷，按照服务协议约定进行仲裁、诉讼。涉及资金的，按照服务协议约定退还客户，对客户造成资金损失的通过风险补偿机制进行赔偿。

## 附件 1-6

# 基于支付标记化的企业移动支付服务 应急预案



本应用按照应急处置预案妥善处理突发安全事件，切实保障业务稳定运行和用户合法权益。

### 1、系统日常监控

在系统上线前进行全链路压测、容灾演练，对相关操作人员进行应急处置培训；在系统上线后定期开展突发事件处置演练，确保应急预案的全面性、合理性和可操作性。建立日常生产运行监控机制，7×24 小时实时监控系統运行状况，第一时间对核心链路、接口、功能模块、硬件资源等的异常情况進行告警。

### 2、系统中断应急预案

总体原则：对于突发事件，根据其影响范围和危害程度，及时采取针对性措施进行分级分类处理，视需要及时关闭增量业务，妥善处置受影响的存量业务，切实保障用户资金和信息安全。

1) 业务中断预案：暂停增量业务的处理，妥善处置存量业务，对受影响的客户做好解释工作，对于客户非紧急处理业务，建议延期办理业务，对于紧急处理业务，视具体情况采用渠道切换、人工处理等方式；

2) 灾备：依照上海银行业务连续应急预案（灾难恢复）

执行。