《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	91310000342052919P-2020-0001	
	创新应用名称	基于多方安全计算的差异化营销平台	
	创新应用类型	科技产品	
	机构信息 1	统一社会信用代码	91310000342052919P
		全球法人识别编码	3003007TBJ3SUR1S6H58
		机构名称	上海冰鉴信息科技有限公司
		持有金融牌照信息	无
	机构信息 2	统一社会信用代码	91310000674637083 2
		全球法人识别编码	300300IM7JD1Y6QFFR87
		机构名称	南京银行股份有限公司上海分行
		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：B0140B231000001 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	2021 年 01 月 29 日	
	技术应用	1.通过多方安全计算技术，在客户授权的前提下，将南京银行上海分行存量客户的权益偏好数据与外部合法合规的支付数据、设备行为数据等进行融合建模，在确保各方原始数据不出域的基础上丰富模型数据源。 2.借助大数据技术，提取有效信息建立营销模型，实现南京银行上海分行存量客户的偏好分析，提升南京银行上海分行差异化营销水平。 3.运用机器学习、决策树等人工智能技术，选取样本、提炼特征变量、精准定位客群特征，降低南京银行上海分行的营销成本，提升营销转化率。 4.基于同态加密、混淆电路等技术，对数据及模型进行加密，以保障数据及模型的传输及使用安全，充分保护客户隐私，提升南京银行上海分行金融服务的安全性。	
	功能服务	本项目综合运用大数据、人工智能、多方安全计算等技术构建差异化营销平台。以差异化营销平台为支撑，通过对南京银行上海分行内存量客户内外部数据的分析评估，细化推演客户的权益偏好，缩小营销产品匹配范围，为不同风格类型的存量客户提供定制化、差异化的营销产品，提升南京银行上海分行营销服务响应率，增强南京银行上海分行金融服务	

		质量及用户粘性。 本项目由上海冰鉴信息科技有限公司负责技术产品研发和技术支持，南京银行股份有限公司上海分行提供金融应用场景并负责平台运维，除此之外，无其他第三方机构参与。
	创新性说明	1.数据保护方面，基于同态加密，混淆电路等技术，实现对数据及模型的加密，营造安全可信任的营销环境，保护消费者个人隐私，提升金融服务的安全性。 2.数据融合方面，运用多方安全计算技术，促进多方数据源的融合应用，打破数据壁垒，充分发挥数据的联动价值。 3.业务效率方面，平台借助人工智能等技术，可以精准推演客户权益偏好，筛选目标客群，有助于更好地降低营销成本，提升营销转化率，增强客户满意度和用户粘性。 4.服务差异化方面，根据模型评估结果对南京银行上海分行客户权益偏好进行分层、分类，对不同类型客户提供差异化营销产品，提升产品匹配度，增强南京银行上海分行存量客户活跃度。
	预期效果	1.通过借助大数据、人工智能等技术，帮助南京银行上海分行为客户提供匹配率更高的金融服务，提升客户对金融服务的获得感和满意度。 2.借助多方安全计算等技术，在原始数据不出域的前提下保障数据融合应用的安全，有效降低客户信息泄露的风险。
	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，预计年营销查询达到5万次。
创新应用服务信息	服务渠道	线上渠道：网上银行、手机银行等
	服务时间	7×24小时
	服务用户	南京银行上海分行的个人用户
	服务协议书	本项目服务协议包括： 1.《委托贷款抵押合同》（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上海分行
	评估时间	2020年11月25日
	有效期限	1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》、《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）等相

		关国家法律法规及金融行业相关政策文件要求进行设计，在客户信息不被公开、被查询客户主体不被识别的基础上，通过安全模型实现客户营销意向性的分析匹配，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。		
	评估材料	《合法合规性评估报告-基于多方安全计算的差异化营销平台》（见附件 1-2）		
技术安全性评估	评估机构	中国金融电子化公司测评中心		
	评估时间	2021 年 3 月 22 日		
	有效期限	1 年		
	评估结论	本项目符合《个人金融信息保护技术规范》（JR/T 0171—2020）、《网上银行系统信息安全通用规范》（JR/T 0068—2020）、《移动金融客户端应用软件安全管理规范》（JR/T 0092—2019）、《多方安全计算金融应用技术规范》（JR/T 0196—2020）、《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。 后续，将在自声明前提交由外部权威专业机构出具的《金融科技创新安全通用规范》（JR/T 0199—2020）标准符合性证明材料。		
	评估材料	《技术安全性评估报告-基于多方安全计算的差异化营销平台》（见附件 1-3）		
风险防控	风控措施	1	风险点	由于人工智能模型存在算法不确定性而导致预测偏差，造成预测结果准确性问题。
			防范措施	针对准确性风险，构建全流程模型管理体系，及时跟进调整模型算法与技术，迭代优化；建立健全营销内容审核、客户投诉处置等全流程人工干预机制，审核确认营销权益产品内容，根据客户反馈情况人工调整客户营销偏好结果。
		2	风险点	应用过程中可能存在数据泄露、滥用等数据安全风险。
			防范措施	在数据使用上，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。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，通过加密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，明示并获取用户同意后，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。
		3	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	本项目按照由申请各方联合制定的风险补偿方案（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。 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	本项目按照由申请各方联合制定的退出机制（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	本项目按照由申请各方联合制定的应急处置预案（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	南京银行上海分行 客服电话：95302 投诉网站：http://www.njcb.com.cn
		投诉受理与处理机制	南京银行上海分行受理后，由牵头业务部门指派相关人员核实情况，沟通、处理相关意见并及时与投诉人反馈，项目团队也将及时跟进、处理相关问题。
	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。 我机构承诺本产品符合《金融科技创新安全通用规范》（JR/T 0199—2020），将在自声明前提交由外部权威专业机构出具的标准符合性证明材料。 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）

3AUVI6GCPTZ4

3AUVI6GCPTZ4

附件 1-1

基于多方安全计算的差异化营销平台服务协议书

本项目服务协议书包括《委托贷款抵押合同》（附件 1-1-1）、《南京银行 APP 用户隐私政策》（附件 1-1-2）。

附件 1-1-1

南京银行 BANK OF NANJING

重要提示

根据中国银行保险业监督管理委员会以及本行有关规定，本行严禁员工发生下列行为：

1、向客户借款；

2、为民间借贷提供担保、鉴证或牵线搭桥；

3、在企业兼职；

4、借用客户账户过渡资金，或利用本人账户为客户过渡资金；

5、代客户保管卡、折、密码及重要凭证等；

6、违规向客户收费、强制捆绑或不当搭售；

7、接受或索取不当利益等。

为保障客户权益，本行郑重提示如下：

以上事项均为本行所明令禁止，任何人员无论以何种原因从事上述行为，均为其个人行为，不代表本行意志，请务必谨慎。

同时，南京银行敦请客户对本行员工予以监督，如发现本行员工存在上述情形，请通过专用邮箱 cxjb@njcb.com.cn 或致电（电话：025－86775624）予以举报，本行将严格保密。

Ea16 委托贷款抵押合同

编号：[合同编号]

抵押权人（甲方）：南京银行股份有限公司[　　]

抵押人（乙方）：[　　]

鉴于：

一、 甲方作为委托贷款受托人、[　　]作为委托贷款委托人（以下称“委托人”）、[　　]作为借款人（以下简称“债务人”）签订了编号为[　　]的《委托贷款借款合同》(以下简称“主合同”)，约定委托人提供资金，由受托人向委托人指定的借款人代为发放借款。

二、甲方与委托人、乙方签订了编号为[　　]的《委托贷款委托抵押协议》(以下简称“委托抵押协议”)，约定委托人委托甲方作为其代理人以甲方名义与乙方签订《委托贷款抵押合同》并办理抵押登记手续。

三、乙方愿意为主合同项下债权提供抵押担保。

根据有关法律、法规、规章，甲、乙双方经协商一致，特订立本合同，以期共同遵照执行。

第一条　乙方保证及声明

一、乙方在本合同项下的承诺，在任何时候、任何情形下均构成其直接的、无条件的和对其有效和有约束力的承诺。

二、乙方承诺恪守诚实守信原则，向甲方提供的各项资料和信息是真实、合法、完整、有效的，不含有任何与事实不符的错误、遗漏、隐瞒或误导性陈述。

三、乙方是本合同项下抵押物的完全的、有效的、合法的所有者或有权处分者，该抵押物不存在所有权、处分权或使用权的争议。

四、乙方完全了解主合同债务人的债务用途及债务履行期限，为主合同债务人提供抵押担保完全出于自愿。

五、本合同项下的抵押物依法可以设定抵押担保，未发生被查封、扣押、监管或被采取其他强制措施等情形，且未被列入征用、拆迁范围。

六、本合同项下的抵押物如已部分或全部出租，乙方保证将设立抵押事宜告知承租人，并将有关出租情况书面告知甲方，且已经甲方认可并书面签收。

七、乙方承诺发生影响乙方承担担保责任的不利事项时应及时书面通知甲方。

八、乙方若为自然人，则乙方确认并保证，在以其财产设定本合同项下抵押担保之前，已对其本人及其家属的生活必需物资作出了妥善的安排，甲方处置本合同项下抵押物受偿债权不会对乙方及其家属的正常生活造成任何影响。

第二条　主债权

本合同项下被担保的主债权为依据主合同由甲方向债务人发放委托贷款而形成的[　　]（全部/部分）债权本金，即[　　]（币种）（大写）[　　]（小写）[　　]元，债务人债务履行期限以主合同及主合同有效附件约定的或载明的期限为准。

若乙方提供部分担保，只要甲方仍有未获受偿债权，则乙方均有义务在担保范围内承担担保责任。

第三条　抵押物

抵押物详见《抵押物清单》（附后）。乙方以《抵押物清单》所列之财产设定抵押担保。甲、乙双方确认，《抵押物清单》对抵押物价值的约定，并不作为甲方依本合同约定对抵押物进行处分的估价依据，也不构成甲方行使抵押权的任何限制。

甲、乙双方确认：抵押物孳息也属于抵押物，受本合同约束，甲方有权对抵押物孳息主张抵押权优先受偿。

第四条　抵押担保范围

乙方抵押担保范围为主债权及利息（包括复利和罚息，下同）、违约金、损害赔偿金以及甲方实现债权和抵押权的有关费用（包括但不限于诉讼费、仲裁费、财产保全费、差旅费、执行费、律师代理费、公证费、评估费、拍卖费等，下同）。

