

《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-2025-0001	
	创新应用名称	基于大模型技术的手机银行支付便利化服务	
	创新应用类型	金融服务	
	机构信息 1	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	2025 年 7 月	
	技术应用	1. 运用语音识别技术，将客户的语音转化为文字内容，作为输入用于后续自然语言处理，实现高效人机交互服务。 2. 运用自然语言处理技术，识别客户以自然语言提出的问题和指令，提取为文本数据内容，提供给人工智能进行意图理解。 3. 运用人工智能技术，基于人工智能的语义理解、推理和生成能力，处理客户提出的各种类型问题；基于智能体理解客户需求 and 情绪，提供准确、自然、流畅的回答，或引导客户进入相应业务流程。	
	功能服务	本应用综合运用自然语言处理和语音识别等人工智能技术，在客户使用手机银行时通过自然语言交流实现问候、主动对话、业务功能操作引导、明细查询、信用卡账单查询等功能，辅助客户完成线上支付交易流程，进一步降低金融服务门槛，提升老年群体移动支付服务体验。不直接涉及资金办理业务。本应用由上海银行负责提供金融应用场景设计、模型训练与部署，阿里云提供技术与运维服务，此外无其他机构参与。	
	创新性说明	1. 在数据应用方面，通过对客户的行为数据、历史对话、客户信息等进行分析，高效识别客户潜在需求，为客户提供定制化的推荐和服务，提升服务效率和温度。 2. 在技术创新方面，基于大语言模型与人工智能技术，不仅能够准确理解客户在各种服务场景（如问候、主动对话、转账等）下的自然语言指令，还能以自然流畅的语言进行回应	

		和引导，提高语义理解准确性和客户交互体验。 3. 在客户服务方面，通过客户问答等方式，能够高效识别客户情绪和需求，快速提供客户办理业务的相关流程指引等，为客户提供个性化的服务引导，优化客户服务体验。
	预期效果	通过智能语音交流的方式纾解老年客户“找不到”“看不懂”等手机银行操作难问题，提高业务办理效率与客户满意度，提升老年群体移动支付服务体验。
	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，预计服务手机银行客户 20 万人。
创新应用 服务信息	服务渠道	手机银行 APP
	服务时间	7 × 24 小时
	服务用户	个人用户
	服务协议书	本应用服务协议书包括： 《上海银行手机银行用户隐私政策》（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网络金融部
	评估时间	2025 年 03 月 12 日
	有效期限	3 年
	评估结论	本应用严格按照《中华人民共和国民法典》、《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》、《中华人民共和国消费者权益保护法实施条例》（中华人民共和国国务院令 第 778 号公布）、《支付结算办法》（银发〔1997〕393 号）、《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）、《银行保险机构消费者权益保护管理办法》（中国银行保险监督管理委员会令 2022 年第 9 号公布）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。本应用严格按照《互联网信息服务深度合成管理规定》（国家互联网信息办公室 中华人民共和国工业和信息化部 中华人民共和国公安部令 第 12 号公布）履行备案手续。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-基于大模型技术的手机银行支付便利化服务》（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金融科技部、数据管理与应用部		
	评估时间	2025 年 05 月 08 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）、《个人信息信息保护技术规范》（JR/T 0171—2020）、《移动金融客户端应用软件安全管理规范》（JR/T 0092—2019）、《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）、《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）、《金融领域科技伦理指引》（JR/T 0258—2022）、《网络安全技术人工智能生成合成内容标识方法》（GB 45438-2025）、《中国人民银行业务领域数据安全管理办法》（中国人民银行令〔2025〕第 3 号）等相关金融行业技术标准规范要求进行设计开发并进行全面安全评估。经评估，本应用符合现有相关行业标准要求。		
	评估材料	《技术安全性评估报告-基于大模型技术的手机银行支付便利化服务》（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。
			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，借助加密技术，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。

		2	风险点	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	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。
		3	风险点	AI 银行与客户的交互可能存在理解不准确、回答不合理等问题，影响客户体验。
			防范措施	一是针对银行、金融、客服相关话题，设置评估指标和测试集，通过监控指标异动及时发现模型潜在问题及优化。二是使用人工与自动化相结合的方式定期分析日志数据，使用大量多样化的真实数据进行训练和测试，不断优化模型，提升数据质量。三是不断优化智能体，提高模型的语言理解和生成能力，定期评估模型能力，及时调整和改进模型，确保有效控制相关潜在风险。
		4	风险点	人工智能可能产生幻觉问题，对输出可靠性带来影响。
			防范措施	①事前：通过内外部服务安全评测，测试问题数千条，涵盖社会主义核心价值观、道德伦理、银行业务合规性等维度。经内部自评及第三方机构（阿里云、财跃星辰）测评，评测结论符合安全标准。 ②事中：制定安全拦截策略。如：建立社会危害词等敏感词黑名单，针对生成内容实时监控，拦截违规内容，确保生成内容的安全性。构建用户情绪实时识别机制，在对话过程中捕捉客户质疑等负面情绪，即时开展安抚工作，并完整记录问题，为后续优化提供依据。 ③事后：持续完善安全拦截策略，根据业务前台用户反馈、技术后台自动化监控预警，定期更新敏感词黑名单；设置安全风险等级，监控 AI 手机银行平台的系统使用情况，可关闭开放式聊天功能；建立监测预警，通过行内已有通道实时监控舆情，重点关注社交媒体、新闻平台和论坛；建立信息发布审核机制，确保发布的知识库、活动等内容合规，并支持快速下线；

			完善应急处置，对技术故障立即修复，及时跟踪。
	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，配套风险拨备资金、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	本应用按照退出机制（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。系统日常监控方面，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，第一时间对核心链路、接口、功能模块、硬件资源等的异常情况进行告警。系统中断应急预案方面，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。	
投诉响应机制	机构投诉	投诉渠道	1、营业网点 向上海银行各营业网点负责人反映问题。 2、客服电话 致电上海银行客服热线（95594）。 3、门户网站 通过门户网站（www.bosc.cn），联系在线客服。 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”。

		投诉受理与处理机制	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
	自律投诉	投诉渠道	受理单位：中国支付清算协会 投诉网站：http://cfp.pcac.org.cn/ 投诉电话：010-66001918 投诉邮箱：fintechts@pcac.org.cn
		投诉受理与处理机制	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。 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。 对外办公时间：周一至周五 上午 8:30-11:30，下午 13:30-17:00
备注	无		
承诺声明	本机构承诺所提交的材料真实有效，遵守国家相关法律法规规定和社会公序良俗，严格落实金融管理部门相关监管要求，认真执行行业相关规则规范，强化全流程风控管理体系建设，有效识别、评估、监测和控制风险，并做出以下声明：		

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。

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。

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。

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。

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。

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。

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。

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）

年 月 日 (盖章)

附件 1-1

上海银行手机银行用户隐私政策

尊敬的上海银行手机银行用户（以下简称“您”），上海银行股份有限公司（以下简称“我行”）重视用户的隐私，您在使用上海银行手机银行 App（以下或简称为“手机银行 App”、“手机银行”、“App”）时，我行将按照《上海银行手机银行用户隐私政策》（以下简称“本政策”）收集、存储、使用及对外提供您的个人信息。为了保证对您的个人隐私信息合法、合理、适度的收集、使用，并在安全、可控的情况下进行传输、存储，我行制定了本政策，请您仔细阅读本政策并确认了解我行对您个人信息的处理规则。阅读过程中，如您有任何疑问，可联系我行的客服（服务热线：95594）咨询。对本政策中与您的权益存在重大关系的条款和个人敏感信息，我行采用粗体字进行标注以提示您注意。如您点击或勾选“同意”并确认提交，即视为您同意本隐私政策，并同意我行将按照本政策来收集、使用、存储和共享您的相关信息。

本政策将帮助您了解以下内容：

一、我行如何收集和使用您的个人信息

二、我行如何使用 Cookie 技术

三、我行如何共享、转让和公开披露您的个人信息

四、我行如何存储和保护您的个人信息

五、您的权利

六、我行如何保护未成年人信息

七、第三方收集和使用您信息的情况

八、本政策如何更新

九、如何联系我行

一、我行如何收集和使用您的个人信息

个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。个人信息包括姓名、出生日期、身份证件信息（身份证、护照等）、个人生物识别信息、通信通讯联系方式、住址、职业信息、账户信息、财产状况、位置信息、行为信息、设备信息、网络信息、正在运行程序等。个人敏感信息是指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的信息，主要包括：身份证件信息（身份证、护照等）、个人生物识别信息、银行账号、征信信息、财产信息、交易信息、位置信息、健康生理信息等。

