《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	913201002496827567-2021-0001	
	创新应用名称	基于人工智能技术的 AI 数字员工服务	
	创新应用类型	金融服务	
	机构信息	统一社会信用代码	913201002496827567
		全球法人识别编码	300300C1086932000062
		机构名称	南京银行股份有限公司
		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：B0140H232010001 发证机关：中国银行业监督管理委员会江苏监管局
	拟正式运营时间	2021 年 02 月 08 日	
	技术应用	1. 基于语音识别和自然语言处理技术，对客户的指令进行语音转写、上下文理解、对话管理和情绪识别，提升 AI 数字员工对客户指令的理解能力，提高业务办理效率。 2. 使用人物形象建模技术，以银行真实行员形象为基础，模拟其形态动作，塑造 3D 拟人 AI 数字员工，提供具有现场交互感的客户服务。 3. 基于语音合成技术，对采集的真实行员声音数据进行训练和定制模仿，将 AI 数字员工交互信息实时、准确地转换为流畅、无差别感知的语音呈现给客户，增加客户在使用过程中的真实感。 4. 利用语音驱动动画技术，保证 AI 数字员工与客户进行交互过程中口型、动作、声音的一致性，为客户提供更自然的拟人数字交互体验。 5. 使用环境降噪、智能打断等技术，让 AI 数字员工在客户发出指令时自动中断语音输出，并实时感知客户情绪，保证双方沟通的连续性，提高交互质量。	
	功能服务	本项目基于人工智能等技术，在手机银行 APP 和营业网点打造客户专属 3D 拟人数字员工，实现转账填单辅助、余额查询、信用卡账单查询、积分查询等基础业务办理，以及客服答疑、产品咨询等功能，为客户提供智能化的银行服务，尤其为老年人等群体提供更贴心、更便利的无障碍金融服务，优化服务体验与流程，提高金融产品的易用性与安全性，更好弥合数字鸿沟。 本项目由南京银行股份有限公司独立研发和运维，此外无其他第三方机构参与。	

	创新性说明	1.在客户服务方面，与传统人工客服相比，AI 数字员工无需排队等待，可以更快速地定位到客户所需办理的业务并获取相关信息，帮助客户更高效地办理业务，为客户提供更温馨、更便捷的个性化银行服务。 2.在语义理解准确性方面，采用神经网络算法，通过自学习机制持续优化语音识别效果，随着人机交互轮次的增加不断提高识别准确率，提升服务质量，为客户提供更贴心的银行服务。 3.在交互通畅性方面，AI 数字员工服务建立具有现场感的交互模式，可随时被客户打断并继续倾听，并在交互过程中实现客户的情绪感知，保证交互沟通的顺畅，提升业务办理效率。 4.在交互真实性方面，引入静态口腔模型并采用关键点映射技术，为语音驱动口型模型进行优化，提供更真实、更自然的交互体验。
	预期效果	1.与传统线下网点相比，AI 数字员工可减少客户经理在与客户交互过程中带来的主观偏差性引导，为客户提供更准确、详细的金融服务内容解读，提高金融产品的易用性。 2.改进银行业传统的线上客户服务模式，为客户提供 24 小时不间断“面对面、屏对屏”的金融服务，节省大量人力成本，实现更高的办理效率和客户的满意度。
	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，预计涉及客户数 300 万人，年交易笔数 1000 万笔。
创新应用服务信息	服务渠道	线上渠道：南京银行手机银行 APP 线下渠道：网点智能交互大屏和智能讲解机器人
	服务时间	线上渠道：7×24 小时 线下渠道：9:00 至 17:00
	服务用户	南京银行客户
	服务协议书	本项目服务协议包括： 1.《南京银行电子银行客户服务协议》（见附件 1-1-1） 2.《南京银行 APP 用户隐私政策》（见附件 1-1-2）
合法合规性评估	评估机构	南京银行股份有限公司
	评估时间	2020 年 12 月 31 日
	有效期限	3 年
	评估结论	本项目严格按照《中华人民共和国网络安全法》、《中华人民共和国消费者权益保护法》等相关国家法律法规及《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）等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，所提供的金融服务符合相关法律法规要求，可依法合规开展业务应用。		
	评估材料	《合法合规性评估报告-基于人工智能技术的AI数字员工服务》（见附件1-2）		
技术安全性评估	评估机构	北京智游网安科技有限公司		
	评估时间	2021年01月08日		
	有效期限	3年		
	评估结论	本项目严格按照《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）、《移动金融基于声纹识别的安全应用技术规范》（JR/T 0164—2018）、《金融科技创新安全通用规范》（JR/T 0199—2020）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，本项目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—基于人工智能技术的AI数字员工服务》（见附件1-3）		
风险防控	风控措施	1	风险点	手机银行登录后即可使用AI数字员工服务，使用过程中存在更换使用人、被他人盗用和恶意使用等风险。
			防范措施	使用声纹识别、图像识别技术作为辅助身份验证手段，提高安全认证水平，切实保障客户信息与资金安全。
		2	风险点	语音识别技术还存在较大的优化空间，可能会因为AI数字员工语音识别不够精准出现交互偏差，导致客户满意度降低、投诉次数增多。
			防范措施	设立转人工客服的机制，在数字员工无法解答客户问题的时候及时切换人工，快速响应客户并安抚客户情绪。
		3	风险点	在语音识别、声纹识别的过程中，可能存在信息泄露的风险问题。
			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。
		4	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	在项目实施过程中，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。
	风险补偿机制	本项目按照风险补偿机制（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，配套风险拨备资金等补偿措施，切实保障金融消费者合法权益。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	本项目按照退出机制（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，对系统服务进行下线。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	本项目按照应急处置预案（见附件 1-6）妥善处理突发事件，遵循“分级负责、分类处置、快速高效、安全稳妥”的原则，切实保障业务稳定运行和用户合法权益。 1. 突发事件分级：突发事件分为一般风险事件和重大风险事件。一般风险事件是指由于数据存储和传输系统故障，导致系统异常、业务中断的问题。重大风险是指由于系统存在漏洞，导致数据被人窃取盗用的问题。 2. 处置原则：一般风险事件，可以通过数据仓库或者灾备机制恢复数据。重大风险事件必须通过合作协议明确各个合作方之间的权责关系，及相应的违规处理方法，包括终止协议和赔付等。 3. 预防预警与培训演练：在项目上线前进行压力测试和容灾演练，并对相关人员进行培训。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，对异常情况进行告警。一旦发生突发事件，根据其影响范围和危害程度，及时采取有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.南京银行各营业网点 向我行营业网点大堂经理、网点负责人反映问题或通过客户意见簿留言。 2.客服电话： 致电客户服务热线（95302），选择人工服务联系客服代表。 3.门户网站： 通过门户网站（www.njcb.com）在线客服进行留言。 4.微信银行： 关注“南京银行”微信公众号，以文字、图片、语音等形式发送投诉内容。
		投诉受理 与处理机制	南京银行接受投诉后，将指派相关分行核实情况，并及时告知客户投诉进展；项目团队也将及时、全力地协助解决相关问题。
	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试点环境，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试点中出现的投诉举报等相关事宜。 对于涉及相关试点城市的金融科技创新应用项目的投诉举报事项，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。 联系方式：010-66001918 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	我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，已全面开展合规性评估和内控审计，能够有效保障业务连续性和用户信息安全，防范资金失窃风险。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）		

33FJAE48E6F4

附件 1-1

基于人工智能技术的 AI 数字员工服务
服务协议书

本项目服务协议书包括:

《南京银行电子银行个人客户服务协议》

《南京银行 APP 用户隐私政策》

南京银行电子银行个人客户服务协议

【重要提示】：

您作为本协议的乙方，请仔细阅读本协议，特别是免除或者限制责任的条款、法律适用和争议解决条款及其他加粗加黑条款。如您对本协议内容及提示信息有疑问或异议的，请勿进行下一步操作。您通过页面勾选“本人已阅读并同意”或以南京银行股份有限公司认可的其他方式选择接受本协议的，即表示您与南京银行股份有限公司已达成本协议并同意接受本协议的全部约定内容。

甲方：南京银行股份有限公司

乙方：申请南京银行电子银行业务的客户

为明确甲乙双方的权利和义务，规范双方业务行为，甲乙双方本着平等互利的原则，签订本协议并共同遵守。

第一条 定义

如无特别说明，下列用语在本协议中的含义为：

电子银行业务：指甲方利用面向社会公众开放的通讯通道或开放型公众网络、甲方特定自助服务设施或为乙方建立的专用网络等电子银行渠道向乙方提供的银行服务。甲方电子银行渠道包括但不限于个人手机银行、个人网上银行、短信银行、个人电话银行、微信银行等。

身份认证要素：指在电子银行交易中甲方用于认证乙方身份的信息要素，如客户号、登录名、账号（卡号）、密码、数字证书、USB Key、动态口令、签约设置手机号码等。

数字证书：是指用于存放用户身份标识，并对用户发送的电子银行交易信息进行数字及电子签名的有效印鉴。数字证书的存放介质是USBKEY/蓝牙key。

密码：指乙方在电子银行服务中使用的各种密码，如登录密码、交易密码、账户密码等。

电子银行业务指令：指客户凭借相关的身份认证要素通过各类电子银行业务渠道（包括但不限于个人网银、手机银行等）发起的交易请求的统称。

第二条 电子银行服务的开通及服务内容

（一）个人手机银行服务的开通及服务内容

乙方通过甲方手机银行途径登记乙方个人身份基本信息及账户信息，通过甲方识别校验，并按照要求完成其他相关操作后，便可自助开通注册版个人手机银行；该版本手机银行可以提供的服务包括：查询、小额转账、理财业务、基金业务等。乙方可通过银行网点、智能设备、专业版个人网上银行等渠道签约开通专业版个人手机银行，该版本手机银行可以提供的服务包括：查询、转账、理财业务、基金业务、证券业务、信用卡、贷款业务等。

（二）个人网上银行服务的开通及服务内容

乙方通过甲方网站登记乙方个人身份基本信息及账户信息，通过甲方识别校验，并按照要求完成其他相关操作后，便可开通过客版个人网上银行、注册版个人网上银行；过客版提供的服务包括：借记卡明细、余额查询；注册版提供的服务包括：查询、存款业务、基金业务、信用卡业务、生活缴费等。乙方可在银行柜台、智能柜台等渠道签约开通专业版个人网上银行。专业版提供的服务包括：查询、转账、贷款业务、存款业务、基金业务、信用卡业务、保险业务、生活缴费等。