乙方确认并自愿接受，当债务人未按主合同约定履行其债务时，无论甲方对主合同项下的债权是否拥有其他担保（包括但不限于物权担保），甲方均有权直接要求乙方在其担保范围内承担担保责任。

第五条　被担保的主合同的变更

乙方确认，除增加债权本金金额或延长债务履行期限外，甲方与债务人协议变更主合同条款的，均视为已征得乙方事先同意，无须通知乙方，乙方担保责任不因此而减免。

甲方与债务人依主合同约定变更利率的，亦视为已征得乙方事先同意，甲方无须通知乙方，乙方仍应承担担保责任。

第六条　合同效力的独立性

本合同的效力独立于主合同，主合同全部或部分无效或可撤销或解除并不影响本合同的效力。如主合同被确认为无效或被撤销或解除，则乙方对于债务人因返还财产或赔偿损失等而形成的债务也承担抵押担保责任。

乙方在本合同项下的担保责任不因债务人合并、分立、股权变动，或丧失民事行为能力、失踪、死亡或被宣告失踪、死亡，或其他任何原因而有所改变。

第七条　抵押物和抵押物权属凭证的占管

抵押权存续期间，抵押物由乙方占管。乙方应妥善保管抵押物，负有维修、保养、保持抵押物完好无损的责任，并随时接受甲方的检查。

抵押权存续期间，若抵押物发生毁损、灭失或其他使抵押物价值减少的情形时，乙方应及时通知甲方，并在 10 日内恢复抵押物价值或向甲方提供为甲方所认可的其他担保。因恢复抵押物价值或设定新增担保支出的费用，概由乙方承担。

抵押权存续期间，抵押物他项权证由甲方占管。

第八条　抵押物登记

本合同项下抵押物均须办理抵押物登记，乙方应积极协助甲方自本合同签订之日起 3 日内，持本合同及有关资料到相应登记机关办理抵押物登记。

第九条　抵押物的保险

根据法律、法规、规章有关规定，经甲、乙双方协商，由乙方自主选择保险公司办理本合同项下抵押物的财产保险，保险单正本由甲方占管，保险单注明甲方为抵押物保险的第一受益人。若法律、法规、规章规定发生变化，抵押物保险按最新规定执行。

第十条　第三人损害赔偿

若因第三人的行为导致抵押物价值减少的，损害赔偿金应存入甲方指定的帐户。对上述损害赔偿金，乙方同意甲方有权选择下列方式进行处理，并协助办理有关手续：

（一）清偿或提前清偿主合同项下全部或部分债务；

（二）转为定期存款，存单用于主合同项下债务的质押担保，并与甲方签订相应质押合同；

（三）转为保证金，用于主合同项下债务的质押担保，并与甲方签订相应保证金协议；

（四）经甲方书面同意，用于修复抵押物，以恢复抵押物价值；

（五）乙方提供符合甲方要求的新的担保后，可将损害赔偿金自由处分。

若因第三人的行为导致抵押物价值不足以清偿主合同项下全部债务的，乙方应重新提供甲方认可的担保，抵押物价值未减少的部分，仍作为债权的担保。

第十一条　抵押物的处分

未经甲方书面同意，乙方不得赠与、转让、交换、出租、重复抵押、迁移或以其他方式处分本合同项下的抵押物，否则，处分行为无效。

经甲方书面同意乙方处分本合同项下抵押物的，处分抵押物所得款项应存入甲方指定账户。对上述所得款项，乙方同意甲方有权选择下列方式进行处理，并协助办理有关手续：

（一）清偿或提前清偿主合同项下债务本息及相关费用；

（二）转为定期存款，存单用于主合同项下债务的质押担保，并与甲方签订相应质押合同；

（三）转为保证金，用于主合同项下债务的质押担保，并与甲方签订相应保证金协议；

（四）乙方提供符合甲方要求的新的担保后，可将处分抵押物所得款项自由处分。

因国家建设需要征用、拆迁本合同项下的抵押物时，乙方所获补偿金按前款约定处理。

第十二条　乙方的权利和义务

一、在抵押权受到或可能受到来自任何第三方的侵害时，乙方有义务通知甲方并采取必要措施使抵押权免受侵害。

二、主合同项下债务若为外币债务，则乙方应以主合同约定的币种承担担保责任。若以其它可自由兑换的外币或人民币承担担保责任，应征得甲方同意，并按履行担保责任之日南京银行股份有限公司外汇买卖牌价汇卖价折成主合同约定的币种承担担保责任。

三、乙方应履行以下通知义务：

（一）乙方应在下列事项发生或可能发生之日起 3 日内书面通知甲方：

1、乙方经营财务状况恶化，影响或可能影响其债务偿还能力；

2、乙方卷入或可能卷入诉讼或仲裁程序及其他法律纠纷等；

3、乙方名称、法定代表人（或负责人）、住所、联系电话等发生变更；

4、乙方发生导致乙方丧失或可能丧失担保能力，或对其承担担保责任产生影响的其他事项。

（二）乙方应在下列事项发生或可能发生前 30 日以书面形式通知甲方：

1、乙方分立、转制、合并、终止、合资等；

2、乙方经营范围及注册资本变更；

3、乙方出资额或持股额前五名股东发生变化。

乙方如发生上述事项，影响或可能影响乙方承担担保责任的，乙方应按甲方要求另行提供为甲方所认可的其他担保。

四、乙方如为自然人，除应遵循本合同各项约定外，还应在下列事项发生或可能发生之日起 3 日内以书面形式通知甲方：

（一）乙方个人或其家庭发生变故或收入发生变化，导致其经济状况恶化，影响或可能影响其担保能力的；

（二）乙方工作单位发生变更；

（三）乙方发生失业、离婚、重大疾病等事项；

（四）乙方发生导致乙方丧失或可能丧失担保能力，或对其承担担保责任产生影响的其他事

项。

乙方如发生上述事项，影响或可能影响乙方承担担保责任的，乙方应按甲方要求另行提供为甲方所认可的其他担保。

五、乙方不得以与任何第三方纠纷为理由拒绝履行本合同项下义务。

六、根据法律、法规、规章等规定及本合同约定享有和承担的其他权利与义务。

第十三条　甲方的权利和义务

一、甲方有权要求乙方对甲方未受偿的债权承担本合同项下抵押担保责任，并有权依法处分抵押物。

二、甲方实现抵押权后，应乙方请求，甲方可以向乙方提供其已履行担保责任的有关证明资料，但乙方为债务人的除外。

三、根据法律、法规、规章等规定及本合同约定享有和承担的其他权利与义务。

第十四条　违约及处理

一、以下任一情形发生，对本合同的履行产生重大影响的，均构成违约事件：

（一）乙方或债务人违反本合同或主合同所作的任何声明、保证和承诺，或债务人发生其他违约行为；

（二）乙方或债务人提供无真实贸易、交易背景等虚假材料或隐瞒经营财务事实；

（三）债务人未经甲方同意擅自改变资金用途，挪用资金或用资金从事非法、违规交易；

（四）乙方或债务人出现不良信用记录或其他违约行为；

（五）乙方或债务人通过关联交易或其他方式逃废债务；

（六）乙方或债务人利用与任何第三人之间的虚假合同或安排，包括但不限于以无真实贸易背景的应收票据、应收账款等到银行贴现或质押，套取甲方或其他银行的资金或授信；

（七）乙方、债务人或其关联方未履行与甲方或南京银行股份有限公司各级机构或任何其他第三方债务；

（八）乙方违反法律、法规、规章等规定或本合同的约定，或本合同未生效、无效、被撤销，或乙方经营状况发生不利于甲方债权的变化，或乙方拒绝履行其担保义务；

（九）乙方未按本合同约定办妥抵押物登记手续，或抵押物发生价值减少、毁损或灭失，物理形态发生变化，权属发生争议或遭查封、扣押、留置、拍卖等强制措施，或抵押物被列入征收、征用、拆迁范围等情形；

（十）乙方、债务人或其关联方或其法定代表人、管理层、实际控制人转移资产，甲方认为影响其债权的安全；

（十一）乙方、债务人或其关联方或其法定代表人、管理层、实际控制人发生或涉入或可能涉入诉讼或仲裁案件，或被行政机关、执法机关、司法机关施以或可能施以任何形式的处罚或强制措施；

（十二）乙方或债务人发生停业整顿、解散、破产等事件或出现不利于乙方或债务人的负面讯息；

（十三）乙方或债务人法定代表人或实际控制人无法联系或约见；

（十四）本合同项下任一通知事项实际发生，甲方认为将影响其债权的安全；

（十五）因国家信贷政策、市场环境等发生不利于甲方债权的变化，可能影响甲方债权安全；

（十六）其他违反法律、法规、规章等规定或本协议约定的其他事项。

二、发生以上违约事件之一的，甲方有权行使下述一项或几项权利：

（一）要求乙方或债务人限期纠正违约行为；

（二）要求乙方立即按所有已发放融资金额的100%缴纳/补足保证金；

（三）要求乙方另行提供为甲方所认可的担保；

（四）宣布主合同项下债权提前到期并收回主合同项下债权或解除主合同，依法立即处分抵押物并从所得价款中优先受偿；

（五）要求乙方承担违约责任，并赔偿甲方因此而遭受的任何损失和产生的任何费用和开支（包括但不限于律师费、诉讼费、仲裁费、鉴定费、财产保全费、执行费、公证费、评估费、拍卖费等）；

（六）就本合同项下抵押物采取保全措施；

（七）行使法律、法规、规章规定及本合同约定可以行使的其他权利。

第十五条　法律适用及争议处理

一、本合同按中华人民共和国法律订立，适用中华人民共和国法律。

二、本合同在履行过程中发生争议，可以通过协商解决；协商不成，可按以下第[　　]种方式解决：

（壹）向甲方住所地人民法院起诉。

（贰）提交[　　]仲裁委员会（仲裁地点为[　　]），按照申请仲裁时该会现行有效的仲裁规则进行仲裁。仲裁裁决是终局的，对双方均有约束力。

三、合同双方对诉讼管辖另有约定的，在本合同第十七条“其他约定事项”中另行约定。

在诉讼或仲裁期间，本合同不涉及争议部分的条款仍须履行。

第十六条　合同的生效、变更和解除

一、甲、乙双方自愿协商确认，本合同同时满足以下条件后生效：

乙方为法人或其他组织的，本合同经甲方法定代表人（负责人）或授权代理人签名或加盖名章并加盖单位公章或合同专用章及乙方法定代表人或授权代理人签名或加盖名章并加盖单位公章或合同专用章；乙方为自然人的，本合同经甲方法定代表人（负责人）或授权代理人签名或加盖名章并加盖单位公章或合同专用章及乙方或授权代理人签名。