（一）我行收集个人信息的原则

我行收集您的个人信息遵循合法、正当、必要的原则。我行按照法律法规要求以及业务需要收集您的个人信息，不会收集与业务无关的信息或采取不正当方式收集信息。

（二）我行收集您的个人信息的目的

我行收集您的个人信息，目的在于依法合规地为您提供优质的产品（或服务），该信息对于充分履行您和我行之间的合约很有必要，并使得我行能够遵守相关法律，具体可能包括：

1. 为保护您的账户安全，对您的身份进行识别、验证等；
2. 为评估您的履约能力及履约状况，用于业务准入和风险控制；
3. 为您提供产品（或服务）所必须（包括但不限于为购买理财类产品进行的风险承受能力评估问卷、为评估您的风险偏好，合理提供产品推介和投资建议等）；
4. 为保护您的资金安全；
5. 为履行法定义务（如反洗钱义务等）；
6. 经您许可的其他用途。

（三）我行收集您的个人信息的方式

1. 我行为您提供金融服务时，您主动向我行提供的个人信息；
2. 我行为您提供金融服务过程中形成的与服务相关的信息；
3. 向征信机构、信用管理公司、资信评估机构或有关法律、监管机构许可的类似机构采集您的信用信息和行为信息；
4. 向政府机构、司法机关及其他国家机构（如人民银行、公安部、人力资源和社会保障部门、公积金管理中心、中国互联网金融协会等机构）采集的，与我行为您提供的金融服务相关的必要信息，如您的身份信息、工商信息、税务信息、诉讼信息、社保信息、通讯标签信息等；
5. 经您授权，向合法留存您信息的自然人、法人以及其他组织、电信运营商收集的，与我行为您提供的金融服务相关的必要信息；

6. 经您许可的其他方式和信息。

7、为了向您提供优质服务，上海银行需要获取以下权限和信息。
系统将弹框提示，建议您允许我行获取相关权限。

(1) 获取电话权限（设备状态）

用于确定设备识别码（Android ID），以保证账号登录的安全性。拒绝授权后，您将无法登录手机银行 App。

(2) 获取应用列表信息

用于手机银行 App 判断自身应用状态，我行手机银行不会保存您的应用列表信息。如您拒绝授权应用列表权限，我行手机银行将不会读取应用列表内容，不影响您正常使用手机银行 App 的其他可使用功能。

(3) 存储权限

用于缓存您在使用手机银行 App 过程中产生的文本、图像、视频内容，拒绝授权后，将不影响您正常使用手机银行 App 可用的功能。

(4) 摄像头

用于识别二维码、人脸识别认证、转账时拍照识别卡号、扫一扫、ETC、在线客服等。

(5) 相册

用于上传照片设置您的头像。我行获得的图片信息，加密后存储于数据库中。如您拒绝授权，您将无法使用这些功能，但这不影响您正常使用手机银行的其他功能。

（6）获取位置信息

用于交易风控，包括网点预约、预约取款、信义贷申请等。如您拒绝授权，您将无法使用上述功能，但这不影响您正常使用手机银行的其他功能。

（7）麦克风

用于语音搜索功能。如您拒绝授权、您将无法使用这些功能，但这并不影响您正常使用其他功能。

（8）蓝牙

用于通过蓝牙将客户手机与第三方设备连接并交互。拒绝授权后，无法通过蓝牙激活第三方设备。我行系统后台不保存客户手机蓝牙配置信息。

（9）手机短信

用于动态密码接收，系统后台不保存短信内容。如您拒绝通讯信息（短信）授权，我行手机银行将不读取短信内容。

（10）手机通讯录

在手机号转账、汇款短信通知、推荐有礼、使用智能助理进行语音转账、话费充值过程中，我行将收集您的手机通讯录用于协助您通过通讯录快速选取电话号码，无需您手动输入。拒绝授权后，上述功能仍可以使用，但需要手工输入手机号码。

（11）消息推送通知权限

用于消息推送提醒功能。如您不需要相关功能，可以在“首页-消息中心-消息中心设置”中关闭相应的通知服务。关闭后，您将无法再收到消息推送。

（12）Siri

用于 Siri 唤起功能，上述功能可能需要您在您的设备中向我行开启您的设备、存储、相机（摄像头）、相册、地理位置（位置信息）、手机通讯录、短信、麦克风、网络通讯、蓝牙、应用列表、日历的访问权限，以实现这些功能所涉及的信息的收集和使用。请您注意，您开启这些权限即代表您授权我行可以收集和使用这些信息来实现上述功能，如您取消了这些授权，则我行将不再继续收集和使用您的这些信息，但同时也无法为您提供上述与这些授权所对应的功能。

（13）ANDROID ID

用于设备绑定管理时设备进行绑定、解除绑定时对设备可靠性的校验。如您拒绝授权，在手机设备绑定或解绑时可能会失败，但不影响您正常使用手机银行 App 的其他功能。

（14）读取剪贴板

用于快速转账及口令识别。拒绝授权后，手机银行无法提供相关便捷服务。我行仅在本地访问剪贴板内容，不会收集、存储您的任何剪贴板信息，且单独的剪贴板信息无法识别您的个人身份。

（15）自启动和关联启动

为了让您体验 APP 消息离线提醒功能，提供更优质的服务，APP 在必要时会开启自启动或关联启动功能。我们会向您推送平台信息（如动账消息通知），您可以在“消息中心设置”中选择开启/关闭通知权限。

（16）指纹

用于登录及小额转账。拒绝授权后，手机银行无法提供相关便捷服务。

8、当您在手机银行 App 上进行人脸识别核实身份时，我行会采集您的人脸信息，并将加密后存储于系统后台数据库中，用于业务办理过程留存、辅助识别和核实客户身份。如您注销手机银行 App，我行将不再收集和使用您的人脸信息。对于某些品牌或型号的手机终端自身的本地生物特征认证功能，如人脸识别、指纹识别功能，其信息由手机终端提供商进行处理，我行不留存您应用手机终端相关功能的信息。

（四）我行如何收集您的个人信息

1. 当您在上海银行手机银行 App 上注册时，依据法律法规及监管要求，我行会收集并验证您的姓名、证件类型、证件号码、手机号码信息、短信验证码、银行账号，以帮助您完成用户注册，如果您拒绝提供这些信息，您可能无法完成注册或无法正常使用我行的服务。

2. 当您使用上海银行手机银行 App 功能或服务时，在下列情形中，您可能需要向我行提供或授权我行收集相应服务所需的个人信息。如您

拒绝提供部分功能或服务所需信息，您可能无法使用部分功能或服务，但这不影响您正常使用上海银行手机银行 App 的其他功能或服务。

(1) 在您注册成为我行用户或使用我行服务时，您需提供**您本人的手机号码**，我行将通过发送短信验证码的方式来验证您的身份是否有效。根据相关法律法规的规定，您需通过身份基本信息多重交叉验证后方可使用我行的部分服务，如果您需使用此类服务，则可能需提供**姓名、证件、卡号、手机号**以完成身份基本信息多重交叉验证。同时，为了验证您提供信息的准确性和完整性，我行会与合法留存您的信息的国家机关、金融机构、企事业单位进行核对；如在验证核对过程中我行需要向前述验证机构收集您的信息，我行会依照法律法规的规定要求相关验证机构说明其个人信息来源，并对其个人信息来源的合法性进行确认。

(2) 当使用转账汇款功能时，您需要提供**收款方的姓名、银行账号/手机号、开户银行名称**，并需要提供**您的姓名、付款卡号、证件类型及证件号码**，同时可能采用验证密码、指纹、面容、短信验证码和人脸识别的手段以便于验证您的身份及使用上述功能的支付服务。此外，我行还会收集**您的收款人姓名、收款人账号、收款银行名称**，形成收款人名册，以简化您的转账操作。上述信息属于个人敏感信息，如您拒绝提供该信息，仅会使您无法使用上述功能，但不影响您正常使用上海银行手机银行 App 的其他功能。

(3) 当使用手机银行支付、二维码支付功能等支付功能时，我行需要您提供您的**姓名、身份证号、身份证有效期、手机号码、银行卡号**，

同时可能采用验证密码、指纹、面容、短信验证码和**人脸识别**的手段以便于验证您的身份及使用上述功能。此外，我行还会收集**您的收付款交易信息**，形成交易记录，以简化您的查询操作。上述信息属于个人敏感信息，如您拒绝提供该信息，仅会使您无法使用上述功能，但不影响您正常使用上海银行手机银行 App 的其他功能。

（4）当您使用信用卡还款功能时（含自动还款授权），如您选择使用他行借记卡还款，您需要提供**付款方的姓名、银行账号/手机号**，同时可能采用验证密码、指纹、面容、短信验证码和**人脸识别**的手段以便于验证您的身份。此外，我行还会收集**您的付款银行账号、付款银行名称**，以简化您的还款操作。上述信息属于个人敏感信息，如您拒绝提供该信息，仅会使您无法使用上述功能，但不影响您正常使用上海银行手机银行 App 的其他功能。

（5）当您用信用卡电子账单签约功能时，您需提供**有效电子邮箱**，如未提供或提供的相应信息不准确，仅会使您无法使用上述功能，但不影响您正常使用上海银行手机银行 App 的其他功能。