（三）短信银行服务的开通及服务内容

乙方通过银行网点、专业版个人网上银行、等途径登记乙方个人身份基本信息及账户信息，通过甲方识别校验，并按照要求完成其他相关操作后，成为短信银行客户。客户可享受的服务包括：交易提醒、上行短信查询、安全提示、重要公告、营销信息等服务。

（四）电话银行服务的开通及服务内容

乙方通过95302客户服务电话登记乙方个人身份基本信息及账户信息，通过甲方识别校验，并按照要求完成其他相关操作后，自助开通电话银行，成为电话银行的客户。客户可享受的服务包括：查询、转账、挂失、密码修改、业务申请和金融信息查询等多项金融综合服务。

客户享受上述电子银行服务还须具备相关电子设备、能接入相应电子银行系统的网络等前提条件。

第三条 风险提示

乙方使用甲方电子银行服务，应遵守甲方电子银行业务相关规定，并按照甲方操作流程和各项提示进行正确操作，若乙方违反甲方电子银行业务相关规定，或未按照甲方操作流程和各项提示进行正确操作，可能导致资金转账不成功甚至资金被盗等风险。

第四条 乙方的权利和义务

一、乙方权利

（一）乙方有权向甲方申请注册电子银行业务，经甲方审查审批同意后，将有权在遵守国家法律法规和乙方相关业务规则的前提下根据不同的注册项目享受相应的服务。

（二）乙方有权选择申请电子银行业务种类，有权申请开通电子银行业务自助转账功能，并可在甲方规定的最高限额内设定对外转账限额，具体标准以甲方公告为准。

（三）服务有效期内乙方有权申请办理电子银行业务的变更或注销手续。

（四）协议终止或在服务有效期内中止时，乙方无须退回注册相关业务时发放的身份认证设备，如USB Key。

（五）如遇乙方身份认证要素可能发生泄漏时，乙方有权要求甲方采取冻结等必要手段保障乙方账户资金安全.

（六）因网络、通讯故障等原因，乙方不能通过甲方电子银行系统办理业务时，乙方可到甲方营业网点办理相应银行业务。

（七）乙方如对甲方提供的电子银行服务有疑问、建议或意见，可以拨打甲方客户服务电话95302、登录甲方门户网站www.njcb.com.cn或向甲方营业网点咨询、投诉。

二、乙方义务

（一）乙方申办甲方电子银行业务，使用甲方电子银行服务等，均应按甲方规定的程序办理相关手续，自愿遵守《南京银行电子银行交易规则》，执行南京银行电子银行资费标准。乙方获得上述内容（交易规则、资费等）的途径包括但不限于甲方营业网点、甲方门户网站www.njcb.com.cn、甲方客户服务电话95302等。如果上述内容（指交易规则、资费等）发生变化，乙方继续使用甲方电子银行业务的，视为乙方接受修改后的有关内容；如果乙方不接受的，可以办理电子银行业务注销手续或停止使用甲方电子银行业务相关业务功能。

（二）乙方办理电子银行业务注册、注销、变更、修改限额、重置登录密码等手续时，应保证所提供的资料真实、准确、完整、有效，甲方不承担因乙方提供信息不真实、不完整、不准确、无效或非本人资料所造成的风险及损失。

（三）乙方应通过甲方的官方网站或甲方认可的应用商店（包括但不限于App store、腾讯应用宝、华为应用市场、百度手机助手、小米应用商店、vivo应用商店、搜狗手机助手、联想乐商店等）安装甲方的个人手机银行客户端。甲方不承担因乙方使用非上述渠道所造成的风险及损失。

（四）乙方使用甲方电子银行业务应尽到合理注意义务，通过正确的网址或号码等办理；在安全的网络环境中使用，采取及时更新软件、安装系统安全补丁等合理措施，否则由此产生的安全风险由乙方承担。

（五）乙方在使用电子银行业务时，应当按照甲方业务提示和操作流程进行正确操作，因乙方未进行正确操作导致的损失，甲方不承担责任。乙方使用电子银行业务如果涉及甲方其他业务产品的，应当遵守相关业务产品的协议和有关交易规则、交易提示。

（六）乙方在开通电子银行服务功能时提供的身份认证要素及确认的身份认证方式，将作为甲方判断乙方身份的依据，所有使用上述一种或多种乙方身份认证要素及约定的身份认证方式在电子银行渠道实现的操作与交易均视为乙方行为。乙方必须妥善保管本人身份认证要素，并对通过上述方式完成的金融交易负责。甲方执行通过安全程序的电子支付指令后，乙方不得要求变更或撤销电子支付指令。若乙方发生身份认证要素遗失、被盗、遗忘或怀疑已被他人知悉、盗用等情况，应及时通知甲方并办理更换、挂失或重置等手续。办妥上述手续之前所产生的一切后果由乙方承担，乙方不得以身份认证要素遗失、账号及密码等重要信息丢失、被盗用、遗忘或怀疑已被他人知悉、盗用等任何理由否认签约的效力及履行相关合同的义务。

（七）乙方应按照机密的原则设置和保管密码：避免使用简单密码或将姓名、生日、电话号码等与本人明显相关的信息作为密码；不得将本人密码提供给除法律规定外的任何人。如发生密码泄露、遗失或提供给他人，乙方应立即通过电子银行渠道或拨打甲方客服电话“95302”办理账户冻结，并及时前往甲方营业网点办理密码挂失和重置手续。甲方收到乙方上述申请后，将及时为乙方办理账户冻结、密码挂失或重置密码手续。**甲方不承担非因甲方原因造成乙方信息泄露产生的任何风险或损失。**

（八）乙方在接受甲方电子银行服务过程中，所提供的资料信息如有更改，应及时办理电子银行业务变更手续，甲方不承担因乙方未及时向甲方申请维护更新信息所造成的一切后果及风险或损失。

（九）乙方使用甲方手机安全认证功能的，应当在交易的过程中认真核对短信发送编号、短信发送的内容与正在交易事项是否一致，如果因乙方未认真核对短信内容造成损失的，责任由乙方承担。非甲方原因（如短信网络原因造成迟延、信息丢失，乙方手机号错误、手机关机、欠费停机等原因）导致交易无法完成以及导致损失的，甲方不承担责任。

（十）乙方通过网络页面、app点击确认的方式，或使用USBkey登陆并通过网络页面办理业务、点击确认签订业务合同、协议及与业务相关的法律文件，即表示与甲方达成合同并同意接受合同的全部约定内容以及甲方其他与该业务有关的各项规定，与亲笔签名具有同等法律效力，合同双方无需重新补办书面文书。

（十一）乙方通过甲方电子银行渠道办理个人贷款业务，须按照甲方相关系统使用要求及交易规则进行借款项下相关操作，否则因为操作不当而导致的合同未成立、借款未能发放或错误发放等可能带来的不利后果由乙方自行承担。

（十二）乙方认可电子数据的有效性和证据效力。电子数据包括但不限于甲方各电子银行渠道所生成和保留记载的相关电子合同、电子单据、电子凭证、交易记录等相关资料均构成有效证明合同各方之间权利义务关系的确定证据。

（十三）乙方使用甲方提供的电子银行服务，则视同同意接受甲方发送的活动公告、产品信息、金融资讯、祝福问候等增值服务。乙方主动向甲方服务号码发送的短信，费用由乙方承担。

（十四）如乙方因甲方电子银行系统差错、故障等原因获得不当得利的，乙方同意甲方采取冻结、扣划等自力救济措施。

（十五）如乙方发现甲方对其电子银行业务指令的处理确有错误，应及时通知甲方。

（十六）乙方使用甲方电子银行服务，应按照甲方制定并公布的相应收费标准支付服务费用。具体收费标准及优惠政策等，详见甲方在网站及营业网点公布的《服务价目表》。各项收费如有变动，以甲方最新公告为准。

（十七）乙方与第三方发生纠纷的由双方自行解决，甲方无故意或重大过失的，乙方不得以纠纷为由拒绝支付应付甲方的款项。

（十八）乙方不得有意诋毁、损害甲方声誉或恶意攻击甲方电子银行系统。

（十九）乙方长期不使用电子银行业务，应主动申请办理注销手续。

第五条 甲方的权利和义务

一、甲方权利

（一）甲方有权根据乙方资信情况和自身经营情况，决定是否受理乙方的开通电子银行业务的申请。

（二）甲方有权在符合国家及行业相关规定的范围内，制定各类电子银行业务的收费标准，并通过门户网站、营业网点等渠道提前予以公布。

（三）甲方有权根据业务种类、认证方式、客户类型等业务策略设定不同的电子银行交易限额。

（四）甲方有权对其电子银行系统进行升级、改造，并根据业务发展进行服务变更（包括但不限于增加、调整和停止电子银行服务项目）。甲方对上述服务变更，将通过官方网站、营业网点等渠道提前发布公告，不再逐一通知乙方。如果乙方不接受该变更，有权向甲方申请取消电子银行服务；如果甲方发布的上述相关公告生效后乙方继续使用甲方电子银行服务，视为乙方接受该变更。

（五）甲方有权按照相关服务价格标准向乙方收取服务费用。甲方有权调整电子银行业务服务价格标准，但应按照相关规定通过甲方营业网点、甲方网站（网址：http://www.njcb.com.cn）等方式予以提前公告。

（六）若乙方发生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，甲方有权单方终止乙方的电子银行业务，并保留追究乙方责任的权利。

（七）甲方根据乙方的电子银行业务指令办理业务，为乙方办理转账等业务的时间以甲方在电子银行业务系统中处理的时间为准。对所有使用乙方身份认证要素实现的交易均视为乙方行为，由此产生的电子信息记录均作为处理电子银行业务的有效凭据。

（八）甲方有权根据乙方通过电子银行渠道提交的相关业务申请指令，在必要环节采用身份认证，乙方通过身份认证办理的相关业务均视为乙方行为。

（九）甲方有权根据内部授信政策及审批要求对乙方通过电子银行渠道提交的贷款申请进行审批，甲方有权拒绝不符合其内部授信政策及审批要求的贷款申请。

（十）对所有使用乙方银行账号、登录名、密码或数字证书进行的操作均视为乙方所为，该操作所产生的电子信息记录作为甲方处理电子银行业务的有效凭据。甲方不承担因以下情况没有执行乙方提交的电子交易指令所产生的责任：