二、本合同生效后，除非本合同另有约定，甲、乙任何一方不得擅自变更和解除本合同；确需变更或解除的，应经双方协商一致，并达成书面协议。书面协议达成之前，本合同条款仍然有效。

第十七条　其他约定事项

一、乙方已充分认识到利率风险，如主合同采用浮动利率，乙方自愿承担因利率浮动而增加的担保责任。

二、乙方未履行本合同项下义务时，自愿依法接受强制执行。

三、本合同项下的所有附件以及履行合同有关的法律文书等均为合同的组成部分，与合同正本具有同等的法律效力。

四、若双方于本合同中载明相应的地址，则该地址为双方通讯及联系地址，该通讯及联系地址系银行和法院送达任何书面通知或各类法律文件的指定地址。如乙方通讯及联系地址发生变更时，乙方应及时书面通知甲方，并在甲方书面确认获悉后，对双方发生约束力。

五、[_____]。

第十八条　附则

一、本合同壹式[__]份，甲方执[__]份，乙方执[__]份，抵押物登记部门执[__]份，每份均具有同等法律效力。

二、本合同未尽事宜，按照国家有关法律、法规、规章办理。

第十九条　声明条款

一、甲、乙方签订和履行本合同已得到法律或其公司章程规定的有权决策者或上级部门等有权机构的批准，并已取得必要的、充分的、合法的授权。

二、甲、乙方签订本合同是其真实意思的表示，甲、乙方的签章是真实的，签约代表是经过授权的，本合同对甲、乙方具有法律约束力。

三、乙方有权充分拥有其全部资产，并且向甲方提供的各项资料是真实、合法、有效的，不含有与事实不符的任何错误或遗漏任何事实。

四、乙方已阅读合同首页“重要提示”所有内容，理解并接受甲方提示的风险，愿意积极协助甲方对甲方员工行为予以监督。乙方承诺不与甲方员工个人之间发生资金往来、账户借用等任何不当利益关系，并自愿接受甲方监督。乙方若违反上述承诺，甲方有权追究乙方责任。

五、乙方已阅读本合同所有条款。应乙方要求，甲方已经就本合同做了相应的条款说明。乙方对本合同条款的含义及相应的法律后果已全部知晓并充分理解。

六、甲方系依法设立的银行机构，有资格经营本合同项下业务。

附：抵押物清单

房产抵押					
坐落	[ ]				
丘号	[ ]	抵押面积（m²）	[ ]	所有权证号/不动产登记证号	[ ]
用途	[ ]	是否成套	[ ]	土地使用权证号	[ ]
评估价值(元)	[ ]			协议价值（元）	[ ]
其他	[ ]				
坐落	[ ]				
丘号	[ ]	抵押面积（m²）	[ ]	所有权证号/不动产登记证号	[ ]
用途	[ ]	是否成套	[ ]	土地使用权证号	[ ]
评估价值(元)	[ ]			协议价值（元）	[ ]
其他	[ ]				
坐落	[ ]				
丘号	[ ]	抵押面积（m²）	[ ]	所有权证号/不动产登记证号	[ ]
用途	[ ]	是否成套	[ ]	土地使用权证号	[ ]
评估价值(元)	[ ]			协议价值（元）	[ ]
其他	[ ]				
坐落	[ ]				
丘号	[ ]	抵押面积（m²）	[ ]	所有权证号/不动产登记证号	[ ]
用途	[ ]	是否成套	[ ]	土地使用权证号	[ ]
评估价值(元)	[ ]			协议价值（元）	[ ]
其他	[ ]				

土地使用权抵押					
坐落	[ ]				
地号	[ ]	图号	[ ]	抵押面积（㎡）	[ ]
使用权证号	[ ]	使用权类型	[ ]	评估价值（元）	[ ]
坐落	[ ]				
地号	[ ]	图号	[ ]	抵押面积（㎡）	[ ]
使用权证号	[ ]	使用权类型	[ ]	评估价值（元）	[ ]
坐落	[ ]				
地号	[ ]	图号	[ ]	抵押面积（㎡）	[ ]
使用权证号	[ ]	使用权类型	[ ]	评估价值（元）	[ ]
坐落	[ ]				
地号	[ ]	图号	[ ]	抵押面积（㎡）	[ ]
使用权证号	[ ]	使用权类型	[ ]	评估价值（元）	[ ]
坐落	[ ]				
地号	[ ]	图号	[ ]	抵押面积（㎡）	[ ]
使用权证号	[ ]	使用权类型	[ ]	评估价值（元）	[ ]

其　　他			
名称	[ ]	处所（籍属）	[ ]
数量或面积	[ ]	使用期限	[ ]
评估价值（元）	[ ]	权属证明编号	[ ]
其他	[ ]		
名称	[ ]	处所（籍属）	[ ]
数量或面积	[ ]	使用期限	[ ]
评估价值（元）	[ ]	权属证明编号	[ ]
其他	[ ]		

(签署页)

甲方	
公章	法定代表人（负责人）（签章）： （或授权代理人）： 地址： 邮政编码： 联系电话： 签约日期：　　年　　月　　日
乙方为法人或其他组织	
公章	法定代表人（签章）： （或授权代理人）： 地址： 邮政编码： 联系电话： 签约日期：　　年　　月　　日
乙方为自然人	
签名 （或授权代理人）：	身份证件名称： 身份证件号码： 地址： 邮政编码： 联系电话： 签约日期：　　年　　月　　日

附件 1-1

南京银行 APP 用户隐私政策

3AUVI6GCPTZ4

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

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。

a. 如果我们违反法律法规规定，收集、使用您的个人信息；

b. 如果我们违反了与您的约定，收集、使用您的个人信息；

c. 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；

d. 如果我们不再为您提供产品或服务；

e. 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

您可以通过以下四种方式注销南京银行手机银行：

（1）登录南京银行手机银行，点击“我的-设置-注销手机银行”，根据提示进行操作，即可注销南京银行手机银行。

（2）登录专业版个人网银，点击“自助开通-手机银行-关闭”，输入短信验证码/UK 密码以及账户交易密码，即可注销南京银行手机银行。

（3）使用手机银行预留手机号编辑短信“03SJYHJY”发送至 95302，即可注销南京银行手机银行。

（4）至南京银行任意网点办理注销手机银行。

您注销南京银行 APP 的行为是不可逆行为，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：1.0

协议发布时间：2019 年 10 月 21 日

协议更新时间：2020 年 7 月 31 日

协议生效时间：2020 年 7 月 31 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	NJVideoChatvidyo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	华为技术有限公司
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

附件 1-2

基于多方安全计算的差异化营销平台
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》、《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）等相关国家法律法规及金融行业相关政策文件要求进行设计，在客户信息不被公开、被查询客户主体不被识别的基础上，通过安全模型实现客户营销意向性的分析匹配，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。

南京银行股份有限公司上海分行

2020 年 11 月 25 日

附件 1-3　　报告编号： SHBJGS-安全评估报告-20210322

上海冰鉴信息科技有限公司
基于多方安全计算的差异化营销平台
技术性安全评估报告

产品名称（版本号）	基于多方安全计算的差异化营销平台（V1.0.0）
委托单位	上海冰鉴信息科技有限公司
测评单位	中国金融电子化公司测评中心
报告时间	2021-03-22
有效期至	2022-03-21

中国金融电子化公司测评中心

报告编号： SHBJGS-安全评估报告-20210322

上海冰鉴信息科技有限公司
基于多方安全计算的差异化营销平台
技术性安全评估报告

委托单位	上海冰鉴信息科技有限公司
产品名称（版本号）	基于多方安全计算的差异化营销平台（V1.0.0）
检测类别	委托检测
审核人	
批准人	
报告时间	2021-03-22

中国金融电子化公司测评中心

评 估 报 告 声 明

1. 评估报告经签字、盖章后有效。
2. 本评估报告仅适用于本报告明确指出的委托单位被测样品。
3. 未经本机构书面批准，不得复制本报告中的内容（全文复制除外），以免本报告的使用者对被测样品做出不全面的评价。
4. 在任何情况下，若需引用本报告中的结果或数据都应保持其本来的意义，不得擅自增加、修改、伪造或掩盖本报告的原有内容。
5. 本报告不得复制作为广告材料使用。
6. 当被测样品版本变更或其它任何改变时，本报告检测结果不再适用，涉及到的任何技术、模块或子系统、甚至整个系统都必须按监管机构的要求进行必要的备案或重新检测。不得将本报告检测结果应用于其他版本的被测样品。
7. 本报告的检测结果描述反映的是截至 2021 年 03 月 22 日的情况。由于这些内容在将来可能发生变化或不再适用，任何基于这些信息作出的判断和分析都有可能面临风险。
8. 本报告检测结果的有效性建立在委托单位提供相关信息的真实性基础之上。对于由于委托单位提供不实信息而导致检测结果出现错误的情况，本机构不予负责。
9. 如对本报告的检测结果有异议，请于收到评估报告后 15 日内与本机构联系。
10. 本机构根据特定技术标准出具检测结果为“符合”的检测项仅表明被测样品的业务项符合了相应标准的要求，并不保证该被测样品或者该项业务是绝对安全的。

联系单位：中国金融电子化公司

地　　址：北京市大兴区西红门镇中国人民银行软件开发中心

联 系 人： 刘强

Email　liuqiang@icfcc.com

联系方式：18612321761

目　录

技术性安全评估结论

产品名称	基于多方安全计算的差异化营销平台
产品简介	上海冰鉴信息科技有限公司“基于多方安全计算的差异化营销平台”创新应用，综合使用了大数据、人工智能、多方安全计算等技术，构建差异化营销平台。以差异化营销平台为支撑，通过对南京银行上海分行内存量客户内外部数据的分析评估，细化推演客户的权益偏好，缩小营销产品匹配范围，为不同风格类型的存量客户提供定制化、差异化的营销产品，提升南京银行上海分行营销服务响应率，增强南京银行上海分行金融服务质量及用户粘性。
评估过程简介	中国金融电子化公司测评中心于 2021 年 2 月 22 日至 2021 年 3 月 19 日对基于多方安全计算的差异化营销平台开展了技术性安全评估工作。评估的过程包括评估准备、方案编制、现场评估及分析与报告编制。评估的范围包括交易安全、服务质量、业务连续性、算法安全、数据安全、网络安全、内控管理等七方面内容。
评估结论	**基本符合**