（6）为了让您及时掌握信用卡寄送状态，您可选择卡片邮寄进度查询功能。您需在您的设备上完成证件信息的验证，我行仅接收验证结果，并不收集您的证件信息。如您不需要使用上述功能，可以不提供上述证件信息，不影响您正常使用其他功能。

（7）您可以通过搜索来精准地找到您所需要的商品或服务。我行会保留或统计**您的搜索关键词信息和点击数据**，以方便您重复输入或为

您展示与您搜索内容相关联的商品或服务。请您注意，您的搜索关键词信息无法单独识别您的身份，不属于您的个人信息，为了给您和其他用户提供更高效率的搜索服务，我行有权对其进行使用；只有当您的搜索关键词信息与您的其他信息相互结合使用并可以识别您的身份时，则在结合使用期间，我行会将您的搜索关键词信息作为您的个人信息，与您的搜索历史记录一同按照本隐私政策对其进行处理与保护。

(8) 当您使用短信动账提醒及 App 动账消息服务时，我行会收集您的交易卡号、交易时间、对方户名、对方银行、对方账户信息，以便及时向您发送账户资金变动及相关交易通知。

(9) 为了让您更安全、便捷地使用登录服务，在登录时，我行会收集您的手机号、证件号、登录密码、短信验证码、交易密码、面部信息，以便进行身份验证。如您的设备与上海银行手机银行 App 版本均支持指纹或面容功能，您可选择开通指纹或面容登录功能，通过在您的设备上完成指纹或面容验证进行登录。我行仅接收验证结果，并不收集您的指纹或面容信息。如您不想使用指纹或面容验证，仍可通过其他方式进行登录。

(10) 为了让您更安全、便捷地使用转账、支付服务，如您的设备与上海银行手机银行 App 版本均支持指纹或面容功能，您可选择开通指纹或面容支付功能，您可选择开通指纹或面容支付功能通过在您的设备上完成指纹或面容验证进行转账、支付我行仅接收验证结果，并不收集您的指纹、面容信息。如您不想使用指纹验证，仍可通过其他方式进行支付。

(11) 当您购买我行代销的由基金公司、银行理财子公司、保险公司、贵金属公司、信托或资产管理公司发行或提供的产品时，我行将遵照法律法规、监管要求，并基于您与上述公司的具体交易相应收集您的姓名、性别、国籍、职业、地址、邮政编码、联系方式、证件类型、证件号码、证件有效期、税收居民身份信息、交易账号/投资人理财账户、银行卡号、投资人基金账号、邮箱、年收入、客户风险承受能力等级、交易及所购买的产品信息、录音录像信息（如有），以便于完成代销产品的购买确认。如果您不提供本款所列信息，您可能无法购买相关产品。

(12) 当您使用贷款申请（含信义贷、家装信义贷）、签约、提款功能时，我行将收集您的姓名、身份证件号码、手机号码、户籍所在地、公司地址、公司名称、月收入、教育状况、职业类型、住址联系人信息（关系、姓名、联系电话）、人脸信息，以及地理位置信息（用于交易风控）、设备硬件信息、设备操作系统版本、加速传感器信息，并查询第三方机构数据信息，用于评估您的贷款资质。如您拒绝提供以上相关信息，可能会影响您使用贷款申请\签约\提款功能，但这不影响您正常使用手机银行的其他功能。

(13) 当您更新基金签约信息时，我行将收集您的姓名、身份证件号码、手机号码、住址信息。如您拒绝提供以上相关信息，可能会影响您更新基金签约信息，但这不影响您正常使用手机银行的其他功能。

(14) 当您使用网点服务等基于地理位置的功能时，我行会收集您的位置信息，目的是为了向您提供所在位置的相应服务。如您拒绝提供

该信息，您将无法使用上述功能，但这不影响您正常使用手机银行的其他功能。

(15) 当您使用网点预约中的借记卡挂失补发、存单/存折挂失补发、借记卡开户、申请存款证明功能时，我行会收集您的**姓名、账号、证件号码、详细地址**信息。如您拒绝提供该信息，您将无法使用上述功能，但这不影响您正常使用手机银行的其他功能。

(16) 当您使用手机号转账等涉及通讯录的功能时，我行仅获取您从通讯录中点选的**联系人姓名、手机号**信息，并进行加密传输防止恶意截取。上述信息属于个人敏感信息。如您不需要使用上述功能，可以不提供该信息，不影响您正常使用其他功能。

(17) 当您使用银行卡申请、社保卡申请、添加银行卡等手机银行提供的实名认证服务时，您可能需提供您的**姓名、证件类型、证件号码、银行卡号/账号、手机号、设备信息、位置信息、指纹认证、刷脸认证信息**，且可能会通过验证账号/卡密码、短信验证码方式，对您提供的有关信息进行有效性校验，并对您的操作进行身份安全核验。如您不提供上述信息，我行将无法向您提供需完成实名认证后方可使用的产品或服务。

(18) 当您使用上海银行手机银行 App 在商家进行消费时，我行需要按照法律法规及监管规定对商家进行管理，防范套现或欺诈风险，因此，我行将直接收集或向商家收集您的**交易信息**，包括**交易金额、交易**

对象、交易商品、交易时间、订单信息（如有）。如您不同意我行记录前述信息，则可能无法完成交易，但不影响您使用我行提供的其他服务。

（19）您在手机银行 App 上参加步数保活动时，我行会收集您的**运动与健康信息**，用于给您提供步数计算服务。拒绝提供这些信息仅会使您无法参加步数保活动，但不影响您使用手机银行 App 的其他功能。

（20）您在手机银行 App 设置信用卡的查询密码、交易密码，启用信用卡，我行会收集您的**姓名、手机号码、身份证件号码、卡号、卡片有效期、CVV2**。如您不同意我行记录前述信息，则可能无法完成交易，但不影响您使用我行提供的其他服务。

（21）您在手机银行 App 使用学杂费、医保缴费等生活类服务，我行会收集您的**身份证件号码、姓名**。如您不同意我行记录前述信息，则可能无法完成交易，但不影响您使用我行提供的其他服务。

（22）当您在手机银行使用一键绑卡功能时，您需提供**姓名、证件号码、绑定卡号、手机号码**，如未提供或提供的相应信息不准确，仅会使您无法使用上述功能，但不影响您正常使用上海银行手机银行 App 的其他功能。

（23）当您在手机银行使用证券开户功能时，您需提供**手机号码**，如未提供或提供的相应信息不准确，仅会使您无法使用上述功能，但不影响您正常使用上海银行手机银行 App 的其他功能。

（24）当您在手机银行使用诚意金时，您需提供**刷脸认证信息**，如未提供或提供的相应信息不准确，仅会使您无法使用上述功能，但不影响您正常使用上海银行手机银行 App 的其他功能。

（25）当您在手机银行使用个人信息管理功能时，您需提供**民族、职业、单位名称、家庭地址、单位地址、电子邮箱、刷脸认证信息**，如未提供或提供的相应信息不准确，仅会使您无法使用上述功能，但不影响您正常使用上海银行手机银行 App 的其他功能。

（26）当您在手机银行使用专项分期时，您需提供**刷脸认证信息**，如未提供或提供的相应信息不准确，仅会使您无法使用上述功能，但不影响您正常使用上海银行手机银行 App 的其他功能。

具体功能见附录：

业务	收集个人信息	个人信息相关权限	目的
注册	手机号、验证码、银行卡号、姓名、证件号码	扫描：相机权限、短信	帮助您完成用户注册验证；
登录账号后		位置权限	便于帮助您找到最近的网点；

忘记密码- 重置密码	姓名、证件号码		帮助您完成身份验证
投资者合格认证	资产证明	相机、相册、存储权限	便于您上传识别资产情况以完成投资者合格认证
添加账户	银行卡号	相机权限	帮助您快速识别录入银行卡号；
流水打印	邮箱		方便发送相关文件到您的邮箱中；
申请信用卡	姓名、身份证号、手机号、动态密码	短信	用于申请信息用卡
办卡进度查询	证件号码、手机号、验证码	短信	验证核实身份
借记卡挂失补发、存单挂失补发	证件号码、手机号、详细地址		用于邮寄相关材料
大额转账信息预填	收款人户名、收款人账号	相机权限	便于您大额转账

云网点		相机、麦克风权限	用于云网点服务 视频通话
信用卡启用	证件号码		验证核实身份
大额取现 预约	城市		用于安全封控
扫码取款		相机权限	用于识别二维码
活期现金 存款	户名、代理人姓名、身 份证号码、电话	相机权限	方便您现金存款
银行账号 转账	姓名、银行账号	相机权限、短信	方便您转账
语音转账		麦克风权限	用于语音转账
回单验收	回单流水号		用于验证回单
手机号转 账	手机号、姓名	通讯录	用于手机号转账
上海银行 信用卡分 期预约	姓名、性别、所在城市、 手机号、验证码、身份 证号码	短信	用于预约申请
我的信用	身份证正反面、民族、		用于管理您的个