1. 甲方接收到的电子银行指令信息不明、存在乱码、不完整或信息内容有误等；

2. 乙方账户可用余额或信用额度不足；

3. 乙方账户有挂失、销户等不正常状态；

4. 乙方账户资金被依法冻结或扣划，或存在其他被采取控制措施的情况；

5. 乙方未能按照甲方的有关业务规定正确操作；

6. 乙方拟交易金额大于甲方规定的限额；

7. 乙方在甲方或相关第三方公司公告的非正常交易时间内下达交易指令；

8. 乙方的行为出于欺诈或其他非法目的；

9. 甲方遇到计算机黑客袭击、系统故障、通讯故障、网络拥堵、供电系统故障、电脑病毒、恶意程序攻击等不可归因于甲方的情况。

10. 发生不可抗力（包括但不限于战争、自然灾害等）。

11. 其他不属甲方过失的情况。

（十一）非因甲方过错导致协议终止或在服务有效期内中止时，甲方不退回乙方已支付的有关费用。

（十二）甲方有权修订电子银行交易规则，甲方应将修订内容及时公布在甲方官方网站上。

二、甲方义务

（一）甲方负责为乙方办理电子银行业务，并按乙方注册功能的不同为乙方提供相应的电子银行服务。

（二）甲方在法律法规许可和乙方授权的范围内使用乙方的资料和交易记录。甲方对乙方提供的申请资料和其他信息有保密的义务，但法律法规另有规定的除外。

（三）在甲方系统正常运行并且不出现“甲方权利”中第（八）项的情况下，甲方应根据乙方发送的有效电子指令处理乙方已提交的业务请求。

（四）甲方对电子银行产品所使用的相关软件的合法性承担责任。

（五）甲方有义务为乙方提供电子银行业务咨询服务，并在甲方网站、营业网点公布服务功能介绍、服务操作指南等内容。

（六）甲方收到乙方对电子银行业务的问题反映时，应及时进行调查并告知乙方调查结果。

（七）因甲方过失造成未及时正确执行乙方支付指令，导致乙方损失的，应赔偿乙方的损失，但不包括对指令执行后可以获得的利益的赔偿。甲方的损失赔偿责任在任何情况下均不超过支付指令的金额或乙方直接损失的金额（以较少者为准）。

第六条 服务及交易规则

在遵照甲方电子银行服务规则下，乙方有权在甲方电子银行上享受甲方提供的以下服务。

（一）甲方可以使用公告、电子邮件、发送短信、电话或客户端通知等方式向乙方发送通知，例如通知乙方交易进展情况，或者提示乙方进行相关操作，请乙方及时予以关注。

（二）当乙方在甲方电子银行购买商品及/或服务时，请乙方务必仔细确认所购商品的品名、价格、数量、型号、规格、尺寸或服务的时间、内容、限制性要求等重要事项，并在下单时核实乙方的联系地址、电话、收货人等信息。如乙方填写的收货人非乙方本人的，则该收货人的行为和意思表示产生的法律后果均由乙方承担。

（三）乙方在甲方电子银行交易过程中发生争议的，乙方有权选择与争议方自主协商、或通过甲方客服协助解决交易争议。

第七条 法律适用条款

（一）本协议的成立、生效、履行和解释，均适用中华人民共和国法律；法律无明文规定的，可适用通行的金融惯例。

（二）本协议是甲方的其他既有协议和约定的补充而非替代文件，如本协议与其他既有协议和约定有冲突，涉及电子银行业务的，应以本协议为准。

第八条 差错和争议的解决

（一）乙方发现自身未按规定操作，或由于自身其他原因造成电子银行业务指令未执行、未适当执行、延迟执行的，应及时拨打甲方客户服务电话95302或到甲方营业网点通知甲方。甲方应积极调查并告知乙方调查结果。

（二）本协议在履行过程中发生争议，可以通过协商解决；协商不成的，任何一方均可向**甲方所在地有管辖权的人民法院**提起诉讼。

第九条 协议的中止和终止

一、发生以下情况的，本协议中止：

（一）甲方提供的电子银行服务受乙方注册账户（卡）状态的制约，如乙方账户（卡）因挂失、止付、清户等原因不能使用，相关服务自动中止；

（二）乙方未按时支付电子银行相关服务费用的；

（三）其他导致协议中止情况的。

待上述情况消除后，本协议自动恢复执行。

二、发生以下情况之一时，本协议终止：

（一）乙方电子银行业务注销手续办理完毕；

（二）如甲方与第三方公司终止业务合作，乙方申办相关业务时签订的本协议自动终止；

（三）乙方恶意诋毁、损害甲方声誉或恶意攻击甲方电子银行系统的；

（四）乙方利用甲方电子银行系统从事违法犯罪活动的。协议终止并不意味着终止前所发生的未完成交易指令的撤销，也不能消除因终止前的交易所带来的任何法律后果。

第十条 协议的效力和生效

（一）甲方相关业务回单、各类电子银行业务申请书为本协议的组成部分。

（二）本协议自乙方阅读并签署或在线上勾选“本人已阅读并同意”且甲方在电子银行系统为乙方完成注册起生效。

（三）本协议的任何条款如因任何原因而被确认无效，都不影响本协议其他条款的效力。

（四）若乙方的银行卡开通电子银行业务相关功能后办理换卡手续，与原银行卡相关的电子银行服务自动转至新银行卡，本协议继续有效。

（五）本协议由甲方制定、修改。甲方如对本协议进行修改，自修改后发布之日起生效。甲方将通过官方网站、营业网点等渠道同步修改更新，不再逐一通知乙方。乙方若因对协议的修改有异议而决定不继续使用甲方提供的电子银行服务的，可办理电子银行业务的注销手续（如需）；未注销电子银行业务的，视为同意接受修改后的协议内容，受修改后协议的约束。

南京银行APP用户隐私政策

尊敬的用户（以下简称“您”），感谢您使用南京银行APP，南京银行APP由南京银行股份有限公司（以下简称“我们”）管理。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，我们依据《中华人民共和国网络安全法》、《信息安全技术个人信息安全规范》（GB/T 35273-2017）以及其他相关法律法规和技术规范，制定了《南京银行APP用户隐私政策》（以下简称“本政策”）。您在使用南京银行APP时，我们将按照本政策处理和保护您的个人信息。

本政策与您使用我们的服务关系紧密，请您在使用/继续使用南京银行APP前，仔细阅读并充分理解本政策，并在需要时，按照本政策的指引，做出您认为适当的选择。**对本政策中与您的权益存在重大关系的条款，我们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，并同意我们将按照本政策来收集、使用、存储和共享您的相关信息；如您不同意本政策中的任何条款，将有可能导致南京银行APP的产品与服务无法正常运行，或者无法达到我们拟达到的服务效果，您应立即停止访问和使用南京银行APP。**

阅读过程中，如您有任何疑问，可联系我们的客服（全国服务热线：95302）咨询。

本政策将帮助您了解以下内容：

一、如何收集和使用您的个人信息

二、如何使用Cookie和同类技术

三、对外提供您的个人信息

四、如何存储和保护您的个人信息

五、如何管理您的个人信息

六、未成年人信息的保护

七、本政策的适用及更新

八、如何联系我们

一、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，如**姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息**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个人信息，如**个人财产信息、个人健康生理信息、个人生物识别信息、个人身份信息、网络身份标识信息及其他信息**。

上述信息所包含的内容，均出自于GB/T35273《信息安全技术个人信息安全规范》。

（一）收集

1. 您在使用以下服务时，**我们将会收集或验证您的个人信息和设备信息**：

（1）**在您注册南京银行APP时**，我们会验证您的**姓名、身份证件信息、手机号码信息、短信验证码、银行卡信息、交易密码**，以帮助您完成注册；

（2）**在您使用账号成功登录南京银行APP时**，我们需要获取您的**设备类型、设备型号名称、MAC地址、IP版本号、IP地址信息**用于身份验证，以防账户风险；

（3）**在您在线开立南京银行II、III类账户、为II、III类账户新增绑定银行卡时**，我们会收集您的**姓名、身份证件信息（包括证件类型、证件号码、姓名、性别、民族）、手机号码信息、短信验证码、银行卡信息，并进行人脸活体识别和OCR上传证件**，以便验证您的身份的真实性；

如果您拒绝提供这些信息，对应服务将无法进行，您可以以游客身份浏览部分页面及功能。

2. 您在使用以下服务时，**我们将会收集或验证您的个人信息**：

（1）**当您在线申请信用卡、申请贷款时**，我们会收集您的**姓名、身份证件信息（包括证件类型、证件号码、姓名、性别、民族）、手机号码信息、短信验证码、银行卡信息，并进行人脸活体识别和OCR上传证件**，以便验证您的身份的真实性；

（2）**在您使用信用卡激活服务时**，我们会校验**信用卡CVV信息及卡片有效期**；使用转账服务时，我们会收集您的**收款人、收款账户、转账金额**信息和进行**人脸活体识别**；

如果您拒绝提供前述信息，对应服务将无法进行，但不影响您使用我们提供的其他服务。

3. 您在使用转账汇款以及手机号码绑定服务时，根据您每日转账金额的大小，我们需要调用或使用您的设备功能用于验证您的身份，以保障您的账户和资金安全。您可以**使用交易密码、面容识别/指纹识别、短信动态密码、语音动态密码、数字证书（如华为手机盾、蓝牙KEY）、人脸活体识别方式完成验证**，当您选择**面容识别/指纹识别**方式时，我们仅接收设备验证结果，并**不收集您的指纹信息和面容ID信息**，当安全风险等级提高时，我们可能会提示您进行再次验证。如您不想使用上述功能，每日转账限额会有相应的限制，但不影响您使用我们提供的其他服务。

4. 您在使用以下服务时，**我们可能需要您在您的设备中向我们开启您的摄像头（相机）、相册、地理位置（定位）、麦克风、通讯录、日历等功能的访问权限，以实现这些功能所涉及的信息收集和使用**：

（1）基于摄像头（相机）的功能：您可开启摄像头进行身份校验（**身份证识别及人脸活体识别**）、银行卡识别、拍照并上传图片操作以及使用视频服务。

（2）基于相册的功能：当您进行身份认证需要提交证明材料时，您可从本地相册中选择图片上传；当您获取转账汇款电子回单时，您帮助我们完成将电子回单图片存入本地相册的操作。