总体评价

中国金融电子化公司测评中心依据 JR/T 0199-2020《金融科技创新安全通用规范》对上海冰鉴信息科技有限公司送检的基于多方安全计算的差异化营销平台进行技术性安全评估，总体情况如下：

交易安全方面，基于多方安全计算的差异化营销平台主要业务功能是通过对南京银行上海分行内存量客户内外部数据的分析评估，细化推演客户的权益偏好，缩小营销产品匹配范围，为不同风格类型的存量客户提供定制化、差异化的营销产品，该平台不涉及资金交易，故交易安全检测项不适用。

服务质量方面，上海冰鉴信息科技有限公司制定了服务质量相关的管理要求，且内部对系统进行了丰富的性能测试，确保系统能够满足服务质量目标。

业务连续性方面，上海冰鉴信息科技有限公司制定了《冰鉴科技-业务连续性管理办法》、《冰鉴科技-备份恢复管理制度》、《冰鉴科技-数据安全应急演练方案》，明确了应急处理流程、业务运营中断事件响应策略、安全事件处理及监管管理要求。基于多方安全计算的差异化营销平台部署在阿里云上，阿里云公共云平台已通过网络安全等级保护三级测评， 基础设施安全由阿里云提供保障。

算法安全方面，业务场景采用了逻辑回归和 GBDT 两种模型，前者的目标函数是平均对数似然损失，后者分情况提供了对数损失、指数损失函数；算法目标函数本身运算复杂度低，同时对不同算法采用了不同的策略来降低运算成本；使用了大量的密文交互，包括秘密分享、混淆电路、同态加密等算法来保证数据训练以及模型传输、存储的安全管理。

数据安全方面，上海冰鉴信息科技有限公司制定了《冰鉴科技-数据管理办法》，明确了数据的分类、质量管理要求以及数据质量管理部门和机制；基于多方安全计算的差异化营销平台不涉及个人金融信息的收集，平台使用 HTTPS 加密协议进行加密传输，采用基于同态加密、混淆电路等技术，实现对数据及模型的加密处理；申请机构开发测试环境与生产环境进行了有效隔离，对个人金融信息进行了有效保护。存在不足之处在于基于多方安全计算的差异化营销平台操作人员用户手机号未屏蔽显示，平台暂未提供日志管理功能。

网络安全方面，基于多方安全计算的差异化营销平台不涉及 APP 客户端，因此部分仿冒钓鱼检查项不适用；上海冰鉴信息科技有限公司对基于多方安全计算的差异化营销平台进行了技术选型评估、源码审计、漏洞扫描测试等，及时进行漏洞修复，并提供了《冰鉴科技-技术选型报告》、《冰鉴科技-系统源代码安全审计报告》、《华为云漏洞扫描服务安全报告》；定期对信息安全事件进行分析，并对自身的控制措施进行安全评估、整改。存在不足之处在于目前仅有阿里云公共云平台的等级保护测评报告，暂未开展基于多方安全计算的差异化营销平台的等级保护测评和渗透测试。

内控管理方面，上海冰鉴信息科技有限公司提供了《冰鉴科技-技术选型报告》、《金融科技创新应用声明书》、《基于多方安全计算的差异化营销平台风险补偿机制》、《基于多方安全计算的差异化营销平台退出机制》、《基于多方安全计算的差异化营销平台应急预案》，对金融科技应用的必要性、可行性、战略规划、风险防范、运营策略、内部审计和外部评估等内容进行了规范化管理。申请机构制定了《金融科技创新应用管理制度及工作组织机制》，制度对金融科技应用创新、实施、管理过程进行了描述，但暂未制定定期进行评估事项以及未指定牵头负责部门、未建立工作协调机制、联合运营机制、问题协同处理机制等控制措施。

本次技术性安全评估共检测 161 个检测项，判定结果为“符合”的有 110 项，判定结果为“部分符合”的有 5 项，判定结果为“不符合”的有 2 项，判定结果为“不适用”的有 44 项。从本次技术性安全评估的结果看，系统还存在一些可进一步完善的方面，现对委托方上海冰鉴信息科技有限公司送检的基于多方安全计算的差异化营销平台提出如下建议：

申请机构目前仅有阿里云公共云和同环境个人反欺诈评估服务系统的等级保护测评报告，应对基于多方安全计算的差异化营销平台开展专门的等级保护测评工作；应定期对应用系统和应用程序接口进行漏洞扫描和渗透测试，并形成完善的测试报告和整改记录；应定期对金融科技创新应用的管理制度和业务流程进行评估。

综合上述评价结果，上海冰鉴信息科技有限公司基于多方安全计算的差异化营销平台已具备了基本的安全保护措施，但在数据安全、网络安全、内控管理方面仍存在一些问题。结合风险评价与风险对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益造成的危害情况，上海冰鉴信息科技有限公司基于多方安全计算的差异化营销平台在本次技术性安全评估结果中存在不符合项和部分符合项，但不会导致该产品

面临高等级的安全风险，因此对该产品的基本安全状态进行综合判断，得出技术性安全评估的结论为基本符合。

综合判定：基于多方安全计算的差异化营销平台基本符合 JR/T 0199-2020《金融科技创新安全通用规范》的要求。

1. 概述

1.1 检测目标

本次检测目标是在基于多方安全计算的差异化营销平台版本确定的基础上，对基于多方安全计算的差异化营销平台的交易安全、服务质量、业务连续性、算法安全、数据安全、网络安全、内控管理等七个方面的内容进行安全检测，客观、公正评估基于多方安全计算的差异化营销平台技术标准符合性和安全性，保障基于多方安全计算的差异化营销平台的安全稳定运行。

1.2 检测依据和标准

JR/T 0199-2020《金融科技创新安全通用规范》

1.3 被测软件概述

上海冰鉴信息科技有限公司“基于多方安全计算的差异化营销平台”创新应用，综合使用了大数据、人工智能、多方安全计算等技术，构建差异化营销平台。以差异化营销平台为支撑，通过对南京银行上海分行内存量客户内外部数据的分析评估，细化推演客户的权益偏好，缩小营销产品匹配范围，为不同风格类型的存量客户提供定制化、差异化的营销产品，提升南京银行上海分行营销服务响应率，增强南京银行上海分行金融服务质量及用户粘性。

2. 评估环境

2.1 硬件/软件环境

序号	IP 地址	设备用途	操作系统版本	中间件	物理位置
1	10.30.7.11	应用服务器（生产中心）	CentOS Linux release 7.7.1908 (Core)	MySQL-5.7.30 Redis-4.0 docker-ce-19.03.4-3	浙江省杭州市萧山区
2	10.30.8.11	应用服务器（生产中心）	CentOS Linux release 7.7.1908 (Core)	MySQL-5.7.30 Redis-4.0 docker-ce-19.03.4-3	浙江省杭州市萧山区

2.2 检测工具

序号	检测工具名称及版本	检测工具应用说明
1	BurpSUite Professional	数据抓包分析
2	天镜漏洞扫描 V6.0	漏洞扫描

3. 评估方法

本次现场检测工作采用访谈、检查、测试等方法。

其中访谈是检测人员通过与被测系统有关人员进行交流、讨论等活动以获取证据的一种方法；访谈使用到的工具主要是访谈列表。检测人员针对访谈列表上的问题，逐项与客户端软件有关人员进行交流、讨论，根据被访谈人员的回答了解和确认客户端软件的安全保护情况；

检查是检测人员通过对检测对象进行观察、查验、分析等活动以获取证据的一种方法；检查使用到的工具主要是核查列表。检测人员针对核查列表上的问题，通过观察、查验、分析等活动，逐项核实。根据检查对象的不同，检查可以进一步分为文档审查、现场观测和配置核查等方式；

测试可以细分为工具测试和手工验证等，类型包括功能测试、安全测试等。其中工具测试是指利用抓包工具对目标设备进行通讯报文的抓取，并用日志分析工具进行分析，直观地验证系统平台的安全状况。包括信息获取、密码分析等方式。手工验证是指根据要求上机验证安全功能和配置的实现情况。

4. 评估内容及结果

4.1 交易安全

测评对象	测评指标	结果记录	结果判定	问题编号
交易验证	交易验证应组合选用下列三类要素：仅客户本人知悉的要素，如静态密码等；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；客户本人生物特性要	基于多方安全计算的差异化营销平台不涉及资金交易，故此项不适用。	不适用	

测评对象	测评指标	结果记录	结果判定	问题编号
	素，如指纹、虹膜、声纹等。			
	申请机构应确保采用的要素相互独立，即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。	基于多方安全计算的差异化营销平台不涉及资金交易，故此项不适用。	不适用	
	申请机构应严格限制使用初始交易密码并提示客户及时修改，建立交易密码复杂度校验机制，避免交易密码过于简单（如“111111”、“123456”等）或与个人金融信息（如出生日期、证件号码、手机号码等）相似度过高。	基于多方安全计算的差异化营销平台不涉及资金交易，故此项不适用。	不适用	
	申请机构采用数字证书、电子签名作为认证要素的，数字证书及生成电子签名的过程应符合《中华人民共和国电子签名法》、JR/T0118 等有关规定，确保数字证书的唯一性、完整性及交易的抗抵赖性。	基于多方安全计算的差异化营销平台不涉及资金交易，故此项不适用。	不适用	
	申请机构采用一次性密码作为验证要素的，应切实防范一次性密码获取端与交易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。	基于多方安全计算的差异化营销平台不涉及资金交易，故此项不适用。	不适用	
	申请机构采用客户本人生物特征作为验证要素的，应符合国家、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。	基于多方安全计算的差异化营销平台不涉及资金交易，故此项不适用。	不适用	
	申请机构应经过客户确认并进行交易验证，交易验证宜同时采用上述三类要素中的两类要素，不足两类的应采取相应的风险补偿措施。	基于多方安全计算的差异化营销平台不涉及资金交易，故此项不适用。	不适用	
	进行支付交易时，申请机构应采取交易验证强度与交易额度相匹配的技术措施，提高交易的安全性。	基于多方安全计算的差异化营销平台不涉及资金交易，故此项不	不适用	