卡-个人信息管理	职业、单位名称、家庭住址、家庭电话、家庭邮编、单位地址、单位电话、单位邮编、邮箱		人信息
我的信用卡-设置查询密码	银行账户、密码		用于设置查询密码
话费充值	手机号	通讯录	用于快速输入充值手机号
生活缴费	城市、缴费号码	相机权限	帮助快速识别缴费号码，以查询缴费信息
学费	学校、证件号码		用于查询学费信息
热门活动、特惠商户	城市		用于查询城市优惠信息
ETC 申请	行驶证、身份证正反面	相机权限	用于识别录入身份信息
速通卡	手机号、验证码	短信	用于验证核实手机号

在线客服- 预约电话 人工服务	姓名、手机号		用于预约人工服务
在线客服		麦克风	用于语音输入
数字员工		麦克风	用于语音输入
意见反馈		麦克风、相机	用于语音输入及 图片上传
登录密码 修改	密码		用于修改密码
更换头像		相机、存储权限、 相册权限	用于上传头像图 片
搜索		麦克风	用于语音输入

3. 当您使用上海银行手机银行 App 服务时，为了维护服务的安全稳定运行，降低交易和资金风险，我行会收集以下基础信息，包括您的设备型号、设备类型、操作系统手机银行软件版本号、登录 IP 地址、MAC 地址、接入网络的方式、类型和状态、网络质量数据、设备加速器（如重力感应设备）、操作日志、服务日志信息（您在手机银行搜索、查看的信息、服务故障信息）、地理位置信息、应用列表信息、Android ID、IMSI，这些信息是为您提供服务必须收集的基础信息，以保障您正常使用我行的服务。

4. 当您使用上海银行手机银行 App 的功能或服务时，在某些特定使用场景下，我行可能会使用具有相应业务资质及能力的**第三方服务商提供的软件服务工具包（简称“SDK”）**来为您提供服务，由第三方服务商收集您的必要信息，使用频率为触发相关业务时获取。具体包括以下几种：

（1）个推 SDK。为了向您及时推送服务通知，我们使用了个推 SDK，该 SDK 需要获取您的**手机终端唯一标志信息（IMEI 号）、手机型号、系统类型、系统版本、网络类型、SIM 卡运营商信息**，用于实现 App 推送服务。个推 SDK 服务商为每日互动股份有限公司。

（2）vivo 推送 SDK。支持 vivo 品牌手机向您及时推送服务通知，我们使用了 vivo 推送 SDK，该 SDK 需要获取您的**手机终端唯一标志信息（IMEI 号）、手机型号、系统类型、系统版本、网络类型、SIM 卡运营商信息**，用于实现 App 推送服务。vivo 推送 SDK 服务商为维沃移动通信有限公司。

（3）小米推送 SDK（含米聊）。支持小米品牌手机向您及时推送服务通知，我们使用了小米推送 SDK，该 SDK 需要获取您的**手机终端唯一标志信息（IMEI 号）、手机型号、系统类型、系统版本、网络类型、SIM 卡运营商信息**，用于实现 App 推送服务。小米推送 SDK 服务商为北京小米移动软件有限公司。

（4）OPPO 推送 SDK。支持 OPPO 品牌手机向您及时推送服务通知，我们使用了 OPPO 推送 SDK，该 SDK 需要获取您的**手机终端唯一标志信**

息（IMEI 号）、手机型号、系统类型、系统版本、网络类型、SIM 卡运营商信息，用于实现 App 推送服务。OPPO 推送 SDK 服务商为 OPPO 广东移动通信有限公司。

（5）华为推送 SDK（含华为 update SDK、taoweiji huaweipush-server-sdk）。支持华为品牌手机向您及时推送服务通知，我们使用了华为推送 SDK，该 SDK 需要获取您的手机终端唯一标志信息（IMEI 号）、手机型号、系统类型、系统版本、网络类型、SIM 卡运营商信息，用于实现 App 推送服务。华为推送 SDK 服务商为华为技术有限公司。

（6）指纹比对 SDK（含支付宝支付 SDK）。为了向您提供指纹比对服务，我们使用了指纹比对 SDK，该 SDK 需要获取您设备上的指纹信息。指纹比对 SDK 服务商为杭州蚂蚁上数信息技术有限公司。

（7）通用 E 盾 SDK。为了向您提供通用 E 盾密码验证服务，我们使用了通用 E 盾 SDK，该 SDK 需要获取您的蓝牙权限。通用 E 盾 SDK 服务商为飞天诚信科技股份有限公司、神州融安科技（北京）有限公司。

（8）OCR 识别 SDK。为了向您提供身份证及银行卡图像识别服务，我们使用了 OCR 识别 SDK，该 SDK 需要获取您的相机权限。OCR 识别 SDK 服务商为上海合合信息科技。

（9）人脸识别 SDK。为了向您提供人脸比对服务，我们使用了人脸识别 SDK，该 SDK 需要获取您的相机、AndroidID。人脸识别 SDK 服务商为

北京商汤科技开发有限公司、上海宜签网络科技有限公司、平安科技(深圳)有限公司。

(10) 设备指纹 SDK (READ_PHONE_STATE、ACCESS_COARSE_LOCATION)。当您使用手机银行服务时，需要采集您的手机设备信息，包括 IDFA 标识码、IDFV 标识码、IP 地址、IMSI、mac 地址、WiFi IP 地址、Android ID、当前电池电量、磁盘大小、已用磁盘大小、时区、内存整体大小、手机系统时间、设备制式、设备名称、系统版本、设备型号、设备分辨率、CPU 核心数量、本地语言信息、是否连接到移动网络标识、是否连接到 WiFi 网络标识、所用网络型号、运营商名称、移动网络国家代码、移动网络国家移动代码、移动网络代码、设备屏幕宽度、设备屏幕高度、设备是否为模拟器标识、设备是否越狱标识、WiFi bssid、WiFi ssid、粗略定位、本机蓝牙 MAC 地址、应用列表、传感器列表、App 版本号、SDK 版本号、APPID、是否使用 VPN 标识、代理信息 IP 和端口、上一次获取的 token 值，以上信息加密存储于我行后台，用于保障您的交易安全。设备指纹 SDK 服务商为浙江邦盛科技股份有限公司。

(11) 科大讯飞 SDK (RECORD_AUDIO)。为了向您提供语音文本识别服务，我们使用了科大讯飞 SDK，该 SDK 需要获取您的录音信息、Android ID，用于实现语音识别功能。科大讯飞 SDK 服务商为科大讯飞股份有限公司。

(12) 云视频 SDK (含 youth banner、TooTallNate Java-WebSocket、READ_PHONE_STATE)。为了向您提供远程视频柜员服务，我们使用了云视频 SDK，该 SDK 需要获取您的**相机权限**。云视频 SDK 服务商为随锐科技集团股份有限公司。

(13) 密码键盘 SDK (READ_SETTINGS、WRITE_SETTINGS)。为了向您提供密码控件服务，我们使用了密码键盘 SDK。密码键盘 SDK 服务商为北京微通新成网络科技有限公司。

(14) 百度定位 SDK (含百度平台、WRITE_EXTERNAL_STORAGE)。为了向您提供基于位置的服务，我们使用了百度定位 SDK，该 SDK 需要获取您的**手机终端唯一标志信息 (IMEI 号)、经纬度信息、Android ID、WIFI 名称、创建外部存储文件权限、新建外部文件权限、读写外部存储文件、读取外部存储文件、WIFI-BSSID**，用于实现定位功能。在后台静默服务时会获取 WI-FI BSSID 信息。百度定位 SDK 服务商为北京百度网讯科技有限公司。

(15) 梆梆安全 SDK。为了保证 App 安全，我们使用了梆梆安全 SDK，该 SDK 需要获取您的**手机终端唯一标志信息 (IMEI 号)、手机型号、系统类型、系统版本、网络类型、设备 App 列表信息**，用于实现 App 安全加固。梆梆安全 SDK 服务商为北京梆梆安全科技有限公司。

(16) 高德定位 SDK (ACCESS_FINE_LOCATION、ACCESS_COARSE_LOCATION、READ_EXTERNAL_STORAGE)。为了向您提供基于位置的服务，我们使用了高德定位 SDK，该 SDK 需要获取您的**手机**

终端唯一标志信息（IMEI 号）、外部存储目录、IMSI、Wi-Fi MAC 地址、硬件序列号、SIM 卡运营商名称、MEID、经纬度信息、精确维位置、粗略位置、ANDROID id、MAC 地址、IP、WI-FI BSSID、WI-FI SSID、读取外部存储文件、获取加速度传感器，用于实现定位功能。高德定位 SDK 服务商为高德软件有限公司。