（3）基于地理位置的功能：您可开启定位服务，以便在网点地图、网点预约、生活缴费等功能中获得更好的客户体验。

（4）基于麦克风的功能：您可选择麦克风设备来进行特定场景的语音搜索与视频对话。

（5）基于通讯录的功能：当您使用话费充值、转账汇款时，您可选择并导入通讯录中的联系人信息，开启该功能将避免您手动重复填写上述信息。

（6）基于指纹、面容等生物特征识别的功能：您可授权调取您使用的设备的**面容识别/指纹验证**功能，帮助我们完成**个人身份识别、登录、验证、确权、交易等**指令操作。**当您进行面容识别/指纹验证时，我们仅收集验证结果，并不收集您的生物特征信息。**

（7）基于电话的功能：您在使用“联系我们”和“客服热线”功能时，可一键拨打客服号码咨询业务，开启该功能将避免您手动重复填写电话号码。

（8）基于短信的功能：当您转账过程中需要输入短信验证码时，开启该功能可自动读取您的短信验证码，避免您手动重复填写上述信息。

（9）基于蓝牙的功能：当您转账过程中需要使用蓝牙KEY认证时，开启蓝牙服务，以便我们签名验签您的转账信息。

您确认并同意开启这些权限即代表您授权我们可以收集和使用这些信息；您也可以遵循您所使用设备的操作系统指示变更或者取消这些授权，则我们将不再继续收集和使用您的这些信息，也无法为您提供上述与这些授权所对应的功能，但这不会对您使用南京银行APP其他服务产生影响。

5．根据相关法律法规及国家标准，在以下情形中，**我们可能会依法收集并使用您的个人信息无需征得您的授权同意：**

（1）与国家安全、国防安全有关的；

（2）与公共安全、公共卫生、重大公共利益有关的；

（3）与犯罪侦查、起诉、审判和判决执行等有关的；

（4）根据您的要求签订和履行合同所必需的；

（5）出于维护您或他人的生命安全等重大合法权益但又很难得到您本人同意的；

（6）所收集的用户信息是您自行向社会公众公开的；

（7）从合法公开披露的信息中收集用户信息，如合法的新闻报道、政府信息公开等渠道；

（8）用于维护服务的安全和合规所必需的，例如发现、处置产品和服务的故障；

（9）法律法规规定的其他情形。

6．**我们向您提供的服务是不断更新和发展的，如您选择使用了前述说明当中尚未涵盖的其他服务，基于该服务我们需要收集您的信息的，我们会通过页面提示、交互流程或协议约定的方式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。我们会按照本政策以及相应的用户协议约定收集、使用、存储、对外提供及保护您的信息。**

（二）使用

我们为了遵守国家法律法规及监管要求，以及向您提供服务及提升服务质量，或保障您的账户和资金安全，**我们会在以下情形中使用您的信息：**

1. 我们会根据本隐私政策的约定并为实现我们的服务或功能对所收集的您的个人信息进行使用。

2. 为了使您知晓使用南京银行APP服务的状态，我们会向您发送服务提醒。您可以通过手机系统设置中的通知设置，关闭服务提醒，也可以通过通知设置重新开启服务提醒。

3. 为了保障服务的稳定性与安全性，我们会将您的信息用于身份验证、安全防范、诈骗监测、预防或禁止非法活动、降低风险、存档和备份用途。

4. 根据法律法规或监管要求向相关部门进行报告。

5. 邀请您参与我们服务或功能有关的客户调研。

6. 在收集您的个人信息后，我们在通过技术手段对您的信息数据进行去标识化处理后，该等去标识化的信息将无法识别信息主体，去标识化的信息我们有权在不经您同意的情况下直接使用，有权对用户数据库进行分析并予以商业化的利用。

7. 我们会对我们的服务或功能使用情况进行统计，并可能会与公众或第三方共享这些统计信息，以展示我们的服务或功能的整体使用趋势。但这些统计信息不包含您的任何身份识别信息。

8. 当我们展示您的信息时，我们会采用包括内容替换、匿名化处理方式对您的信息进行脱敏，以保护您的信息安全。

二、如何使用Cookie和同类技术

为确保南京银行APP带给您更轻松的使用体验，我们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。借助于Cookie，南京银行APP能够简化您重复输入信息以登录账户的步骤、存储您的偏好设置、帮助判断您的登录状态以及账户或数据安全。我们不会将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，大部分网络浏览器都设有阻止Cookie的功能。如果您选择管理或删除移动设备上保存的所有Cookie，则需要您在每一次访问南京银行APP时更改用户设置。

三、对外提供您的个人信息

（一）共享

1. 业务共享

我们承诺对您的信息进行保密。**除法律法规及监管部门另有规定外，我们仅在以下情形中与第三方共享您的信息，第三方包括我们的关联公司、合作金融机构以及其他合作伙伴**，您的信息类型包括**有效证件信息、联系方式**。在将信息提供给第三方前，我们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。我们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，要求第三方对您的信息采取保护措施。

（1）某些产品或服务可能由第三方提供或由我们与第三方共同提供，因此，只有共享您的信息，才能提供您需要的产品或服务。例如：您通过南京银行APP购买基金产品和保险产品时，我们需要向合作金融机构提供您的**有效证件信息与联系方式**，以保证您完成购买流程合规性要求以及保证您的资产

准确无误的登记；又如：您通过南京银行APP进行水电煤等生活缴费时，我们需要把您填写的**户号和姓名等信息**提供给合作的公共事业单位，才能使您完成缴费；

（2）如您选择参与我们和第三方联合开展的抽奖、竞赛或类似推广活动，我们可能与其共享活动过程中产生的、为完成活动所必要的信息，以便第三方能及时向您发放奖品或为您提供服务，我们会依据法律法规或国家标准的要求，在活动规则页面或通过其他途径向您明确告知需要向第三方提供何种个人信息；

（3）在某些特定使用场景下，我们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，**与第三方服务商共享您的必要信息。共享信息的类型、SDK名称及第三方公司类型详见附件。**我们会对合作方获取有关信息的软件工具开发包（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，令其按照我们的委托目的、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。

（4）事先获得您明确同意的情况下，我们会在法律法规允许且不违背公序良俗的范围内，依据您的授权范围与第三方共享您的信息。

2. 实名认证

为准确核实您的身份信息，以便为您提供服务，在获得您授权的前提下，需要将您的**证件信息、卡片信息、设备信息、IP地址、GPS等**信息提供给中国人民银行、中国银联、公安部及其它第三方合作机构进行身份验证。

3. 关于向TalkingData共享信息的特别条款：

我们使用由第三方TalkingData提供的统计分析服务，TalkingData及其服务由我们审慎地选择，且我们和TalkingData将共同运用各种安全技术和程序对数据进行加密处理，实施完善的机制来保护您的个人信息安全，以免遭受未经授权的访问、使用或披露。

（1）服务申明

如果您选择使用我们的服务，那么您同意我们及TalkingData收集和使用与此策略相关的信息。我们收集的个人信息将用于提供和改进服务。除本隐私政策所述外，我们不会使用或分享您的信息；

（2）使用TalkingData服务详述

a. TalkingData为移动应用提供数据统计分析服务，为了您在使用我们的服务时获得更好的体验，通过您在应用中集成了TalkingData数据SDK或API后，您的应用将通过技术手段收集和传送您的相关数据，通过我们的服务来分析这些数据以了解您的应用在不同终端设备上、使用平台或应用分发渠道的表现和使用的情况；

b. 您的数据通常包括但不限于：SDK或API版本、平台、时间戳、应用标识符、应用程序版本、应用分发渠道、iOS供应商标识符(IDFV)、iOS广告标识符(IDFA)、安卓广告主标识符、网卡(MAC)地址、国际移动设备识别码(IMEI)、设备型号、终端制造厂商、终端设备操作系统版本、会话启动/停止时间、语言所在地、移动网络/国家代码、时区和网络状态(WiFi等)、硬盘、CPU、电池使用及地理位置情况等；

c. 根据您移动应用的类型和您对统计分析选项的要求，您的数据还有可能包括:使用者性别、年龄、用户触发特定事件、错误报告和页面浏览量等;

（3）安全

a. 我们重视您的信任，对于您提供的个人信息及数据将全部保存在南京银行的服务器上，我们努力使用商业上可接受的方法来保护信息的安全性和保密性，包括但不限于：防火墙和数据备份措施；数据中心的访问权限限制；对移动终端的识别性信息进行加密处理等;

b. 我们已经建立健全数据安全管理体系，包括对用户信息进行分级分类、加密保存、数据访问权限划分，指定内部数据管理制度和操作规程，从数据的获取、使用、销毁都有严格的流程要求，避免用户隐私数据被非法使用;

c. 我们会采取一切合理可行的措施，确保未收集无关的个人信息，我们只会在达成本政策所述目的所需的期限内保留您的个人信息，除非需要延长保留或受到法律的允许。另外请您理解，根据目前技术水平，在互联网上没有任何传输方法或电子存储方法是100%安全可靠的，所以我们无法保证它的绝对安全。

（二）转让

我们不会将您的个人信息转让给任何公司、组织和个人，**但以下情况除外:**

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. 在涉及资产转让、收购、兼并、重组或破产清算时，如涉及到个人信息转让，我们会向您告知有关情况，并要求新的持有您的个人信息的公司、组织继续受本政策的约束，否则我们将要求该公司、组织重新向您征求授权同意。

（三）公开披露

除在公布中奖活动名单时会脱敏展示中奖者手机号或南京银行APP登录名外，原则上我们不会将您的信息进行公开披露，但经您另行明确同意的除外。如确需披露，我们会获取您的同意，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。

（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的，或者此处约定的其他合理情形的，**我们可能会共享、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、如何存储和保护您的个人信息

（一）我们在中华人民共和国境内收集和产生的个人信息将存储在中华人民共和国内。如部分产品涉及跨境业务，我们需要向境外机构传输境内收集的相关个人信息的，我们会按照法律法规和相关监管部门的规定执行，并通过签订协议、现场核查等有效措施，要求境外机构为所获得的您的个人信息保密。我们仅在法律法规要求的最短期限内，以及为实现本政策声明的目的所必须的最低时限内保存您的个人信息。当超出数据保存期限后，我们会对您的信息进行删除或匿名化处理。例如：当您使用南京银行APP服务时，我们需要一直保存您的手机号码，以保证您正常使用该服务，当您注销南京银行APP账户后，我们将删除相应信息。