测评对象	测评指标	结果记录	结果判定	问题编号
		适用。		
交易确认	申请机构应采取有效措施，确保客户在执行支付指令前可对收付款客户名称和账号、交易金额等交易信息进行确认，并在支付指令完成后展现交易信息或及时将结果通知客户。	基于多方安全计算的差异化营销平台不涉及资金交易，故此项不适用。	不适用	
	申请机构应确保交易信息的真实性、完整性、可追溯性以及在支付全流程中的一致性，不得篡改或者隐匿交易信息。	基于多方安全计算的差异化营销平台不涉及资金交易，故此项不适用。	不适用	
	申请机构应采用静态密码、动态口令、数字证书等可靠的技术手段实现本人主动确认，保障用户的知情 权、财产安全权等合法权益。	基于多方安全计算的差异化营销平台不涉及资金交易，故此项不适用。	不适用	
交易监控系统建立	申请机构应建立支付交易监控系统，能够甄别并预警潜在风险的交易，例如套现、洗钱、欺诈等可疑交易，并生成风险监控报告。	基于多方安全计算的差异化营销平台不涉及资金交易，故此项不适用。	不适用	
	申请机构应根据交易的风险特征建立风险交易模型，有效监测可疑交易，对可疑交易建立报告、复核、查结机制。	基于多方安全计算的差异化营销平台不涉及资金交易，故此项不适用。	不适用	
	申请机构应采用大数据分析、客户行为建模等手段，建立交易风险监控模型和系统，对异常交易进行及时预警，并采取调查核实、风险提示、延迟结算等处理措施	基于多方安全计算的差异化营销平台不涉及资金交易，故此项不适用。	不适用	
	申请机构应不使用交易行为分析、机器学习等不断优化风险评估模型，提高欺诈交易拦截成功率，切实提升交易安全防护能力。	基于多方安全计算的差异化营销平台不涉及资金交易，故此项不适用。	不适用	
交易风险识别	申请机构应支持欺诈风险的识别，包括但不限于非面欺诈、账户盗用、伪冒申请、商户合谋、	基于多方安全计算的差异化营销平台不涉及资金	不适用	

测评对象	测评指标	结果记录	结果判定	问题编号
	营销欺诈等风险。	交易，故此项不适用。		
	申请机构应支持对合规风险的识别，包括但不限于非面欺诈、账户盗用、伪冒申请、商户合谋、营销欺诈等风险。	基于多方安全计算的差异化营销平台不涉及资金交易，故此项不适用。	不适用	
交易风险处置	申请机构应针对拦截阻断的交易进行风险核查，分析原因与风险特征，以确认当时的决策是否准确恰当。	基于多方安全计算的差异化营销平台不涉及资金交易，故此项不适用。	不适用	
	申请机构应针对挂起确认和提示预警的交易进行风险核查，分析原因与风险特征，以确认当时的决策是否准确恰当。	基于多方安全计算的差异化营销平台不涉及资金交易，故此项不适用。	不适用	
	申请机构应对于存有风险的业务相关元素，基于潜在关系进行关联排查，以挖掘是否存在同类风险或衍生风险，弥补事中监测决策可能未识别的潜在风险敞口。	基于多方安全计算的差异化营销平台不涉及资金交易，故此项不适用。	不适用	
	申请机构应配合公安、司法机关开展风险案件协查。	基于多方安全计算的差异化营销平台不涉及资金交易，故此项不适用。	不适用	
	申请机构对于明确产生的风险损失，应建立快速挽损、风险责任认定，将风险化解、转移或者赔偿的处置方式，并控制后续风险损失敞口。	基于多方安全计算的差异化营销平台不涉及资金交易，故此项不适用。	不适用	

4.2 服务质量

测评对象	测评指标	结果记录	结果判定	问题编号
服务质量	申请机构应建立服务质量管理规范，包括 QoS 预测、QoS 建立、QoS 监控、QoS 维护等过程管理。	申请机构提供了《质量管理规范》，第六章节“服务质量管理”包括 QoS 预测分析、QoS 建	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
		立规范、QoS 监控规范、QoS 维护规范等过程管理。		
	申请机构应通过对创新应用的业务功能、预期用户数、服务地域、服务时间等特性进行充分分析，从服务可用性、吞吐量、时间延迟等方面预测 QoS。	申请机构提供了《质量管理规范》，从业务功能、预期用户数、服务地域、服务时间等多个方面分析，从 TPS、响应时间等方面来预测 QoS。	符合	
	申请机构应以满足用户或相关方的业务期望为基础，根据具体资源情况建立 QoS 目标，设置可接受最低质量（LQA）极限。	申请机构在产品上线前进行了性能测试，以满足用户或相关方的业务期望为基础，根据具体资源情况建立了 QoS 目标，并设置了可接受最低质量（LQA）极限。	符合	
	申请机构应对通信线路、网络设备、主机设备、应用软件的运行情况进行 QoS 监控，检查服务可用性、吞吐量、时间延迟等是否满足 QoS 目标，对系统的服务水平低于 LQA 时进行预警。	申请机构对 ICMP response time、IPv4 Connecttios、Active VPN tunnels、Network Traffic wan1、Network Traffic wan2、Network Traffic lan 监控，系统的服务水平低于 LQA 通过钉钉和企业微信进行预警。	符合	
	申请机构应在可接受的级别上为满足 QoS 进行资源分配。	申请机构进行了 Network Traffic wan 划分，满足 QoS 资源分配。	符合	

4.3 业务连续性

测评对象	测评指标	结果记录	结果判定	问题编号
业务影响分析	申请机构应根据当前的业务场景，使用恰当的分析方法，对所面临的威胁和当前体系的脆弱性进行深入剖析，评估各类风险发	申请机构建立了《冰鉴科技-业务连续性管理办法》，在办法第二章业务中断分析章节对所面临的威胁和当前	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
	生的概率和可能导致的损失。	体系的脆弱性进行深入剖析，评估各类风险发生的概率和可能导致的损失，并对系统开展了应用漏洞扫描，针对发现的漏洞进行了整改。		
	申请机构应对风险可能造成的业务影响进行研判。	申请机构建立了《冰鉴科技-业务连续性管理办法》，在办法第二章业务中断分析章节对业务中断成因、业务中断的企业影响进行了研判，第七章系统 RTO 与 RPO 对灾难恢复时间目标及恢复点目标进行了阐述。	符合	
	申请机构应根据监管要求、业务性质、业务服务范围、数据集中程度、业务时间敏感性、功能关联性等要素进行业务功能分析，并在此基础上评估业务中断可能造成的影响，确定灾难恢复目标及恢复优先级。	申请机构建立了《冰鉴科技-业务连续性管理办法》，在办法第二章业务中断分析章节对业务中断成因、业务中断的企业影响进行了研判，并在第七章系统 RTO 与 RPO 对灾难恢复时间目标及恢复点目标进行了阐述。	符合	
业务连续性管理	申请机构应制定业务连续性策略及计划。	申请机构建立了《冰鉴科技-业务连续性管理办法》，在办法第八章业务连续性策略规划章节描述了业务系统业务连续性策略及计划。	符合	
	申请机构应从应用和数据等技术方面确保业务连续性，避免单点故障。	申请机构建立了《冰鉴科技-业务连续性管理办法》和《冰鉴科技-构建高可用的跨 AZ 部署方案》，通过构建高可用的跨 AZ 部署方案	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
		来确保业务连续性，避免单点故障。		
	申请机构应将业务连续性管理整合到组织的流程和架构中，明确指定相关部门负责业务连续性的管理。	申请机构建立了业务连续性管理制度《业务连续性管理制度》，在文档第四章组织架构章节明确指定了相关部门负责业务连续性的管理。	符合	
	申请机构应制定员工在业务连续性方面的培训计划和考核标准。	申请机构建立了业务连续性管理办法《冰鉴科技-业务连续性管理办法》，在管理办法第五章培训与演练章节描述了“定期对员工进行业务连续性管理办法的培训”，具有业务连续性的培训记录和考核记录。	符合	
	申请机构应定期或在业务系统发生显著变化时，测试并更新业务连续性计划与过程，以确保其持续有效。	申请机构建立了《冰鉴科技-业务连续性管理办法》，在办法第八章业务连续性策略规划章节描述了业务系统业务连续性策略及计划，并定期或在业务系统发生显著变化时，测试并更新业务连续性计划。	符合	
	申请机构应至少每年组织 1 次业务连续性专项内部审计或委托第三方进行的审计，并形成包括审计意见、改进计划和改进结果的审计报告。	申请机构每年会组织一次业务连续性专项内部审计，具有《冰鉴科技-2020 年业务连续性审计报告》，报告包括审计意见、改进计划和改进结果等内容。	符合	
	申请机构使用的科技产品应至少支持容灾能力 3 级要求，容灾等级划分及关键指标要求参见附录。	基于多方安全计算的差异化营销平台满足容灾能力 3 级要求，在《冰鉴科技-业务连续	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
		性管理办法》第七章系统 RTO 与 RPO 章节对容灾能力进行了说明，系统可用性为 99.99%。		
资源配置	申请机构应避免机房采用的多路市电输入均来自于同一个变电站,应对 UPS 等重要设备的报警日志进行及时审核和处理	基于多方安全计算的差异化营销平台部署在阿里云上，阿里云公共云平台已通过网络安全等级保护三级测评， 基础设施安全由阿里云提供保障，因此能够满足要求。	符合	
	申请机构应提供冗余通信线路，并选择与主用通信线路不同的电信运营商和不同的物理路径	基于多方安全计算的差异化营销平台部署在阿里云上，阿里云公共云平台已通过网络安全等级保护三级测评，因此能够满足要求。	符合	
	申请机构核心层、汇聚层的设备和重要的接入层设备均应双机热备，例如，核心交换机、服务器群接入交换机、重要业务管理终端接入交换机、核心路由器、防火墙、均衡负载器、带宽管理器及其他相关重要设备	基于多方安全计算的差异化营销平台部署在阿里云上，阿里云公共云平台已通过网络安全等级保护三级测评，因此能够满足要求。	符合	
	申请机构 Web 服务器、中间件服务器、前置服务器、数据库服务器等关键数据处理系统均应双机热备或多机集群，并设置磁盘冗余阵列或分布式多副本存储技术，以避免单一部件故障影响设备运行的风险	基于多方安全计算的差异化营销平台部署在阿里云上，阿里云公共云平台已通过网络安全等级保护三级测评，通过阿里云多可用区部署，来实现服务器负载均衡，在同机房内通过多机集群和双机热备来保障系统的高可用，在《冰鉴科技-构建高可用的跨 AZ 部	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
		署方案》文档中进行了描述。		
	申请机构应梳理并维护关键的设备部件、备件清单，采取有效的措施防止因单个设备部件出现故障，导致冗余设备无法正常启用或切换的风险。	基于多方安全计算的差异化营销平台部署在阿里云上，在同机房内通过多机集群和双机热备来保障系统的高可用，梳理并维护了关键的设备部件、备件清单，当设备服务器出现异常风险时，阿里云平台会发送邮件通知申请机构进行修复。	符合	
备份与恢复管理	申请机构应根据系统的业务影响性分析结果，制定不同数据的备份策略，并实施应用级备份，以保证灾难发生时，能尽快恢复业务运营	申请机构建立了《冰鉴科技-备份恢复管理制度》，制度中 2.制定备份与恢复策略章节中描述了数据备份策略、恢复策略。	符合	
	申请机构应建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存，明确规定备份数据的保存期，做好备份数据的销毁申请、审查和登记工作	申请机构建立了《冰鉴科技-备份恢复管理制度》，在文档中对备份和恢复的程序进行了说明，并具有备份恢复记录，具有《销毁申请》和《数据操作流程记录表》。	符合	
	申请机构应定期执行恢复程序，检查并测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份恢复	申请机构会定期执行恢复程序，检查并测试备份介质的有效性，具有《备份与恢复测试报告》。	符合	
	申请机构应对技术方案中关键技术应用的可行性进行验证测试，并记录和保存验证测试的结果，以满足灾难恢复策略的要求	申请机构对备份恢复方案中关键技术应用的可行性进行了验证测试，具有《备份与恢复测试报告》。	符合	
	申请机构应在统一的灾难恢复策略下建立完善的系统灾难恢复体系，开展灾	申请机构建立了《冰鉴科技-备份恢复管理制	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
	难恢复需求分析、策略及计划制定、灾备系统建设及演练等工作，并根据实际情况对其进行分析和改进，确保各环节的正确性以及灾难恢复体系的有效性	度》，在文档第 2 章制定备份与恢复策略章节根据资产识别的结果和备份级别制定备份计划，具有《备份与恢复测试报告》和《数据操作流程记录表》。		
	申请机构的同城数据备份中心，应保证可以接管所有核心业务的运行，与生产中心直线距离应满足 JR/T 0071 相关安全技术要求	基于多方安全计算的差异化营销平台部署在阿里云华东区机房，生产中心选择阿里云杭州-萧山-B 和杭州-萧山-D，地址杭州市萧山区高教园区弘慧路。灾备中心选择阿里云-杭州-临安-A，地址杭州市临安区道路运输管理处青山管理所。生产中心与灾备中心直线距离为 43 千米。 在《冰鉴科技-构建高可用的跨 AZ 两地三中心部署方案》第 2 章对同城数据备份中心进行了说明。	符合	
	申请机构的异地数据备份中心，与生产中心直线距离应满足 JR/T 0071 相关安全技术要求	基于多方安全计算的差异化营销平台部署在阿里云上，异地灾备中心位于上海市浦东新区新金桥路 2222 号，与生产中心直线距离 170 千米。 在《冰鉴科技-构建高可用的跨 AZ 两地三中心部署方案》第 3 章对异地数据备份中心进行了说明。	符合	
	申请机构应实时监控生产中心和灾备中心的业务应用可用性和性能状态，并具备告警功能	基于多方安全计算的差异化营销平台部署在阿里云上，通过阿里云监控插件和	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
		Prometheus+grafana 对服务器资源利用情况进行监控和告警。使用的是 EFK（elasticsearch+flume+kibana）对应用运行状态进行监控， EFK 含监控管理、日志管理功能,通过实时查询 EFK 里面收集到的应用日志,检索 error 字段、对比过去一段时间的结果进行告警,告警接收渠道有钉钉和企业微信。		
	申请机构应能够有效监控灾备切换过程和同步状态	基于多方安全计算的差异化营销平台部署在阿里云上，能够有效监控灾备切换过程和同步状态，并通知申请机构。	符合	
应急预案及演练	申请机构应建立业务连续性预案程序，预案应包括应急和系统灾难恢复两部分。应急部分包括但不限于灾难场景和范围定义、应急的管理机构和决策机制、应急响应的流程、工具和工作制度等内容。系统灾难恢复部分包括但不限于灾难恢复的范围和目标、灾难恢复的总体规程、各系统恢复的切换步骤、操作手册和业务功能恢复验证测试方法等内容	申请机构建立了《冰鉴科技-业务连续性管理制度》，在制度中明确了应急和系统灾难恢复内容，并具有《冰鉴科技-数据安全应急演练方案》。	符合	
	申请机构应建立应急预案演练制度，定期组织有业务部门参与的桌面演练和生产系统实战演练，定期对双机热备系统进行切换演练，备份系统与生产系	申请机构建立了《冰鉴科技-数据安全应急演练方案》，并定期组织有业务部门进行数据安全事件应急演练，具有系统灾备切换演练	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
	统的切换要至少每年演练一次。针对 DDoS、网络钓鱼等重要安全威胁，定期开展有相关单位、部门参与的联合演练	记录。针对 DDoS、网络钓鱼等重要安全威胁，定期开展有相关单位、部门参与的联合演练，具有相关的演练记录。		
	申请机构应急和灾难恢复流程不应引入数据泄露的风险	申请机构应急和灾难恢复流程均在机构内部进行，不涉及外部机构，应急和灾难恢复流程均要经过严格的流程管控，没有引入数据泄露的风险。	符合	