（17）MPAAS SDK（含 Okio、Jsoup、Facebook Soloader Nativeloader SDK、Android Beacon Library、Kotlinx Coroutines Android SDK、Android Support Library V4、checker-framework、Apache Commons Codec、RxJavaFX、Reactive Streams、阿里设备标识 SDK、Android Support Library Compat、Greenrobot EventBus、IVianuu injekt-coroutines-jvm、Apache Commons IO、新浪微博 SDK、Kotlin Stdlib、Android Lifecycle ViewModel、uc webview sdk、Facebook Soloader SDK、RxAndroid、OkHttp、ReactiveX rxjava3 rxandroid、Chromium（获取网络额外信息、Wi-Fi SSID）、Alipay（存储权限、相机权限）、BumpTech Glide（获取照片信息）、Kotlin Stdlib Jdk7、Kotlin Stdlib Jdk8、阿里聚数据风控 SDK、蚂蚁消息推送 SDK、Jsoup、阿里 fastjson、淘宝无限开发平台、Appache、bouncycastle、阿里百川、阿里 UC 奔溃 SDK、UC 浏览器服务 SDK、阿里 one SDK、org.java_websocket(Android ID)、阿里无线保镖 SDK、READ_PHONE_STATE、BROADCAST_STICKY、REORDER_TASKS、WRITE_EXTERNAL_STROAGE、WI-FI SSID、加速传感器、陀螺仪传感器）。为了向您提供手机银行系统框架服务，我们使用了 MPAAS SDK，在使用

该 SDK 提供的服务时，为了保证交易安全性会在前后台以及应用停止静默获取您的手机终端唯一标志信息（IMEI 号）、存储权限、当前运行程序、进程优先级、创建外部存储文件、设备运行应用列表、IP、当前运行应用进程。MPAAS SDK 服务商为阿里云计算有限公司。

（18）芯盾 SDK（READ_PHONE_STATE）。为了向您提供短信加固服务，我们使用了芯盾 SDK。该 SDK 需要获取您的 Android ID、IMEI、IMSI、WI-FI BSSID、WI-FI SSID、传感器列表、IP 地址、本机 MAC 地址、地理定位、粗略定位。芯盾 SDK 服务商为北京芯盾时代科技有限公司。

（19）银联支付 SDK（含 square logging-interceptor、square okhttp-ws、数美（MAC 地址、AndroidID、IP、Wi-Fi SSID、传感器列表）、READ_PHONE_STATE、ACCESS_LOCATION_EXTRA_COMMANDS）。为了向您提供银联云闪付服务，我们使用了银联支付 SDK，在使用该 SDK 提供的服务时，为了保证交易安全性会在前台遍历静默获取 Android ID、IP、IMSI、SIM 卡运营商、WI-FI BSSID、WI-FI SSID、加速度传感器、外部存储目录、应用包信息、手机参数信息、硬件序列号、粗略定位、重力传感器、陀螺仪传感器、访问精确位置、当前运行应用进程；该 SDK 需要获取您的相册权限、硬件序列号、Android ID、IP、IMSI、位置信息（包含粗略定位及精确位置）、传感器列表。银联支付 SDK 服务商为中国银联股份有限公司。

(20) 微信 SDK (含微信开放平台)。为了向您提供分享服务，我们使用了微信 SDK，该 SDK 需要获取您的 **OPENID、微信名字**。微信 SDK 服务商为深圳市腾讯计算机系统有限公司。

(21) QQSDK (含 QQ 开放平台)。为了向您提供分享服务，我们使用了 QQSDK。QQSDK 服务商为深圳市腾讯计算机系统有限公司。

(22) 手写签名 SDK。为了向您提供远程双录保险交易、房贷申请、信托购买服务，我们使用了手写签名 SDK，该 SDK 需要获取您的**姓名、身份证号**。手写签名 SDK 服务商为北京数字认证股份有限公司。

(23) 神策数据 SDK。为了向您提供安全分析服务，我们使用了神策数据 SDK，该 SDK 需要获取您的**当前运行应用进程、Android ID**。神策数据 SDK 服务商为神策网络科技（北京）有限公司。

(24) 屹通 SDK (READ_PHONE_STATE)。为了向您提供手机银行系统框架服务，我们使用了屹通 SDK，该 SDK 需要获取您的**剪贴板权限、手机参数、Android id、IP、MAC、IMSI、WIFI MAC 地址、电话权限、IMEI、剪贴板、手机参数信息**。屹通 SDK 服务商为上海屹通信息科技有限公司。

(25) 上海社保卡 SDK (essclib.esscpermission.checker、RCORD_AUDIO、CAMERA、ACCESS_FINE_LOCATION、READ_EXTENAL_STORAGE)。为了向您提供上海社保卡申请服务，我们使用了上海社保卡 SDK，该 SDK 需要获取您的**相机权限、通讯录权限、存**

储权限、录音、精确位置、遍历外部存储文件或文件夹。上海社保卡 SDK 服务商为金保信社保卡科技有限公司。

(26) 数字人 SDK。为了向您提供数字人服务，我们使用了数字人 SDK，该 SDK 需要获取您的**麦克风权限**。数字人 SDK 服务商为北京商汤科技开发有限公司。

(27) ynet SDK (READ_PHONE_STATE)。为了向您提供基础框架服务，我们使用了 ynet SDK，该 SDK 需要获取您的 IP、IMSI、MAC、WI-FI MAC 地址信息。ynet SDK 服务商为北京易诚互动网络科技股份有限公司。

(28) 行为采集 SDK（数据存储在我行）。为统计产品的客户访问情况，以便于优化服务流程，我们使用了行为采集 SDK，数据存储在我行。该 SDK 需要获取您的设备识别信息（IDFV 苹果应用开发商标识符、GAID 谷歌广告标识符、设备硬件序列号）、设备硬件信息（设备品牌、设备型号、屏幕分辨率、屏幕密度-安卓）、应用信息（开发者应用名、应用包名、版本号、应用发布渠道、应用内语言、应用内地区/国家、应用进程信息-安卓）、操作系统信息（越狱状态-IOS 端、系统版本号、系统 API 版本-安卓、系统国家/区域信息、系统语言）、SIM 卡信息（MCC 移动国家码、MNC 移动网络码）、运营商信息、网络访问模式、WI-FI 网络状态权限-安卓、网络状态权限-安卓、IP 地址、Android ID、MAC 地址。行为采集 SDK 服务商为北京火山引擎科技有限公司。

(29) 无感本机认证 SDK。为了向您提供无感本机认证服务、快捷登录账号服务。我们使用了无感本机认证 SDK，该 SDK 需要获取您的设

备信息（设备型号、设备制造商、操作系统版本、屏幕尺寸）、网络相关信息（IP 地址、网络类型）、设备标识信息（OAID、subid、ICCID）、SIM 卡信息（运营商信息、是否双卡、SIM 卡 MCC/MNC）。无感本机认证 SDK 服务商为武汉极意网络科技有限公司。

（30）其他插件。Commons Lang、sqlcipher-for-android、GreenDAO 应用于数据库加密、Apache HttpClient 应用于 PDF 下载、Glide-transformations 应用于图片下载、JetBrains Java Annotations 应用于注释、EasyPermissionsSDK 应用于权限申请、com.ynet.finmall SDK 应用于 mpaas 基础方法调用、版面底层逻辑。

如您不同意上述第三方服务商收集前述信息，可能无法获得相应服务，但不影响您正常使用手机银行 App 的其他功能或服务。如您同意上述相关第三方服务商收集前述信息发生信息泄露的，由相关第三方服务商承担相应的法律责任。

5. 为向您提供更加准确和便捷的服务，或经您同意后为提升服务体验、改进服务质量，或为防范风险，我行会收集您反馈意见、建议时提供的信息，收集您使用上海银行手机银行 App 功能或服务的类别、方式

和操作信息，我行会对这些信息进行综合统计、加工分析，并会根据上述信息向您提供相应服务或产品。

6. 我行在向您提供其他业务功能时，会另行向您说明信息收集的范围与目的，并征得您的同意后方收集提供相应服务所必要的您的信息。我行会按照本政策以及相应的用户协议约定收集、使用、储存、对外提供及保护您的信息。

（五）我行如何使用您的个人信息

1. 在我行向您提供金融产品或服务，以及改进这些产品或服务时使用。

2. 在我行向您提供金融服务期间，您授权我行持续收集和使用您的相关个人信息。在您注销服务或取消授权时，我行将停止收集及使用您的相关个人信息，但我行会根据法律法规及监管的要求在业务资料归档、审计、监管协查等领域继续使用此前收集的您的相关个人信息。

3. 为向您提供更加准确、个性和便捷的服务，提升服务体验、改进服务质量，或为防范风险，经您同意后我行会对您服务使用情况的相关信息统计、分析，并会根据上述信息在“首页-猜您喜欢”等页面对您进行定向推送，为您提供精准的推荐产品、营销广告及功能服务，您可通过“我的-安全中心-其他-开启个性化推荐”路径对个性化推荐进行关闭。