（二）为保障您的信息安全，我们致力于使用各种安全技术及配套的管理体系来尽量降低您的信息被泄露、毁损、误用、非授权访问、非授权披露和更改的风险。例如：通过网络安全层软件（SSL）进行加密传输、信息加密存储、严格限制数据中心的访问、使用专用网络通道及网络代理。同时我们设立了相关内控制度，对可能接触到您的信息的工作人员采取最小够用授权原则；对工作人员处理您的信息的行为进行系统监控，不断对工作人员培训相关法律法规及隐私安全准则和安全意识强化宣导。

（三）我们会定期组织内部相关人员进行应急响应培训和应急演练，使其掌握岗位职责和应急处置策略和规程。在不幸发生个人信息安全事件后，我们将按照法律法规的要求，及时向您告知：安全事件的基本情况和可能的影响、我们已采取或将要采取的处置措施、您可自主防范和降低风险的建议、对您的补救措施等。我们将及时将事件相关情况以APP推送通知、发送邮件/短消息等方式（我们将根据实际情况选择一种或多种方式）告知您，难以逐一告知个人信息主体时，我们会采取合理、有效的方式发布公告。同时，我们还将按照监管部门要求，主动上报个人信息安全事件的处置情况。若您的合法权益受损，我们将承担相应的法律责任。

（四）您接入南京银行APP所用的系统和通讯网络，有可能因我们可控范围外的因素而出现问题。因此，**我们强烈建议您采取积极措施保护个人信息的安全，包括但不限于使用复杂密码、定期修改密码、不将自己的账号密码及相关个人信息透露给他人。请您务必妥善保管好您的南京银行APP登录名及其他身份要素。您在使用南京银行APP时，我们会通过您的登录名及其他身份要素来识别您的身份。一旦您泄漏了前述信息，您可能会蒙受损失，并可能产生对您不利的法律后果。如您发现南京银行APP登录名及/或其他身份要素可能或已经泄露时，请您立即和我们取得联系，以便我们及时采取相应措施以避免或降低相关损失。**

（五）请您理解，尽管已经采取了上述合理有效措施，并已经遵守了相关法律规定要求的标准，由于技术的限制以及可能存在的各种恶意手段，在互联网行业，即便竭尽所能加强安全措施，也不可能始终保证信息百分之百的安全，我们将尽力确保您提供给我们的个人信息的安全性。

（六）您一旦离开南京银行APP，浏览或使用其他网站、服务及内容资源，我们将没有能力和直接义务保护您在南京银行APP之外的软件、网站提交的任何个人信息，无论您登录、浏览或使用上述软件、网站是否基于南京银行APP上的链接或引导。

（七）在您终止使用南京银行APP后，我们会停止对您的信息的收集和使用，法律法规或监管部门另有规定的除外。如我们停止运营，我们将及时停止收集您个人信息的活动，将停止运营的通知以逐一送达或公告的形式通知您，并对所持有的您的个人信息进行删除或匿名化处理，法律法规或监管部门另有规定的除外。

五、如何管理您的个人信息

按照中国相关的法律法规和监管规定，我们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

您有权通过我们柜面、南京银行APP等渠道访问及更正、更新您的个人信息，法律法规另有规定的除外。您有责任及时更新您的个人信息。在您修改个人信息之前，我们会验证您的身份。您登录南京银行APP后，可以进行个人信息设置、登录设置、安全设置、支付设置和通知设置：

1. 个人信息设置--主要功能包括个人基本信息修改（含国籍、证件有效期、学历、婚姻状态、职业信息、住宅信息、收入信息）、登录别名设置、个人头像设置。

2. 登录设置--主要功能包括登录密码修改、登录方式设置（含手势密码登录、面部识别/指纹登录和登录密码登录）。

3. 安全设置--主要功能包括修改安全认证方式修改（含面部识别/指纹认证、动态密码认证、鑫盾安全认证和手机盾认证）、蓝牙KEY设置、转账限额设置（含日累计限额、日累计笔数、年累计限额、小额指纹转账限额）。

4. 支付设置--主要功能包括网上支付开通/关闭、交易安全锁（含无卡支付锁、他行ATM锁、POS锁、境外锁）。

5. 通知设置--主要功能包括待办提醒开/关、精彩活动提醒开/关、动账通知开/关。

对于修改个人签约手机号信息，可通过我们柜台或智能柜台办理。

对于您在行使上述权利过程中遇到的困难，或其他可能未/无法向您提供在线自行更正/修改权限的，我们会通过网点或官方邮箱对您的身份进行验证，在更正不影响信息的客观性和准确性的情况下，您有权对错误或不完整的信息作出更正或修改，或在特定情况下，尤其是数据错误时，通过我们公布的反馈与报错等措施将您的更正/修改申请提交给我们，要求我们更正或修改您的数据，但法律法规另有规定的除外。但出于安全性和身份识别的考虑，您可能无法修改注册时提交的某些初始注册信息。

（二）删除

1. 一般而言，我们只会在法律法规规定或必需且最短的时间内保存您的个人信息。您在我们的产品与/或服务页面中可以直接清除或删除的信息，包括绑定银行卡、消息记录、缓存记录。例如：您可以通过“首页-我的账户-点击卡号-卡管理-删除下挂”路径删除南京银行APP中下挂的账户；您可以通过“首页-消息中心（右上角）-动账通知”路径删除您的动账消息等。

2. 在以下情形下，您可以直接向我们提出删除您个人信息的请求，但已做数据匿名化处理或法律法规另有规定的除外。

- 你如果我们违反法律法规规定，收集、使用您的个人信息；
- 如果我们违反了与您的约定，收集、使用您的个人信息；
- 如果您不再使用我们的产品或服务，或您注销了南京银行App账号；
- 如果我们不再为您提供产品或服务；
- 法律法规等规定的其他情形。

当您从我们的服务中删除信息后，我们可能不会立即在备份系统中删除相应的信息，但会在备份更新时删除这些信息。

（三）改变您授权同意的范围或撤回您的授权

您可以通过删除信息、关闭设备功能、在隐私设置等方式改变部分您授权我们继续收集个人信息的范围或撤回您的授权。您也可以通过注销账户的方式，撤回我们继续收集您个人信息的全部授权。

请您注意，您注销南京银行APP的同时，将视同您撤回了对本政策的同意，我们将不再收集相应的个人信息。但您撤回同意的决定，不会影响此前基于您的授权而开展的个人信息收集。

（四）注销账户

您可通过南京银行个人专业版网上银行（自助开通-手机银行-关闭）、短信银行（使用手机银行预留手机号编辑短信“03SJYHJY”发送至95302）或通过南京银行网点注销您的南京银行APP账户。**您注销南京银行APP的行为是不可追溯行为，一旦您注销成功，我们将不会再收集、使用或对外提供与该账户相关的个人信息，但您在使用南京银行APP服务期间提供或产生的信息我们仍需按照监管要求的时间进行保存，且在该保存的时间内依法配合有权机关的查询。**

（五）响应您的请求

如果您无法通过上述方式访问、更正或删除您的用户信息，或您需要访问、更正或删除您在使用我们服务或功能时所产生的其他用户信息，或您认为我们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们取得联系。为了保障安全，我们可能需要您提供书面请求，或以其他方式证明您的身份，我们将在收到您反馈并验证您的身份后的15天内答复您的请求。**对于您合理的请求，我们原则上不收取费用，但对多次重复、超出合理限度的请求，我们将视情况收取一定成本费用。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，我们可能会将予以拒绝。**

尽管有上述约定，但根据相关法律法规、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，我们将可能无法响应您的请求：**

1. 与国家安全、国防安全相关的。

2. 与公共安全、公共卫生、重大公共利益相关的。

3. 与犯罪侦查、起诉、审判和判决执行等相关的。

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、未成年人信息的保护

（一）未成年人使用我们服务，必须在其父母或者其他监护人的监护下进行。我们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们的服务或向我们提供您的信息。对于经父母或监护人同意而使用您的信息的情况，我们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们的服务或向我们提供信息，请您立即终止使用我们的服务并及时通知我们，以便我们采取相应的措施。**

（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们。

七、本政策的适用及更新

根据国家法律法规变化及服务运营需要，我们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们官网（www.njcb.com.cn）、南京银行APP等渠道公布，**您对本政策修改内容无异议的，应当在登录南京银行APP后以点击确认的方式对新政策进行确认，否则将不能再使用南京银行APP。**

八、如何联系我们

如您对本政策存在任何疑问，或任何相关的投诉、意见，请通过南京银行APP中“我的-智能客服”联系人工客服，或通过客服热线95302、南京银行官方微信、以及我们各营业网点进行咨询或反映。为保障安全，我们需要先验证您的身份和凭证资料，验证通过后将在五个工作日内作出答复，特殊情形下最长将在不超过15天或法律法规规定期限内作出答复。如您不同意本政策授权条款的部分或全部，应当停止使用南京银行APP。

公司名称：南京银行股份有限公司

注册地址：江苏省南京市玄武区中山路288号

个人信息保护负责人联系方式：95302@njcb.com.cn

版本号：1.1

协议发布时间：2019年10月21日

协议更新时间：2020年 月 日

协议生效时间：2020年 月 日

附件：SDK收集使用个人信息情况列举

是否嵌入第三方代码、插件传输个人信息	SDK名称	涉及信息	使用场景	第三方机构名称

是	旷视人脸	相机权限，人脸信息	贷款申请	北京旷视科技有限公司
是	佐罗人脸	相机权限，人脸信息	注册	阿里巴巴网络技术有限公司
是	ifaa 指纹	设备号,设备类型	登录，转账，支付	北京一砂信息技术有限公司
是	语音识别	音频权限	智能搜索	科大讯飞股份有限公司
是	鑫口令	手机号	活动	安讯科技有限责任公司
是	设备指纹	客户号、个人常用设备信息	交易反欺诈	邦盛科技有限公司
是	蓝牙市名卡充值	蓝牙权限	充值	南京市市民卡公司
是	听云	客户号和设备号，设备类型	性能监测	北京基调网络股份有限公司
是	手机盾	客户号和设备号，设备类型	转账	北京扬帆伟业科技有限公司
是	蓝牙 ukey	蓝牙权限	转账	飞天诚信科技股份有限公司
是	鑫盾	设备号和客户号	转账	北京芯盾集团有限公司
是	身份证识别 OCR	相机权限	ETC，个人信息补录	上海合合信息科技股份有限公司
是	银行卡识别 OCR	相机权限	注册	上海合合信息科技股份有限公司
是	智能 3d 机器人	姓名、性别、客户等级、客户号、银行卡号、积分、总资产等	数字营业厅	南京硅基智能科技有限公司
是	NJVideoChat vidyo 视频	客户号，设备号，设备类型，运营商和设备信号，相机权限	法人面签，视频核保等	信雅达系统工程股份有限公司
是	飞虎视屏	相机权限	视频互动，法人面签，视频核保	飞虎互动科技有限公司
是	极验	设备号，设备类型	安全验证	武汉极意网络科技有限公司
是	直销 eid	设备号，设备类型	注册	北京科蓝软件系统股份有限公司
是	华为推送	设备号，设备类型	动账通知	华为