4.4 算法安全

测评对象	测评指标	结果记录	结果判定	问题编号
算法设计	申请机构应正确定义目标函数，避免目标函数错误导致决策偏离预期甚至出现伤害性结果	查阅设计文档及相关代码，申请机构人工智能算法正确定义了目标函数，针对实际业务场景采用了逻辑回归和 GBDT 两种模型，前者的目标函数是平均对数似然损失，后者分情况提供了对数损失、指数损失函数。访谈技术相关人员，确认系统通过核验算法原理、充分考察环境常识、结合业务原理来避免人工智能算法目标函数定义的错误。	符合	
	申请机构应避免算法目标函数运算成本过高，确保算法目标函数运算的占用资源不会使整体运行效率明显降低。	经访谈算法设计人员，申请机构人工智能算法目标函数本身运算复杂度低，同时对不同算法采用了不同的策略来降低运算成本，比如对于逻辑回归会根据不同情况使用不同的梯度下降方式，比如在不同的数据量级、精度要求下采用不同的批量、随机、小批量梯度下降方式，平衡业务需求与成本；GBDT 模型可以通过调整基模型	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
		数量、树深度、学习率等来提升运行速率；同时两种模型都可通过多进程在不过多占用资源的情况下保证运行效率。		
	申请机构算法表达能力应充分，避免算法在实际使用时面对不同于训练阶段的全新情况产生错误的结果	经访谈算法设计人员，申请机构采用的算法是充分结合了市场业务需求，一方面经过了市场的长期检验、另一方面也会根据具体应用采用相应的创新选择出来的。逻辑回归算法本身的可解释性就很强，而 GBDT 也可以通过不同树模型分析给出可解释的规则策略，因而在不同于训练阶段的全新情况出现时，由于算法对特征的可解释性可迅速察觉到变化大的因素，从而能积极的响应并作出调整，因此避免产生错误的结果。	符合	
	申请机构应避免应用于金融业务中的人工智能算法存在因设计者和开发者的主观选择造成的偏见的决策结果	经访谈算法设计人员，申请机构人工智能算法避免了算法潜藏的偏见和歧视，一方面在算法的设计上，是结合了市场调研和客观分析的结果，同时在不同的模型选择上，也是基于大量的案例和业务背景优中选优的结果，对于数据的使用，是在保证安全性、经济性、有效性的基础上做出的合理选择和应用。通过充分的理论基础加实践经验，以及设计团队对市场的实时跟踪分析，保证算法选择客观可靠，避免了因设计者和开发者的主观选择造成的偏见和决策结果。	符合	
	申请机构应避免应用于金融业务中的人工智能算法存在因客观训练数据造成的偏见决策结果	经访谈算法设计人员，申请机构人工智能算法拥有充分的数据清洗、特征筛选、数据核验等技术，以及相应的 iv 图分析功能，使得数据入模前，可以	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
		对数据的分布、特征维度、基本效果有一定的认识，从而避免了黑盒式的训练数据，导致结果偏差。并且可以通过改变随机数改变数据训练集测试集的划分，进行交叉检测，避免因数据误差带来的结果偏差。因此，整个系统避免了应用于金融业务中的人工智能算法存在因客观训练数据造成偏见的决策结果。		
	申请机构应根据不同业务场景需要设计对应的算法或者模型。	经访谈算法设计人员，申请机构人工智能算法根据不同业务场景需要设计了对应的算法和模型，比如对于特征维度少且对成本预算有限的情况可使用其提供的逻辑回归算法，对于特征维度高且特征区分度不是特别明显的情况可以采用基于树模型的 GBDT 算法。	符合	
算法可解释性	申请机构算法特征变量若从业务出发，其定义应满足相关业务逻辑和规则。	查阅设计文档，及访谈算法设计人员，特征变量主要包括和风险相关垂直领域或者消息触达高的领域的用户行为特征，这类特征与业务高度契合，定义也满足业务逻辑和规则。查看代码，确定代码实现与算法设计一致。	符合	
	申请机构算法特征分布应符合人的常识和业务规则，尽量避免特征变量的值是异常数据点。	经访谈算法设计人员，算法特征设计贴合业务逻辑与规则，且衍生处理过程包含了常规提取与处理、深度网络计算，都使用了脱敏、降维、数据的合理转化、异常值校验，因此特征的取值尽量避免了异常的数据点。	符合	
	申请机构算法应明确记录特征选择的业务逻辑和算法依据。	经访谈算法设计人员，申请机构人工智能算法明确记录了在做特征选择时应根据不同的业务背景做相关性、数量上的衡	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
		量，同时根据业务逻辑推荐最佳的算法。		
	申请机构算法应能够标识代表性样本或非代表性样本，并对其进行相关说明。	经访谈算法设计人员，申请机构对代表性样本，比如包括模型对应的训练集、测试集，或者非代表性样本，比如用于测试的数据集，都有相应的 id 与之对应，且有明确的追溯窗口，可以查看数据的逻辑和正确性，且代码实心与算法设计一致。	符合	
	申请机构在模型构建过程中，应根据具体业务场景和具体算法，至少定义 1 项具体的指标来度量可解释性。	经访谈算法设计人员，申请机构人工智能算法在模型构建过程中，根据不同的业务场景和不同算法，对最终模型入模特征定义了包括重要性、相关性、稳定性等，以及最终的模型效果给出了 auc、ks、gini 等指标来对结果假以解释，因而式至少定义了 1 项具体指标来度量可解释性的。	符合	
	申请机构应避免科技产品中的算法存在非公开性、算法复杂性造成的决策结果不可解释的问题。	经访谈算法设计人员，申请机构通过对不同算法采用不同措施来避免不可解释性，其中对于公开算法，会研究核心代码，根据算法本身可解释性的程度给出一定的改进，使得应用工程中能够给出相应的可解释性。避免了存在非公开下、算法复杂性造成的决策结果不可解释的问题。	符合	
	申请机构应通过代码注释等方式提高算法的可读性。	经查看算法代码，申请机构有通过大量通俗易懂的代码注释来提高算法的可读性。	符合	
算法可追溯性	申请机构应记录训练数据获取时间、训练数据量、数据存储介质标识。	经查看申请机构训练数据记录，记录内容包括训练数据获取、关联、建模等过程的时间，同时数据量、特征维度都可获取，数据的形式、存储介质也很明确。	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
	申请机构应对使用的训练数据有完整签名或校验码。	经访谈算法设计人员，申请机构对使用的训练数据有完整的签名，保证在模型确认、模型上线部署的过程中可以唯一的查找到该训练数据集。	符合	
	申请机构应保存建模过程中建模脚本及参数迭代的相关记录。	经查看，申请机构保存了建模过程中建模脚本以及参数迭代、训练等的日志与记录。	符合	
	申请机构应对建模过程的操作者进行标识，记录建模的起止时间戳和迭代次数。	经查看，申请机构对建模过程中的操作者做了登录校验和标识，同时记录了建模的起止时间戳及耗时，以及训练过程中的迭代次数等信息。	符合	
	申请机构应记录算法模型部署的操作者，标识部署时间及相关结果。	经查看，申请机构通过日志、可视化界面记录了算法模型部署的操作者，并标识了部署时间以及相关结果。	符合	
	申请机构应保存算法模型部署的相关脚本。	经查看，申请机构保存了算法模型部署的相关脚本。	符合	
算法攻击防范	申请机构应加强算法关于训练数据、模型的传输、存储等方面的安全管理，防范训练数据、模型被窃取。	经访谈算法设计人员，申请机构使用了大量的密文交互，包括秘密分享、混淆电路、同态加密等算法来保证数据训练以及模型传输、存储的安全管理，且检查相关机制确认得到有效部署。	符合	
	申请机构应保障算法训练步骤安全，防范训练过程被窃取导致训练信息泄露，进而恶意构建相似模型。	经访谈算法设计人员，申请机构使用了基于多方安全计算的秘密分享，保证模型每个训练步骤生成的中间结果拆分为多个分片，交由不同部门保管。从少于门限数量的分片无法获取任何有效信息，从而防范训练信息泄露被恶意构建相似模型。	符合	
	申请机构算法模型应具有辨识度，如	经访谈算法设计人员，申请机构算法模型具有可辨识的日志	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
	模型添加水印等，通过合适途径辨别恶意伪构模型。	编码，同时经发布的模型一定具有唯一对应的一串服务号，保障了模型的辨识度。		
	申请机构应确保训练数据来源可信、可靠，避免采集到标签错误等恶意药饵数据。	经访谈算法设计人员，申请机构训练数据主要是基于全域数据与技术能力建立的精准消息推送、用户行为数据，同时利用树模型等机器学习模型、神经网络进行数据的清洗、处理、变幻来保证数据来源可信、可靠，且相关措施得到有效部署。	符合	
	申请机构应确保训练数据分布合理，防止药饵攻击数据点混入，造成模型倾斜等错误状况。	经访谈算法设计人员，申请机构使用了多种脱敏、降维、特征编码技术，达到数据分布合理且保效甚至提高效果。从而有效防止药饵攻击数据点混入，保证模型无误。	符合	
	申请机构在满足用户需求的前提下，算法模型输出的反馈信息应遵循最小够用的原则，避免泄露信息过多造成逆向攻击。	经访谈算法设计人员，确保模型输出的反馈信息都遵循最小够用原则，不会泄露中间结果及敏感信息。	符合	
	申请机构应通过限制攻击者对人工智能算法测试频率，避免恶意探测获取人工智能算法信息，逆向构建恶意模型。	经访谈算法设计人员，申请机构通过分布式网络分配多个参与实体各自持有秘钥输入防止攻击者测试成功，同时给非分配密钥频繁测试进行预警，从而避免恶意探测获取人工智能算法信息，进一步避免逆向构建恶意模型。	符合	