4. 将您的个人信息用于法律允许的其它用途。

（六）征得授权同意的例外

根据相关法律法规、监管要求及国家标准，以下情形中遇到国家有权机关或者监管机关要求我行提供的，或者出于对您的权利、权益进行充分保护的目 的，或者此处约定的其他合理情形的，我行会收集、使用您的相关个人信息而无需另行征求您的授权同意：

1. 与国家安全、国防安全直接相关的；
2. 与公共安全、公共卫生、重大公共利益直接相关的；
3. 与犯罪侦查、起诉、审判和判决执行等直接相关的；
4. 出于维护您或其他个人的生命、财产等重大合法权益但又很难得到您本人同意的；
5. 所收集的个人信息是您自行向社会公众公开的；
6. 从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道；
7. 根据您要求签订和履行合同所必需的；
8. 用于维护所提供的产品或服务的安全稳定运行所必需的，例如发现、处置产品或服务的故障；
9. 出于公共利益开展统计或学术研究所必需，且其对外提供学术研究或描述的结果时，对结果中所包含的个人信息进行去标识化处理的；
10. 法律法规及监管要求规定的其他情形。

二、我行如何使用 Cookie 技术

为确保上海银行手机银行 App 正常运转，我行会在您移动设备上存储名为 Cookie 的小数据文件。Cookie 通常包含标识符、站点名称以及一些号码和字符。我行不会将 Cookie 用于本政策所述目的之外的任何用途。您可根据自己的偏好管理或删除 Cookie。您可以清除移动设备上保存的所有 Cookie。

三、我行如何共享、转让和公开披露您的个人信息

（一）共享

我行不会向其他任何公司、组织和个人共享或转让您的个人信息，但以下情况除外：

1. 事先获得您的明确同意；
2. 如业务需要对外共享您的个人信息，我行会向您告知共享个人信息的目的、数据接收方的类型，并征得您的授权同意。涉及敏感信息的，我行还会告知敏感信息的类型、数据接收方的身份，并征得您的明示授权同意。
3. 请您理解，我行可能会根据法律法规规定，或按政府主管部门的强制性要求，对外共享您的个人信息。
4. 对我行与之共享个人信息的公司、组织和个人，我行会与其签署严格的保密协议，要求他们按照我行的说明、本隐私政策以及其他任何相关的保密和安全措施来处理个人信息。
5. 我行会对合作方获取有关信息的应用程序接口（API）、软件工具开发包（SDK）进行严格的安全检测，并与合作方约定严格的数据保

护措施，令其按照我行的委托目的、服务说明、本隐私权政策以及其他任何相关的保密和安全措施来处理个人信息。

6. 我行可能会向合作方（主要是推送服务或移动设备厂商）提供您的部分账户信息及交易信息，以便及时向您的移动设备发送账户资金变动及相关交易通知。

7. 当您在上海银行手机银行 App 中使用第三方提供的服务时，第三方可能会获取您的**昵称、头像、位置、姓名、手机号码信息及其他提供第三方服务所必须的信息**；在经过您的明示同意后，第三方可获取您的以上信息；对于您在使用第三方提供的服务时主动提供给第三方的相关信息，我行将视为您允许该第三方获取上述此类信息；对于您在使用该第三方服务时产生的信息，应由您与该第三方依法约定上述信息的收集和使用事项。如您拒绝第三方在提供服务时收集、使用或者传递上述信息，将可能会导致您无法在上海银行手机银行 App 中使用第三方的相应服务，但这不影响您使用上海银行手机银行 App 的其他功能。我行不对第三方服务提供者的身份信息保护能力和数据安全能力负责，若您发现个人身份信息被侵犯，请进行投诉。

8. 当您与上海银行在发生贷款或者担保信用业务时，我行可能会向中国人民银行金融信用信息基础数据库、百行征信有限公司、朴道征信有限公司、教育部学生服务与素质发展中心、中国司法大数据研究院有限公司、金保信社保卡科技有限公司、北京中数智汇科技股份有限公司、中国银行保险信息技术管理有限公司、钱塘征信有限公司、电子认证服

务机构、社会保障管理机构、住房公积金管理机构查询、使用或提供您的信用、资产信息。上海银行依法对您的相关信息承担保密责任，并保证要求合作机构对您的相关信息承担保密责任。

（二）转让

1. 事先获得您的明确同意；

2. 根据法律法规或强制性的行政或司法要求；

3. 根据法律法规和商业惯例，在合并、收购、资产转让等类似交易中，如涉及到个人信息转让，我行会要求新的持有您个人信息的公司、组织继续受本隐私政策的约束，否则我行将要求该公司、组织重新向您征求授权同意。

（三）公开披露

1. 我行不会公开披露您的个人信息，如确需披露，我行会获取您的同意，并告知您披露个人信息的目的、类型；涉及敏感信息的还会告知敏感信息的内容，并事先征得您的明示同意。

2. 请您理解，在法律、法律程序、诉讼或政府主管部门强制性要求的情况下，我行可能会公开披露您的个人信息。

（四）征得授权同意的例外

根据相关法律法规、监管要求等规定，以下情形中遇到国家有权机关或者监管机关强制性要求的，或者出于对您的权利、权益进行充分保护的目，或者此处约定的其他合理情形的，我行可能会共享、转让、公开披露用户信息无需事先征得您授权同意：

1. 与国家安全、国防安全直接相关的；
2. 与公共安全、公共卫生、重大公共利益直接相关的；
3. 与犯罪侦查、起诉、审判和判决执行等直接相关的；
4. 出于维护您或其他个人的生命、财产、声誉等重大合法权益但又很难得到本人同意的；
5. 您自行向社会公众公开的个人信息；
6. 从合法公开披露的信息中收集的用户信息，如合法的新闻报道、政府信息公开等渠道。

四、我行如何存储和保护您的个人信息

（一）存储

按照相关法律法规规定，我行将中华人民共和国境内（不包括香港、澳门特别行政区及台湾地区）提供服务过程中收集和产生的您的个人信息存储在中华人民共和国境内（不包括香港、澳门特别行政区及台湾地区）。但为处理跨境业务并在获得您的授权同意后，您的个人信息可能会被转移到境外。此种情况下我行会采取有效措施保护您的信息安全，例如，跨境汇款业务中的客户姓名、汇款人账号、汇款人地址数据通过加密传输的方式保护您的信息安全。

我行仅在法律法规要求的期限内，以及为实现本政策声明的目的所必须的时限内保留您的个人信息。例如：

手机号码：当您需要使用手机银行服务时，我行需要一直保存您的

手机号码，以保证您正常使用该服务，当您注销手机银行账户后，我行将删除相应的信息；

用户头像：当您设置了头像以后，我行会一直保存您的头像，用于登录页面展示使用。当您选择恢复默认为头像后，我行将删除您设置的头像信息。

（二）保护

1. 我行已获得等级保护测评与备案。我行使用符合业界标准的安全防护措施保护您提供的个人信息，防止数据遭到未经授权的访问、公开披露、使用、修改、损坏或丢失。我行会采取一切合理可行的措施，保护您的个人信息。例如：我行会使用加密技术确保数据的保密性；我行会使用受信赖的保护机制防止数据遭到恶意攻击；我行会部署访问控制机制，确保只有授权人员才可访问个人信息；以及我行会举办安全和隐私保护培训课程，加强员工对于保护个人信息重要性的认识。

2. 请您理解，由于技术水平局限以及可能存在的恶意攻击，有可能出现我行无法合理预见、防范、避免、控制的意外情况。互联网并非绝对安全的环境，请使用复杂密码，协助我行保证您的账号安全。

3. 如发生个人信息安全事件，我行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您，或采取合理、有效的方式发布公告。同时，我行还将依据监管规定，主动上报个人信息安全事件处置情况。

五、您的权利

按照中国相关的法规和监管规定，我行保障您对自己的个人信息行使以下权利：

（一）访问、更正及更新您的个人信息

您有权通过我行网上银行、手机银行、电话银行等渠道访问及更正、更新您的个人信息，法律法规规定的例外情况除外。您有责任及时更新您的个人信息。

您可以通过手机银行“我的-安全中心-个人信息管理-客户信息维护”，查询姓名、性别、出生日期、证件类型、证件号码，此类基本信息暂无法线上修改，只能前往线下网点修改；还可以查询地址信息、工作信息、联系信息、更多信息，更新身份证有效期，此类信息可以通过手机银行线上修改。

（二）删除您的个人信息

在以下情形中，您可以向我行提出删除个人信息的请求：

1. 如果我行处理您个人信息的行为违反法律法规；
2. 如果我行收集、使用您的个人信息，却未征得您的同意；
3. 如果我行处理个人信息的行为违反了与您的约定；
4. 如果您终止我行的服务；
5. 如果我行不再为您提供服务。