是	百度地图	位置信息	地图定位	北京百度网讯科技有限公司
是	高德地图	位置信息	地图定位	高德软件有限公司
是	AndFix 热修复工具	存储权限，存储图片和文件	直销银行同盾	阿里巴巴网络技术有限公司
是	数据库加密 SDK	存储权限，本地保存数据	智能客服聊天	Sqlcipher 开源项目
是	腾讯开发插件库	设备号，设备类型	分享	深圳市腾讯计算机系统有限公司
是	极光推送	设备号，设备类型	直销推送	深圳市和讯华谷信息技术有限公司
是	Zxing 二维码扫描	相机权限	二维码识别和生成	谷歌
是	网易云信-即时通讯	麦克风权限，相机权限	飞虎视频通讯	网易公司
是	QQ 互联	设备号，设备类型	分享	深圳市腾讯计算机系统有限公司
是	支付宝支付	设备号，设备类型	支付	支付宝（中国）网络技术有限公司
是	腾讯 TBS	设备号，设备类型	框架	深圳市腾讯计算机系统有限公司

33FJAE4AW 2RL

附件 1-2

基于人工智能技术的 AI 数字员工服务合法合规性评估报告

本项目严格按照《中华人民共和国网络安全法》、《中华人民共和国消费者权益保护法》等相关国家法律法规及《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）等金融行业相关政策文件要求进行设计，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要求，可依法合规开展业务应用。具体报告内容如下:

基于人工智能技术的 AI 数字员工服务以金融业数字化转型、人工智能迅速发展为背景，依托南京银行手机银行客户端，利用先进的语音交互、形象建模等技术构建面向在线客户的数字员工智能服务体系，打造专属的 3D 拟人数字员工，实现基础业务办理、客服答疑、产品咨询等功能，为广大基础客群提供 24 小时不间断服务，同时提供准确、标准化的产品信息解读，节省大量客服人力成本，提高业务办理效率，提升客户体验。

在业务合规方面，基于人工智能技术的 AI 数字员工服务是在我行现有各类业务功能的基础上，利用先进技术对银行服务模式进行创新，没有创造新的金融产品，符合相关监管

文件的要求。

在数据合规方面，我行严格执行《银行业金融机构数据治理指引》，依法合规采集和应用客户数据，不断完善数据安全技术，定期审计数据安全，做到依法保护客户隐私和数据安全。

在网络安全合规方面，我行严格执行《中华人民共和国网络安全法》，合理设置和使用防火墙、防病毒网关、入侵检测等安全产品，同时基于大数据、人工智能等技术进行实时监控，全面识别安全风险事件，保证客户信息的安全。

在技术提供方资质及行为合规方面，在合作前根据不同类型制定不同的准入标准，合作过程中严格遵循行内风险政策和准入要求对技术提供方进行资质审查，定期跟踪监控合作方经营、资质变化情况，及时发现过程风险问题并视情况采取风险提示、警告、整改、终止合作等措施。

经评估，该项目与现行监管要求不违背，所提供金融服务符合相关法律法规及金融行业政策文件要求，可依法合规开展业务。

南京银行股份有限公司

2020 年 12 月 31 日

33FJAE4AW 2RK

附件 1-3

基于人工智能技术的 AI 数字员工服务
技术安全性评估报告

本项目严格按照《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）、《移动金融基于声纹识别的安全应用技术规范》（JR/T 0164—2018）、《金融科技创新安全通用规范》（JR/T 0199—2020）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，本项目符合现有相关行业标准要求。

北京智游网安科技有限公司

2021 年 01 月 08 日

目录

目录.....1

1 检测依据.....3

2 检测结果概览.....4

2.1 分析结果统计.....4

2.2 分析结果概览.....4

3 检测详情.....5

3.1 移动 SDK 基本信息检测.....5

3.1.1 SDK 版本信息.....5

3.1.2 应用权限信息检测.....6

3.2 移动 SDK 安全规范检测.....6

3.2.1 程序/代码安全.....6

3.2.1.1 源代码反编译安全（安全）.....6

3.2.1.2 代码混淆检测（安全）.....8

3.2.1.3 SO 保护检测（安全）.....8

3.2.1.4 H5 代码安全（安全）.....10

3.2.1.5 权限滥用检测（安全）.....10

3.2.1.6 硬编码检测（安全）.....12

3.2.2 数据安全.....13

3.2.2.1 敏感信息获取检测（安全）.....13

3.2.2.2 证书文件明文储存检测（安全）.....14

3.2.3 漏洞检测.....15

3.2.3.1 未移除有风险的 WebView 系统隐藏接口漏洞（安全）.....15

3.2.3.2 WebView 组件忽略 SSL 证书验证错误检测（安全）.....16

3.2.4 移动金融规范检测.....18

3.2.4.1 合规检测（安全）.....18

4 深圳爱加密科技有限公司.....19

1 检测依据

《信息安全技术移动智能终端个人信息保护技术要求》

《YD/T 1438-2006 数字移动台应用层软件功能要求和测试方法》

《YD/T 2307-2011 数字移动通信终端通用功能技术要求和测试方法》

《电子银行业务管理办法》

《电子银行安全评估指引》

《中国金融移动支付客户端技术规范》

《中国金融移动支付应用安全规范》

《移动互联网应用软件安全评估大纲》

《JR/T 0171—2020 个人金融信息保护技术规范》

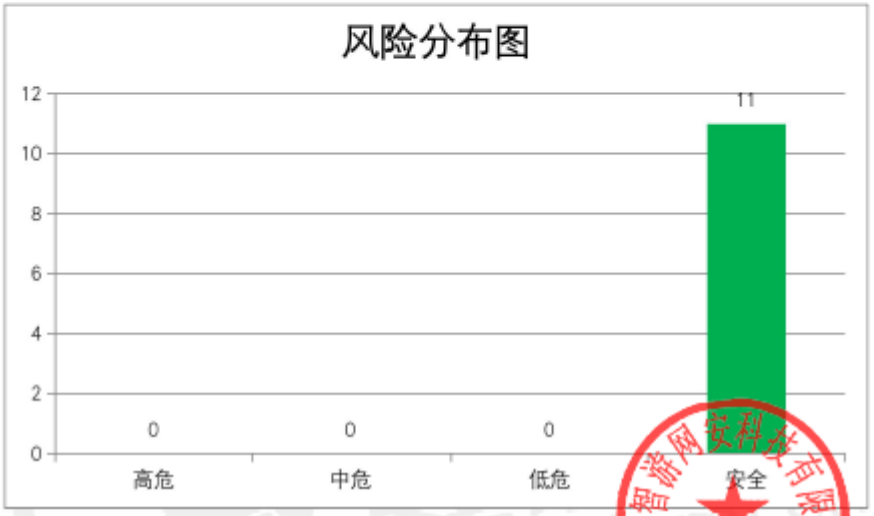
《JR/T 0092—2019 移动金融客户端应用软件安全管理规范》

《JR/T 0164—2018 移动金融基于声纹识别的安全应用技术规范》

《JR/T 0199—2020 金融科技创新安全通用规范》

2 检测结果概览

2.1 分析结果统计



2.2 分析结果概览

序号	风险大类	检测项目	危险系数
1	程序/代码安全	源代码反编译安全	安全
2		代码混淆检测	安全
3		SO 保护检测	安全
4		H5 代码安全	安全
5		权限滥用检测	安全
6		密钥硬编码风险	安全
7	数据安全	敏感信息获取检测	安全

序号	风险大类	检测项目	危险系数
8		证书文件明文储存检测	安全
9	漏洞检测	未移除有风险的 WebView 系统隐藏接口漏洞	安全
10		WebView 组件忽略 SSL 证书验证错误检测	安全
11	移动金融规范检测	合规检测	安全

3 检测详情

3.1 移动 SDK 基本信息检测

3.1.1 SDK 版本信息

SDK 版本	20200811093738
SDK 信息	MD5 Hash
dh_basic-release-39_20200811093738_sec.aar	6985F2535799CEFFB8B811E319C96574
dh_sdk_njcb-release-39_20200811093751_sec.aar	25C409466908814B1226F429C75BD849

3.1.2 应用权限信息检测

序号	权限描述	权限名称	敏感等级
高敏感权限：0 项			
中敏感权限：0 项			
低敏感权限：5 项			
1	访问网络	android.permission.INTERNET	低
2	访问网络信息	android.permission.ACCESS_NETWORK_STATE	低
3	写入外部存储	android.permission.WRITE_EXTERNAL_STORAGE	低
	读取外部存储	android.permission. READ_EXTERNAL_STORAGE	低
4	修改音频设置	android.permission. MODIFY_AUDIO_SETTINGS	低
5	录制音频	android.permission.RECORD_AUDIO	低