4.5 数据安全

4.5.1 数据质量

测评对象	测评指标	结果记录	结果判定	问题编号
数据质量	申请机构应对数据进行分	申请机构建立了数据	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
	类管理，明确不同数据之间的关系和依赖性，制定数据质量管理目标。	管理制度《冰鉴科技-数据管理办法》，对数据进行了分类管理，数据分为原始数据、标识数据、指标数据等，并明确不同数据之间的关系和依赖性以及数据质量管理目标。		
	申请机构应明确数据质量管理部门和机制，定义数据质量管理的角色和职责，建立数据质量管理办法。	申请机构建立了数据管理制度《冰鉴科技-数据管理办法》，在管理办法第二章节组织架构中明确数据质量管理部门和机制，定义数据质量管理的角色和职责。	符合	
	申请机构应研发数据质量相关技术，支撑数据质量管理和数据质量提升。	申请机构研发数据质量相关技术对数据的完整性、准确性、一致性、及时性进行监控及判别，并在《冰鉴科技-数据管理办法》中第7章节质量监控中进行了描述。	符合	
	申请机构应识别数据生命周期各个阶段的数据质量关键因素，构建数据质量评估框架，包括但不限于数 据的准确性、完整性、一致性、可访问性、及时性、相关性和可信度等。	申请机构建立了数据管理制度《冰鉴科技-数据管理办法》，在办法第7章节质量监控中对数据的完整性、准确性、一致性、及时性、可访问性、相关性、可信度等内容进行了描述。	符合	
	申请机构应采用定性评估、定量评估或综合评估等方法，评估和持续优化数据质量。	申请机构建立了数据管理制度《冰鉴科技-数据管理办法》，在办法第7章质量监控章节中定义了质量监控评估标准。	符合	

4.5.2 个人金融信息保护

4.5.2.1 全生命周期防护

测评对象	测评指标	结果记录	结果判定	问题编号
收集	应采取技术措施（如弹窗、明显位置 URL 链接等），引导个人金融信息主体查阅隐私政策，并获得其明示同意后，开展有关个人金融信息的收集活动。	基于多方安全计算的差异化营销平台不涉及个人金融信息的收集，故此项不适用。	不适用	
	应遵循合法、正当、必要的原则，向个人金融信息主体明示收集与使用个人金融信息的目的、方式、范围和规则等，不得收集与所提供服务无关的个人金融信息。	基于多方安全计算的差异化营销平台不涉及个人金融信息的收集，故此项不适用。	不适用	
	应通过受理终端、客户端应用软件、浏览器等方式收集 C3（用户鉴别信息）类别个人金融信息时，应使用加密等技术措施保证数据的保密性，防止其被未授权的第三方获取。	基于多方安全计算的差异化营销平台不涉及个人金融信息的收集，故此项不适用。	不适用	
	客户端应用软件向移动终端操作系统申请权限时，应遵循最小权限原则。	基于多方安全计算的差异化营销平台不涉及个人金融信息的收集，故此项不适用。	不适用	
	应确保收集个人金融信息来源的可追溯性。	基于多方安全计算的差异化营销平台不涉及个人金融信息的收集，故此项不适用。	不适用	
	不应委托或授权无金融业相关资质的机构收集 C3（用户鉴别信息）、C2(可识别主体身份与金融状况的个人金融信息）类别个人金融信息。	基于多方安全计算的差异化营销平台不涉及个人金融信息的收集，故此项不适用。	不适用	
传输	应根据个人金融信息的不同类别，采用技术手段保证个人金融信息的安全传输，如安全通道、数据加密等技术措施。	基于多方安全计算的差异化营销平台使用 HTTPS 加密协议进行加密传输，采用基于同态加密、混淆电路等技术，实现对数据及模型的加密处理，并在《冰	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
		鉴科技-数据安全管理办法》第五章数据全生命周期安全管理中对数据传输进行了要求。		
	个人金融信息传输的接收方应对接收的个人金融信息进行完整性校验。	基于多方安全计算的差异化营销平台使用 HTTPS 加密传输协议进行加密传输，可保障数据通信过程的完整性和保密性。	符合	
存储	受理终端、个人终端及客户端应用软件均不应存储银行卡磁道数据（或芯片等效信息）、银行卡有效期、卡片验证码（CVN 和 CVN2）、银行卡密码、网络支付密码等支付敏感信息及个人生物识别信息的样本数据、模板，仅可保存完成当前交易所必需的基本信息要素，并在完成交易后及时予以清除。	申请机构不涉及银行卡磁道数据（或芯片等效信息）、银行卡有效期、卡片验证码（CVN 和 CVN2）、银行卡密码、网络支付密码等支付敏感信息及个人生物识别信息的样本数据、模板，故此项不适用。	不适用	
	不应留存非本机构的银行卡磁道数据（或芯片等效信息）、银行卡有效期、卡片验证码（CVN 和 CVN2）、银行卡密码、网络支付密码等 C3（用户鉴别信息）类别个人金融信息。若确有必要留存的，应取得个人金融信息主体及账户管理机构的授权。	申请机构不涉及银行卡磁道数据（或芯片等效信息）、银行卡有效期、卡片验证码（CVN 和 CVN2）、银行卡密码、网络支付密码等 C3（用户鉴别信息）类别个人金融信息收集和存储，故此项不适用。	不适用	
	C3（用户鉴别信息）类别个人金融信息应采用加密措施确保数据存储的保密性。	申请机构登录密码在数据库中通过哈希算法进行加密存储。	符合	
	应将个人生物识别信息的样本数据、模板与银行账号或支付账号、身份证号等用户个人隐私信息进行隔离存储。	申请机构基于多方安全计算的差异化营销平台不涉及个人生物识别信息的样本数据、模板，故此项不适用。	不适用	
使用	对于银行卡号、手机号码、证件类识别标识或其他识别	申请机构基于多方安全计算的差异化营销	不符合	BJKJ-001