您可以联系我行客服热线:95594,来申请删除个人信息,受理您的问题后,我行会及时、妥善处理。一般情况下,我行将在 15 个工作日内给予答复和完成处理。

(三) 管理您的信息及取消授权

您有权决定是否继续对您个人信息采集、使用等进行授权。您可以通过不同品牌手机的设置-应用信息-权限路径对已授权权限进行取消,取消后我行将不再继续使用您相应的授权。请您理解如您取消授权,我行将无法为您提供电子渠道服务(含上海银行手机银行、网上银行)服务,也不再继续处理您相应的个人信息(如您已就具体产品或服务与我行另行签署授权的除外),但您取消本隐私政策授权的决定,不会影响我行此前基于您授权已开展的个人信息处理。

(四) 个人信息主体注销账户

如您为我行电子银行注册用户,您可以到网点通过我行柜面或E动终端或自助设备等渠道注销您的电子银行,也可选择通过以下方式自助注销。

注销手机银行,您可下载我行手机银行客户端,启动客户端,在“首页”搜索“自助注销”,输入手机号码、附加码、短信验证码,验证人脸识别,验证通过后即可注销手机银行。

您注销电子银行用户的行为是不可逆行为，一旦您注销您的电子银行用户，我行将不再通过上海银行手机银行 App 收集您的个人信息，并将删除有关您上海银行手机银行 App 的一切信息，法律法规或监管机构对个人信息存储时间另有规定的除外。

如您非我行电子银行用户，您可以自主选择卸载或停止使用上海银行手机银行 App 客户端，以阻止我行获取您的个人信息。请您注意，我行电子银行用户仅在手机设备中删除上海银行手机银行 App 时，我行不会注销您的电子银行用户，有关您电子银行用户的一切信息不会删除。您仍需注销您的电子银行用户方能达到以上目的。

（五）获取您的个人信息副本

您有权获取您的个人信息副本。如您需要获取我们收集的您的个人信息副本，您随时联系我们（通过本政策第九条中所述的联系方式）。在符合相关法律规定且技术可行的前提下，我们将根据您的要求向您提供相应的个人信息副本。

（六）约束信息系统自动决策

在某些业务功能中，我们可能仅依据信息系统、算法等在内的非人工自动决策机制做出决定。如果这些决定显著影响您的合法权益，您有权要求我们作出解释，我们也将提供适当的救济方式。

（七）响应您的上述请求

如果您无法通过上述方式访问、更正或删除您的用户信息（含删除备份数据）以及注销账户，或您需要访问、更正或删除您在使用我行服务或功能时所产生的其他用户信息，或您认为我行存在任何违反法律法规或与您关于用户信息的收集或使用的约定，您均可通过本政策中的联系方式与我行取得联系。为了保障安全，我行可能需要您提供书面请求，或以其他方式证明您的身份，我行将在收到您反馈并验证您的身份后的15个工作日内完成核查和处理。**对于您合理的请求，我行不收取费用。对于非法、违规、无正当理由、可能无端重复、需要过多技术手段（例如，需要开发新系统或从根本上改变现行惯例）、给他人合法权益带来风险或者非常不切实际的请求，我行可能会予以拒绝。**

此外，根据相关法律法规、监管要求等规定，以下情形中遇到国家有权机关或者监管机关要求的，或者存在以下约定其他情形的，我行将可能无法响应您的请求：

1. 与国家安全、国防安全直接相关的；
2. 与公共安全、公共卫生、重大公共利益直接相关的；
3. 与犯罪侦查、起诉、审判和判决执行等直接相关的；
4. 有充分证据表明您存在主观恶意或滥用权利的；
5. 响应您的请求将导致您或其他个人、组织的合法权益受到严重损害的。
6. 涉及商业秘密的。

六、我行如何保护未成年人信息

（一）未成年人使用我行服务，必须在其父母或者其他监护人的监护下进行。我行将根据国家相关法律法规的规定保护未成年人的个人信息的保密性及安全性。

（二）如您为未成年人，请您的父母或监护人阅读本政策，并在征得您父母或监护人同意的前提下使用我行的服务或向我行提供您的信息。对于经父母或监护人同意而使用您的信息的情况，我行只会在受到法律允许、父母或监护人明确同意或者保护您的权益所必要的情况下使用或共享此信息。如您的监护人不同意您按照本政策使用我行的服务或向我行提供信息，请您立即终止使用我行的服务并及时通知我行，以便我行采取相应的措施。

（三）如您为未成年人的父母或监护人，当您对您所监护的未成年人的个人信息处理存在疑问时，请通过本政策中的联系方式联系我行。

（四）如您为14周岁以下的儿童，请在征得您父母或监护人同意的前提下使用手机银行App内（包含我行和第三方）提供的服务或向我行和第三方提供您的信息。

七、第三方收集和使用您信息的情况

当您在手机银行 App 中使用第三方提供的服务时，第三方可能会获取您的**昵称、头像、位置、姓名、证件类型、证件号码、证件有效期、手机号码信息**及其他提供第三方服务所必须的信息；在经过您的明示同意后，第三方可获取您的以上信息。在将信息提供给第三方前，我行将尽商业上合理的努力评估该第三方收集信息的合法性、正当性、必要性。我行会与第三方签订相关法律文件并要求第三方处理您的个人信息时遵守法律法规和签署的法律文件，要求第三方对您的信息采取保护措施。

请您注意，您访问的第三方网站经营者、通过我们接入的第三方服务可能有自己的隐私保护政策；当您查看第三方创建的网页或使用第三方开发的应用程序时，这些第三方可能会放置他们自己的 Cookie 或像素标签，这些 Cookie 或像素标签不受我们的控制，且它们的使用不受本政策的约束。我们会尽商业上的合理努力去要求这些主体对您的个人信息采取保护措施，但我们无法保证这些主体一定会按照我们的要求采取保护措施。如您发现这些第三方创建的网页或第三方开发的程序存在风险时，建议您终止相关操作以保护您的合法权益。

如您拒绝第三方在提供服务时收集、使用或者传递上述信息，将可能会导致您无法在手机银行 App 中使用第三方的相应服务，但这不影响您使用手机银行 App 的其他功能。

对于您在使用第三方提供的服务时主动提供给第三方的相关信息，我行将视为您允许该第三方获取上述此类信息；对于您在使用第三方服

务时产生的信息，应由您与该第三方依法约定上述信息的收集和使用事项。

请您理解，第三方提供的服务由该第三方独立运营并独立承担全部责任。因第三方所提供服务或其使用您的信息产生的纠纷，或其违反相关法律法规或本协议约定，或您在使用其服务过程中遭受的损失，请您与该第三方协商解决。对于需由第三方解决的问题，我行将尽商业上合理的努力推动第三方解决。如需要更改或删除三方授权信息请拨打 95594 在客服引导下进行操作,具体包括以下几种：

SDK 名称	场景描述	涉及收集的个人信息字段	数据接收方名称
个推 SDK	App 推送服务	手机终端唯一标志信息（IMEI 号）、手机型号、系统类型、系统版本、网络类型、SIM 卡运营商信息	每日互动股份有限公司
vivo 推送 SDK	App 推送服务	手机终端唯一标志信息（IMEI 号）、手机型号、系统类型、系统版本、网络类型、SIM 卡运营商信息	维沃移动通信有限公司
小米推送 SDK	App 推送服务	手机终端唯一标志信息（IMEI 号）、手机型号、系统类型、系统版本、网络类型、SIM 卡运营商信息	北京小米移动软件有限公司
OPPO 推送 SDK	App 推送服务	手机终端唯一标志信息（IMEI 号）、手机型号、系统类型、系统版本、网络类型、SIM 卡运营商信息	OPPO 广东移动通信有限公司
华为推送 SDK	App 推送服务	手机终端唯一标志信息（IMEI 号）、手机型号、系统类型、系统版本、网络类型、SIM 卡运营商信息	华为技术有限公司
指纹比对 SDK	指纹登录及指纹支付	设备上的指纹信息	杭州蚂蚁上数信息技术有限公司
通用 E 盾	E 盾安全服务	蓝牙权限	飞天诚信科技

SDK			股份有限公司、神州融安科技（北京）有限公司
OCR 识别 SDK	身份证、银行卡识别	相机权限	上海合合信息科技
人脸识别（活体检测）SDK	人脸识别和人脸安全服务	相机、Android ID	北京商汤科技开发有限公司、上海宜签网络科技有限公司、平安科技（深圳）有限公司
设备指纹 SDK	设备指纹服务	设备型号、电量、设备时间、系统内存、Android ID、IDFA 标识码、IDFV 标识码、IP 地址、IMSI、mac 地址、WiFi IP 地址、当前电池电量、磁盘大小、已用磁盘大小、时区、内存整体大小、手机系统时间、设备制式、设备名称、系统版本、设备型号、设备分辨率、CPU 核心数量、本地语言信息、是否连接到移动网络标识、是否连接到 WiFi 网络标识、所用网络型号、运营商名称、移动网络国家代码、移动网络国家移动代码、移动网络代码、设备屏幕宽度、设备屏幕高度、设备是否为模拟器标识、设备是否越狱标识、WiFi bssid、WiFi ssid、粗略定位、本机蓝牙 MAC 地址、应用列表、传感器列表、App 版本号、SDK 版本号、APPID、是否使用 VPN 标识、代理信息 IP 和端口、上一次获取的 token 值	浙江邦盛科技股份有限公司
科大讯飞 SDK	语音识别服务	麦克风权限、AndroidID	科大讯飞股份有限公司
云视频 SDK	远程柜员服务	相机权限	随锐科技集团股份有限公司
密码键盘	密码控件	无	北京微通新成