3.2 移动 SDK 安全规范检测

3.2.1 程序/代码安全

3.2.1.1 源代码反编译安全（安全）

检测说明：

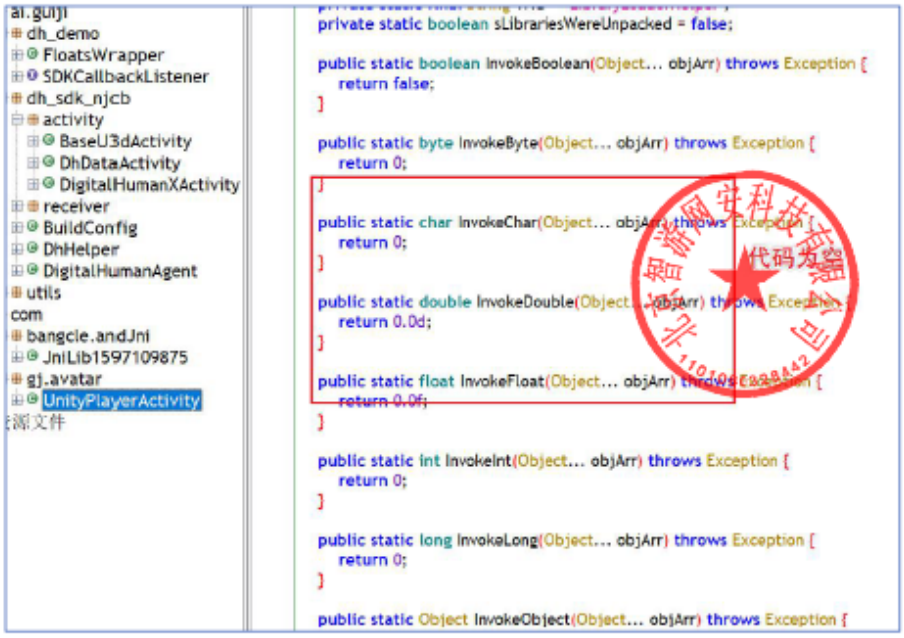
Java 代码加壳即在 Java 代码外面包裹上另外一段代码，保护里面的 Java 代码不被非法修改或反编译。Java 文件未进行加壳保护，可能面临被反编译的风险。攻击者通过反编译工具得到 sdk 的代码，导致代码逻辑泄露、重要数据加密代码逻辑泄露等。

分析方案：

对 SDK 进行反编译，并查看 SDK 关键代码是否做了安全防护。

检测详情：

使用 jd-gui、jadx 对 jar 进行反编译，获取 sdk 的代码，如下



发现 SDK 中的逻辑代码已被掏空处理，此项视为安全。

结果描述：

该 SDK 中的 Java 代码加壳。

测试结果：

安全系数：安全

解决方案:

N/A

3.2.1.2 代码混淆检测（安全）

检测说明:

检测 APK 程序中 Java 代码是否进行过混淆

代码未进行混淆会在代码被反编译后出现核心代码被窃取，逆向代码还原到源工程得风险。

分析方案:

对 SDK 进行反编译，并查看 SDK 关键代码是否做了混淆处理。

检测详情:

经检测，发现 SDK 代码进行安全防护。此项视安全。

结果描述:

代码经过混淆保护

测试结果:

安全系数：安全

解决方案:

N/A

3.2.1.3 SO 保护检测（安全）

检测说明:

检测 APK 程序中的 SO 文件是否进行保护

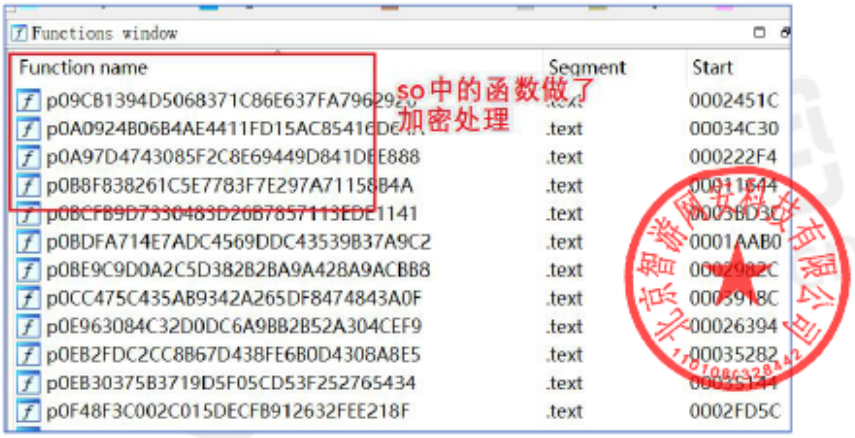
Android SO 通过 C/C++代码来实现，相对于 Java 代码来说其反编译难度要大很多，但对于经验丰富的破解者来说，仍然是很容易的事。应用的关键性功能或算法，都会在 SO 中实现，如果 SO 被逆向，应用的关键性代码和算法都将会暴露。

分析方案：

使用 IDA Pro 反编译 SO 文件，查看 SO 文件是否做了加壳、混淆防护。

检测详情：

使用 IDA 打开 so 文件，在其 Exports 的导出方法里，经检测，此项检测安全：



结果描述：

应用调用的 so 文件，经过混淆防护。

测试结果：

安全系数：安全

解决方案：

N/A

3.2.1.4 H5 代码安全（安全）

检测说明：

随着 html5 的普及，越来越多的轻应用开始使用这种轻巧的方式来开发 Android 客户端，其中不乏涉及到金融、银行等 APP。它的加载方式用两种，一种是加载本地的 html5 网页；一种是网络加载的方式。相比而言，本地加载较危险，特别是未做加密处理的，会有会导致直接泄漏 html5 代码

分析方案：

反编译 sdk，查找是否存在 H5 代码

检测详情：

经过分析未发现 SDK 使用 H5 模块此项视为安全。

结果描述：

未发现应用存在本地 html5 文件

测试结果：

安全系数：安全

解决方案

N/A

3.2.1.5 权限滥用检测（安全）

检测说明：

检测 APK 中是否存在权限滥用风险

权限滥用漏洞一般归类于逻辑问题，是指应用功能开放过多或权限限制不严格，导致攻击者可以通过直接或间接调用的方式达到攻击效果。有些恶意程序可以应用权限对应用造成破

坏，比如利用权限滥用漏洞有时可以使用某些特殊的功能，例如：访问摄像头、利用麦克风录音、编写并植入木马、反弹 shell 等等。

分析方案：

查看配置文件获取 sdk 使用的权限->分析 sdk 需要使用的权限状况

检测详情：

Sdk 申请的权限如下：

高敏感权限：0 项			
中敏感权限：0 项			
低敏感权限：5 项			
1	访问网络	android.permission.INTERNET	低
2	访问网络信息	android.permission.ACCESS_NETWORK_STATE	低
3	写入外部存储	android.permission.WRITE_EXTERNAL_STORAGE	低
	读取外部存储	android.permission. READ _EXTERNAL_STORAGE	低
4	修改音频设置	android.permission. MODIFY_AUDIO_SETTINGS	低
5	录制音频	android.permission.RECORD_AUDIO	低

经分析，sdk 不存在权限滥用情况，此项检测视为安全。

结果描述：

SDK 不存在权限滥用情况。

测试结果：

安全系数：安全

解决方案：

N/A

3.2.1.6 硬编码检测（安全）

检测说明：

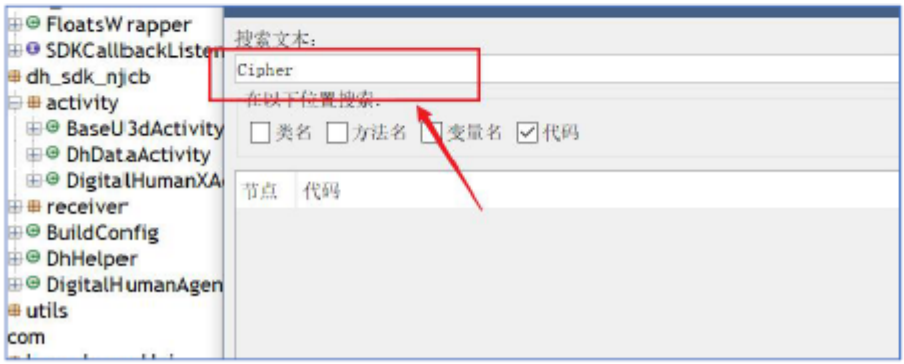
密钥硬编码指在代码中直接将加密算法的密钥设置成固定值，通过反编译，攻击者可以直接查看密钥内容，加密将形同虚设。通常加密算法是公开的，加密数据的保密性依赖密钥。如果密钥泄漏，根据加密算法和加密后的密文，就可以获取加密前的明文。密钥硬编码，将会加密数据处于随时被破解的高危状态，APP 与服务端之间的通信内容随时会被破解，最终导致用户敏感信息泄漏。

分析方案：

使用 android killer 反编译，查看是否存在敏感硬编码的字符串

检测详情：

搜索“Ljavax/crypto/Cipher;->getInstance“字符串查看应用是否存在密钥硬编码风险。



SDK 受到第三方加固保护，此项检测安全。

结果描述：

Sdk 中未发现敏感的硬编码信息。

测试结果：

安全系数：安全

解决方案：

N/A

3.2.2 数据安全

3.2.2.1 敏感信息获取检测（安全）

检测说明：

检测 SDK 是否有获取用户敏感信息的操作

敏感数据包括：用户帐号密码、手机联系人、短信等等。未经用户同意收集用户敏感信息，侵犯用户隐私，会造成极大的影响。

分析方案：

检测 SDK 是否未经用户同意获取用户信息。

检测详情：

SDK 申请的权限有：

序号	权限描述	权限名称	敏感等级
高敏感权限：0 项			

序号	权限描述	权限名称	敏感等级
中敏感权限：0 项			
低敏感权限：4 项			
1	访问网络	android.permission.INTERNET	低
2	访问网络信息	android.permission.ACCESS_NETWORK_STATE	低
3	写入外部存储	android.permission.WRITE_EXTERNAL_STORAGE	低
4	拍照权限	android.permission. CAMERA	低

经过代码扫描，和分析发现应用，未发现收集其他敏感信息。此项视为安全。

结果描述：

SDK 不存在获取用户敏感信息的操作。

测试结果：

安全系数：安全

解决方案：

N/A

3.2.2.2 证书文件明文储存检测（安全）

检测说明：

检测应用资源文件中的证书文件是否为明文存储。

证书文件如果不做密码加密处理，则可以被直接拿出来，进行使用，从而对网络加密传输数据进行解密，有可能会造成用户账号、密码等重要信息泄露。

分析方案：

查看资源是否包含证书文件，证书是否明文储存。

检测详情：

经测试，资源中不包含证书文件。

结果描述：

不存在证书文件明文储存风险。

测试结果：

安全系数：安全

解决方案：

N/A

3.2.3 漏洞检测

3.2.3.1 未移除有风险的 WebView 系统隐藏接口漏洞（安全）

检测说明：

根据 CVE 披露的 WebView 远程代码执行漏洞信息（CVE-2012-663、CVE-2014-7224），Android 系统中存在一共三个有远程代码执行漏洞的隐藏接口。分别是位于 android/webkit/webview 中的“searchBoxJavaBridge”接口、android/webkit/AccessibilityInjector.java 中的“accessibility”接口和“accessibilityTraversal”接口。调用此三个接口的 APP 在开启辅助功能选项中第三方服务的 Android 系统上将面临