SDK			网络科技有限公司
百度定位 SDK	定位功能	位置信息、读写外部存储文件、读取外部存储文件、手机终端唯一标志信息（IMEI 号）、经纬度信息、Android ID、WIFI 名称、创建外部存储文件权限、新建外部文件权限、WIFI-BSSID。	北京百度网讯科技有限公司
梆梆 SDK	防止安卓 App 被破解、反编译、二次打包等威胁	手机终端唯一标志信息（IMEI 号）、手机型号、系统类型、系统版本、网络类型、设备 App 列表信息	北京梆梆安全科技有限公司
高德定位 SDK	定位功能	位置信息、外部存储目录、IMSI、Wi-Fi MAC 地址、硬件序列号、SIM 卡运营商名称、MEID、手机终端唯一标志信息（IMEI 号）、经纬度信息、精确位置、粗略位置、ANDROID id、MAC 地址、IP、WI-FI BSSID、WI-FI SSID、读取外部存储文件、获取加速度传感器	高德软件有限公司
MPAAS SDK (含阿里无线保镖 SDK)	系统框架	手机终端唯一标志信息（IMEI 号）、存储权限、当前运行程序、Wi-Fi SSID、进程优先级、创建外部存储文件、设备运行应用列表、IP、当前运行应用进程	阿里云计算有限公司
芯盾 SDK	短信加固	粗略定位、Android ID、IMSI、WI-FI BSSID、WI-FI SSID、传感器列表、IP 地址、本机 MAC 地址	北京芯盾时代科技有限公司
银联支付 SDK	云闪付	相册权限、硬件序列号、AndroidID、IP、Wi-Fi SSID、IMSI、SIM 卡运营商、WI-FI BSSID、加速度传感器、外部存储目录、应用包信息、手机参数信息、硬件序列号、重力传感器、陀螺仪传感器、访问精确位置、当前运行应用进程、相册权限、位置	中国银联股份有限公司

		信息（包含粗略定位及精确位置）、传感器列表。	
微信 SDK	分享	OPENID、微信名字	深圳市腾讯计算机系统有限公司
手写签名 SDK	远程双录保险交易、房贷申请、信托购买	姓名、身份证号	北京数字认证股份有限公司
神策数据 SDK	安全分析	当前运行应用进程、 Android ID	神策网络科技有限公司（北京）有限公司
屹通 SDK	系统框架	剪贴板权限、IMEI、剪切板、手机参数信息、 Android id、IP、MAC、IMSI、WIFI MAC 地址、电话权限。	上海屹通信息科技发展有限公司
上海社保卡 SDK	社保卡申请	相机权限、通讯录权限、存储权限、 录音、精确位置、遍历外部存储文件或文件夹	金保信社保卡科技有限公司
数字人 SDK	数字人服务	麦克风权限	北京商汤科技开发有限公司
QQ SDK	分享	不涉及	深圳市腾讯计算机系统有限公司
行为采集 SDK	产品访问情况统计	设备识别信息、设备硬件信息、操作系统信息、 SIM 卡信息、运营商信息、网络访问模式、IP 地址、Android ID、MAC 地址、应用信息、WI-FI 网络状态权限（安卓）、网络状态权限（安卓）	北京火山引擎科技有限公司

无感本机认证 SDK	无感本机认证	设备信息、网络相关信息、设备标识信息、SIM 卡信息（运营商信息、是否双卡、SIM 卡 MCC/MNC）	武汉极意网络科技有限公司
y-net SDK	MPAAS 基础方法调用	IP、IMSI、MAC、WI-FI MAC 地址	北京易诚互动网络技术股份有限公司

您在手机银行 App 使用电子社保卡开通、出行贵宾、酒店住宿、运动生活、健康医疗、积分商城时，您可能还需要根据国家法律法规或服务方的要求提供您的姓名、证件号码、上海银行预留的手机号、账号、上海银行信用卡的可用积分、位置信息。如您不同意我行记录前述信息，则可能无法完成交易，但不影响您使用我行提供的其他服务。

八、本政策如何更新

根据国家法律法规变化及服务运营需要，我行将对本政策及相关规则不时地进行修改，修改后的内容会通过我行手机银行 App 渠道通过弹框形式进行公布，公布后即生效，并取代此前相关内容。您应不时关注相关公告、提示信息及协议、规则等相关内容的变动。您知悉并确认，如您不同意更新后的内容，应立即停止使用相应服务，并注销相关的用户，我行将停止收集您的相关个人信息；如您继续使用服务，即视为同意接受更新内容。

九、如何联系我行

如您对本政策存在任何疑问，或任何相关的投诉、意见，请联系我行客服热线：95594。受理您的问题后，我行会及时、妥善处理。一般情况下，我行将在 15 个工作日内给予答复和完成处理，法律法规或监管机构另有规定的除外。如果您对我们的答复、处理不满意，特别是如果

您认为我们的个人信息处理行为损害了您的合法权益，您可以通过向上海银行业保险业纠纷调解中心、上海市金融消费纠纷调解中心寻求解决方案。

我行全称：上海银行股份有限公司，注册地址：中国上海市黄浦区中山南路 688 号。 个人信息保护电子邮箱地址：webmaster@bosc.cn

附件 1-2

基于大模型技术的手机银行支付便利化服务合法合规性评估报告

本应用严格按照《中华人民共和国民法典》、《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》、《支付结算办法》（银发〔1997〕393号）、《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）、《银行保险机构消费者权益保护管理办法》（中国银行保险监督管理委员会令2022年第9号公布）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。本应用严格按照《互联网信息服务深度合成管理规定》（国家互联网信息办公室 中华

人民共和国工业和信息化部 中华人民共和国公安部令 第12号公布)履行备案手续。经反洗钱牵头管理部门评估,该金融服务不涉及反洗钱履职。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

2025年03月12日

附件 1-3

基于大模型技术的手机银行支付便利化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）、《个人金融信息保护技术规范》（JR/T 0171—2020）、《移动金融客户端应用软件安全管理规范》（JR/T 0092—2019）、《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）、《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）、《金融领域科技伦理指引》（JR/T 0258—2022）、《网络安全技术人工智能生成合成内容标识方法》（GB 45438-2025）、《中国人民银行业务领域数据安全管理办法》（中国人民银行令〔2025〕第3号）等相关金融行业技术标准规范要求进行设计开发并进行全面安全评估。经评估，本应用符合现有相关行业标准要求。

上海银行股份有限公司

2025 年 05 月 08 日

附件 1-4

基于大模型技术的手机银行支付便利化服务风险补偿机制

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，切实保障金融消费者合法权益。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。

对于人工智能的幻觉风险、输出结果可靠性，从事前、事中、事后三角度进行控制与应对：

1、事前：通过内外部服务安全评测，测试问题数千条，涵盖社会主义核心价值观、道德伦理、银行业务合规性等维度。经内部自评及第三方机构（阿里云、财跃星辰）测评，评测结论符合安全标准。

2、事中：制定安全拦截策略。如：建立社会危害词等敏感词黑名单，针对生成内容实时监控，拦截违规内容，确保生成内容的安全性。构建用户情绪实时识别机制，在对话过程中捕捉客户质疑等负面情绪，即时开展安抚工作，并完整记录问题，为后续优化提供依据。

3、事后：持续完善安全拦截策略，根据业务前台用户反馈、技术后台自动化监控预警，定期更新敏感词黑名单；设置安全风险等级，监控 AI 手机银行平台的系统使用情况，可关闭开放式聊天功能；建立监测预警，通过行内已有通道实时监测舆情，重点关注社交媒体、新闻平台和论坛；建立信息发布审核机制，确保发布的知识库、活动等内容合规，并支持快速下线；完善应急处置，对技术故障立即修复，及时跟踪。

上海银行股份有限公司

2025 年 03 月 13 日

附件 1-5

基于大模型技术的手机银行支付便利化服务退出机制

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。

上海银行股份有限公司

2025 年 03 月 13 日

附件 1-6

基于大模型技术的手机银行支付便利化服务应急预案

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 小时实时监控系统运行状况，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进行告警。

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。

上海银行股份有限公司

2025 年 03 月 13 日