分析方案：

搜索代码是否使用 addJavascriptInterface 接口与是否将风险接口移除。

检测详情：

在代码中，搜索“addJavascriptInterface”字符串：

SDK 受到第三方加固保护，此项检测安全。

结果描述：

代码未使用 addJavascriptInterface 接口。

测试结果：

安全系数：安全

解决方案：

N/A

3.2.3.2 WebView 组件忽略 SSL 证书验证错误检测（安全）

检测说明：

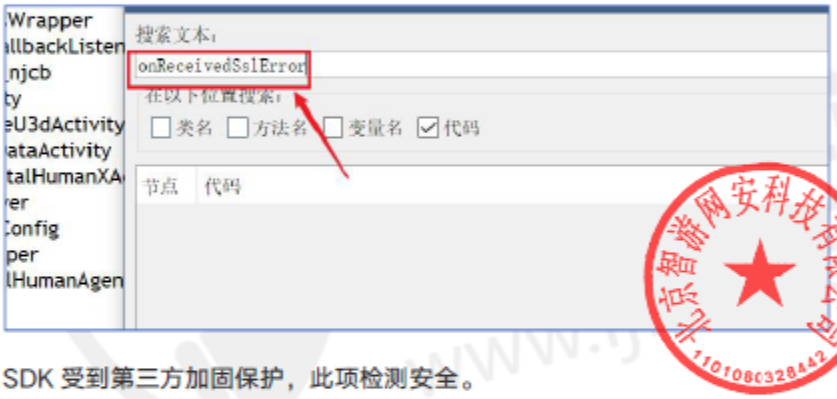
Android WebView 组件加载网页发生证书认证错误时，会调用 WebViewClient 类的 onReceivedSslError 方法，如果该方法实现调用了 handler.proceed()来忽略该证书错误，则会受到中间人攻击的威胁，可能导致隐私泄露。

分析方案：

反编译 sdk->反编译的代码中搜索字符串“onReceivedSslError”

检测详情：

在反编译的代码中搜索字符串“onReceivedSslError”，结果如下：



SDK 受到第三方加固保护，此项检测安全。

结果描述：

SDK 不存在 webview 组件忽略 SSL 证书错误风险。

测试结果：

安全系数：安全

解决方案：

N/A

3.2.4 移动金融规范检测

3.2.4.1 合规检测（安全）

检测说明：

检测目是否符合《R/T 0171—2020 个人金融信息保护技术规范》、《JR/T 0092—2019 移动金融客户端应用软件安全管理规范》、《JR/T 0164—2018 移动金融基于声纹识别的安全应用技术规范》、《JR/T 0199—2020 金融科技创新安全通用规范》等相关标准规范要求进行设计开发并进行安全评估。

分析方案：

使用 SDK 进行业务功能操作，查看相关代码进行分析。

检测详情：

结合以上检测手段和 SDK 功能业务使用过程分析，未发现违规项，此项视为安全。

结果描述：

经检测符合现有相关行业标准要求。

测试结果：

安全系数：安全

解决方案：

N/A

4 深圳爱加密科技有限公司

- **电话：**4000-618-110
- **邮箱：**service@ijiami.cn
- **地址：**北京市海淀区东北旺西路 8 号中关村软件园 10 号楼 2 层 207-2（国永融通大厦）

附件 1-4

基于人工智能技术的 AI 数字员工服务风险补偿机制

本项目按照风险补偿机制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，配套风险拨备资金等补偿措施，切实保障金融消费者合法权益。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。

具体机制如下:

基于人工智能技术的 AI 数字员工服务目前部署在南京银行手机银行客户端，以 3D 拟人数字员工形象，面向手机银行用户提供转账辅助、余额查询、信用卡账单查询、积分查询等基础业务引导、信息预填写、客服答疑、产品咨询等服务，暂不涉及资产管理、资金交易及信贷业务，客户如需办理相关业务，由数字员工提供信息预填写、引导跳转、快捷查询等服务。

基于人工智能技术的 AI 数字员工服务在确保风险可控、监管合规的前提下，采用了语音识别技术、深层神经网络技术、环境降噪技术及智能打断技术等多项技术，同时，基于自然语言处理技术实现客户人机对话场景，并有效地完成语义理解、上下文理解、对话管理和情绪识别，提供了更自然的人机交互过程，改善客户体验。

基于人工智能技术的 AI 数字员工服务在创新过程中已充分考虑消费者权益保护工作相关要求，充分尊重消费者合法权益，

并在执行过程中以消费者权益保护工作为核心，高度重视风险防控工作，主动履行消费者权益保护义务，从源头上预防侵害消费者合法权益事件的发生。

由于本项目暂不涉及资产管理、资金交易或信贷类服务，针对可能存在的金融系统和数据方面的风险隐患，按照申请机构建立的风险补偿机制，可确保因产品或服务的技术缺陷对用户合法权益造成损害时，最大程度降低用户损失。在出现风险时，明确责任认定后，按照相关用户投诉及处理机制向客户做好解释说明和安抚工作，及时引导客户通过柜台等其他渠道办理业务，为客户提供持续、适当的服务，基本满足客户需要和期望。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。

一、针对项目可能存在的风险，做项目风险识别，划分项目风险等级并采取相应的风险措施，从而降低风险、规避风险等，对于那些无法通过风险分散、风险对冲或风险转移的风险进行管理。

二、做好智能服务的监控管理，并建立良好的应急机制，在遭遇不可预知因素发生服务中断时，尽快恢复服务，并在此过程中全力保障客户的合法权益不受侵害。

三、当风险发生时，如因本产品问题造成客户损失时，积极协助客户通过法律途径取得合理补偿，保护客户的合法权益，并最大程度降低客户损失。

四、对产品建立数据应用机制和流程，规范数据获取及数据的使用权限。

附件 1-5

基于人工智能技术的 AI 数字员工服务退出机制

本项目按照退出机制，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

1. 据金融科技创新监管试点情况及监管意见正常退出。

2. 依据法律法规和监管政策要求停止服务。

3. 因特殊情况导致非正常退出时。

4. 其他不可预知风险。

二、退出方案

当触发退出条件时，本项目退出方案包括技术退出和业务退出两部分。

1. 技术退出

南京银行通过回收与本项目相关的系统资源，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，对客户个人信息数据与交易数据进行备份，确保服务退出后，客户不会受到影响。

2. 业务退出

南京银行及时告知客户退出情况，积极配合，保障客户合法权益不受影响，在保障用户资金和信息安全的前提下进行平稳退出。

如遇法律纠纷，依法依规进行仲裁、诉讼。

三、执行部门

南京银行零售基础客户部、数字银行管理部等将根据各自职责开展本项目系统下线工作。

四、数据处理措施

按照《中华人民共和国网络安全法》、《个人金融信息保护技术规范》等要求，金融机构做好数据的归档备份，确保手机银行上其他业务功能不受影响。

五、风险补偿

客户可以通过营业网点、95302 客服热线、门户网站等渠道提出投诉意见和要求。南京银行受理后，由相关部门核实情况，确认责任并联系客户，向客户做好解释说明和安抚工作，及时引导客户通过柜台等其他渠道办理业务，为客户提供持续、适当的服务，基本满足客户需要和期望。

本着依法依规认定，严格审核高效处理的原则，切实保障客户合法权益。如有相关法律纠纷，依法依规进行仲裁、诉讼。

附件 1-6

基于人工智能技术的 AI 数字员工服务应急预案

本项目按照应急处置预案妥善处理突发安全事件，遵循“分级负责、分类处置、快速高效、安全稳妥”的原则，切实保障业务稳定运行和用户合法权益。

1. 突发事件分级：突发事件分为一般风险事件和重大风险事件。一般风险事件是指由于数据存储和传输系统故障，导致系统异常、业务中断的问题。重大风险是指由于系统存在漏洞，导致数据被人窃取盗用的问题。

2. 处置原则：一般风险事件，可以通过数据仓库或者灾备机制恢复数据。重大风险事件必须通过合作协议明确各个合作方之间的权责关系，及相应的违规处理方法，包括终止协议和赔付等。

3. 预防预警与培训演练：在项目上线前进行压力测试和容灾演练，并对相关人员进行培训。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，对异常情况进行告警。一旦发生突发事件，根据其影响范围和危害程度，及时采取有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。

具体应急预案如下：

一、目的和依据

为有效快速、妥善处理基于人工智能技术的AI数字员工服务可能发生的突发事件，按照“分级负责、分类处置、快速高效、安全稳妥”的原则，规范应急处理流程，完善应急体系，构建成熟管理机制，由总行统一领导、相关部门密切配合、各级分支机构协调联动，维护业务服务的正常运行，最大程度避免和减轻突发事件带来的损害，切实保障业务稳定运行和用户合法权益，依据相关规定，制定本应急预案。

二、适用范围

预案适用于由市场因素、产品因素、系统缺陷、网络故障等各种原因所导致的基于人工智能技术的AI数字员工服务产品无法运行或服务的突发事件，需采取的应急处理、操作处置和风险应对操作。

三、突发事件场景

应急预案适用的突发事件场景主要包括:

场景一：网络故障、系统宕机等原因导致基于人工智能技术的AI数字员工服务无法正常运行。

场景二：基于人工智能技术的AI数字员工服务客户端发生故障，导致应用无法启动或正常运行。

场景三：基于人工智能技术的AI数字员工服务可以正常运行，但个别进程出现错误，造成相应的服务无法使用。

四、预案要点

1.建立监测系统，对系统和业务运行情况进行实时监控，及时触发告警并予以系统控制。

2. 建立预警机制，将可能影响的信息纳入预警范围，包括网络异常、应用异常、硬件异常等系统运行异常和自然灾害等其他异常，由系统运维人员负责收集信息，并立即报告相关负责人。

3. 提供 7×24×365 的故障应急反应机制，组建系统保障小组。系统一旦出现中断故障，或影响业务运行的情况，则立即启动故障应急反应程序，系统保障小组立即提供技术支持和技术保障，进行故障诊断和排除。

4. 测试投产前，落实完善服务恢复方案，做好系统压力测试工作，切实做好用户数据保护，全力保障业务连续性。

五、相关组织职责描述

1. 制定机构应急方案责任机制，落实相应责任人，部署、组织各机构和责任人做好应急准备工作，及时报告故障有关情况。

2. 在基于人工智能技术的 AI 数字员工服务出现故障时，协调专业技术人员快速处理故障，尽快恢复业务服务能力。

33FJAE5EUGAO