测评对象	测评指标	结果记录	结果判定	问题编号
	标识信息等可以直接或组合后确定个人金融信息主体的信息应进行屏蔽展示，或由用户选择是否屏蔽展示，如需完整展示，应进行用户身份验证，并做好此类信息管理，防范此类信息泄露风险。	平台只涉及后台操作人员、管理人员的手机号码个人金融信息展示，但目前系统上暂未对上述手机号码进行屏蔽展示。 在《冰鉴科技-数据安全管理办法》第五章数据全生命周期安全管理章节第四节数据使用中数据授权使用、数据处理分析、敏感数据脱敏等要求进行了描述。		
	后台系统应对支付账号、客户法定名称、支付预留手机号码、证件类或其他类识别标识信息等展示宜进行屏蔽处理，如需完整展示，应做好此类个人金融信息管理，采取有效措施防范未经授权的拷贝。	申请机构基于多方安全计算的差异化营销平台不涉及支付账号、客户法定名称、支付预留手机号码等支付信息，故此项不适用。	不适用	
	在个人金融信息共享和转让前，应开展个人金融信息接收方信息安全保障能力评估，并与其签署数据保护责任承诺。	基于多方安全计算的差异化营销平台不涉及外部共享和转让，故此项不适用。	不适用	
	应向个人金融信息主体告知共享、转让个人金融信息的目的、个人金融信息接收方的类型，并事先征得个人金融信息主体明示同意。	基于多方安全计算的差异化营销平台不涉及外部共享和转让，故此项不适用。	不适用	
	支付账号及其等效信息在共享和转让时，除法律法规和行业主管部门另有规定外，应使用支付标记化（按照JR/T0149）技术进行脱敏处理（因业务需要无法使用支付标记化技术时，应进行加密），防范个人金融信息泄露风险。	基于多方安全计算的差异化营销平台不涉及支行账号的共享和转让，故此项不适用。	不适用	

测评对象	测评指标	结果记录	结果判定	问题编号
	应执行严格的审核程序，并准确记录和保存个人金融信息共享和转让情况。记录内容应包括但不限于日期、规模、目的、范围，以及个人金融信息接收方基本情况与使用意图等，并应确保对共享和转让的个人金融信息及其过程可被追溯。	基于多方安全计算的差异化营销平台不涉及外部共享和转让，故此项不适用。	不适用	
	在个人金融信息共享和转让的过程中，应部署信息防泄露监控工具，监控及报告个人金融信息的违规外发行为。	基于多方安全计算的差异化营销平台不涉及外部共享和转让，故此项不适用。	不适用	
	个人金融信息原则上不得公开披露，经法律授权或具备合理事由确需公开披露时，应事先开展个人金融信息安全影响评估，准确记录和保存个人金融信息的公开披露情况，包括公开披露的日期、规模、目的、内容、公开范围等。	基于多方安全计算的差异化营销平台不涉及个人金融信息的公开披露情况，故此项不适用。	不适用	
	因金融产品或服务的需要，将收集的个人金融信息委托给第三方机构（包含外包服务机构与外部合作机构）处理时，应采用去标识化（不应仅使用加密技术）等方式进行脱敏处理，降低个人金融信息被泄露、误用、滥用的风险。	申请机构不涉及个人金融信息委托给第三方机构处理的情况，故此项不适用。	不适用	
	应对委托行为进行个人金融信息安全影响评估，并确保受委托者具备足够的数据安全能力，且提供了足够的安全保护措施。	申请机构不涉及个人金融信息委托给第三方机构处理的情况，故此项不适用。	不适用	
	在个人金融信息加工处理的过程中，应建立个人金融信息防泄露控制规范和机制，防止个人金融信息处理过程	申请机构建立了个人金融信息防泄露控制规范和机制，查看后台日志中的个人金融信	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
	中的调试信息、日志记录等因不受控制的输出而泄露受保护的信息。	息均加密显示，在《冰鉴科技-数据安全管理办法》第四节数据使用章节描述了数据授权使用、敏感数据脱敏等要求。		
	在个人金融信息开发测试过程中，应对开发测试环境与生产环境进行有效隔离。	申请机构开发测试环境与生产环境部署在不同的网段，相互之间无法进行通信。	符合	
	开发环境、测试环境不应使用真实的个人金融信息，应使用虚构的或经过去标识化（不应仅使用加密技术）脱敏处理的个人金融信息，账号、卡号、协议号、支付指令等测试确需个人金融信息除外。	申请机构开发环境和测试环境没有使用真实的个人金融信息，使用的是模拟数据。	符合	
	汇聚融合的个人金融信息不应超出收集时所声明的使用范围。因业务需要确需超范围使用的，应再次征得个人金融信息主体明示同意。	申请机构汇聚融合的个人金融信息没有超出收集时所声明的使用范围。	符合	
删除	应采取技术手段，在金融产品和服务所涉及的系统中去除个人金融信息，使其保持不可被检索和访问。	基于多方安全计算的差异化营销平台删除个人金融信息后，数据会从数据库中直接被删除，系统中将不可被检索和访问。	符合	
销毁	应对个人金融信息存储介质销毁过程进行监督与控制，对待销毁介质的登记、审批、介质交接、销毁执行等过程进行监督。	申请机构建立了《冰鉴科技-数据安全管理办法》，在办法第五章数据全生命周期安全管理章节第六节数据销毁中描述了数据销毁机制和介质销毁的流程，具有数据销毁记录。	符合	

4.5.2.2 安全管理

测评对象	测评指标	结果记录	结果判定	问题编号
安全策略	应建立个人金融信息保护制度体系，明确工作职责，规范工作流程。制度体系的管理范畴应涵盖本机构、外包服务机构与外部合作机构，并确保相关制度发布并传达给本机构员工及外部合作方（包括外包服务机构、外部合作机构）。相关制度应至少包括个人金融信息保护管理规定、日常管理及操作流程、外包服务机构与外部合作机构管理、内外部检查及监督机制、应急处理流程和预案、个人金融信息投诉与申诉处理程序。	申请机构建立个人金融信息保护制度体系《冰鉴科技-数据安全管理办法》和《冰鉴科技-数据安全管理文档》，在制度中明确了日常管理及操作流程、外包服务机构与外部合作机构管理、内外部检查及监督机制、应急处理流程和预案、投诉与申诉处理程序机构的相关要求。	符合	
	应明确个人金融信息保护责任人和个人金融信息保护有关责任机构，并明确工作职责及工作流程。	申请机构建立个人金融信息保护制度体系《冰鉴科技-数据安全管理办法》，在制度第三章机构与人员章节明确了信息保护责任人和责任机构，并明确工作职责及工作流程。	符合	
	应定期（至少每年一次）或在隐私政策发生重大变化时，对个人金融信息处理岗位上的相关人员开展个人金融信息安全专业化培训和考核，确保相关人员熟练掌握隐私政策和相关规程。	在《冰鉴科技-数据安全管理办法》第三章机构与人员章节中的第十条人员培训中描述了建立数据安全教育培训制度，针对新员工开展入职安全教育培训，针对全体员工每半年至少开展一次数据安全教育培训，培训内容包括但不限于数据安全管理与用户个人信息保护相关法律法规、标准制度、安全责	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
		任、知识技能等。		
访问控制	应对个人金融信息使用的权限管理应设置权限指派、回收、过期处理等安全功能。	《冰鉴科技-数据安全管理办法》第五章数据全生命周期安全管理章节中第四节数据使用和第五节数据共享中对数据使用和共享进行了要求，数据使用和共享时要经过授权、严格审批，并要对数据实施脱敏。	符合	
	对于可访问和处理个人金融信息的系统应设置基于角色的访问控制策略，对系统用户个人金融信息的增删改查等操作进行记录，保证操作日志的完备性、可用性及可追溯性，操作日志包括但不限于业务操作日志、系统日志等，并要求系统运维管理类日志不应记录个人金融信息。	申请机构对于可访问和处理个人金融信息的系统设置基于角色的访问控制策略，在后台服务器记录了系统操作日志信息，日志信息中的涉及个人金融信息均已加密显示，但系统中暂未有日志管理功能，建议平台增加日志管理功能。	部分符合	BJKJ-002
监测评估	应定期对涉及个人金融信息的信息系统进行安全检查和评估，特别是对于个人金融信息中的支付信息部分，应采取自行评估或委托外部机构进行检查评估，本机构以及与其合作的外部合作方（包括外包服务机构、外部合作机构）应每年至少开展一次支付信息安全合规评估，对评估过程中发现的问题及时采取补救措施并形成报告存档备查。	《冰鉴科技-数据安全管理办法》第四章数据安全基础管理第四节数据安全评估中规定了定期（至少每年开展一次）及在数据安全管理环境发生重大变更时，对数据安全管理情况开展合规性评估。具有《冰鉴科技-金融科技应用内部审计报告》、《冰鉴科技-安全事件应急演练记录》、《冰鉴科技-网络安全漏洞定期扫描记录》。	符合	
	应采取技术手段对个人金融信息全生命周期进行安	基于多方安全计算的差异化营销平台部署	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
	全风险识别和管控，如恶意代码检测、异常流量监测、用户行为分析等。	在阿里云上，采用了阿里云的 web 应用防护（WAF）高级版，对平台业务流量进行多维度检测和防护，阻挡诸如 SQL 注入或跨站脚本等常见攻击，避免这些攻击影响平台的可用性、安全性或过度消耗资源，降低数据被篡改、失窃的风险，同时带有网页防篡改的功能，对网页发生篡改时提供报警，并利用网页镜像进行及时恢复。		
事件处置	应制定个人金融信息安全事件应急预案，明确安全事件处置流程和岗位职责，并定期组织内部相关人员进行个人金融信息保护应急预案相关培训和应急演练。	申请机构建立了《冰鉴科技-数据安全管理办法》和《冰鉴科技-数据安全应急演练方案》，在制度中明确安全事件处置流程和岗位职责，并定期组织内部相关人员进行个人金融信息保护应急预案相关培训和应急演练，具有安全事件应急演练记录和个人信息安全预案培训记录。	符合	
	应建立投诉与申诉管理机制，包括跟踪流程，并在规定的时间内，对投诉、申诉进行响应。	申请机构建立了投诉与申诉管理机制，在《冰鉴科技-数据安全管理办法》第四章数据安全基础管理第七节投诉处理章节中描述了投诉渠道应至少包括以下一种：电子邮件、电话、传真、在线客服、在线表格，并针对有效投诉线索依法依规开展处置和记录，自接到投诉之日起十	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
		五日内答复投诉人。		

4.6 网络安全

4.6.1 基本安全要求

测评对象	测评指标	结果记录	结果判定	问题编号
业务影响分析	申请机构应按照 GB/T 22240 进行定级，并满足 JR/T 0071 中对应等级的要求。	基于多方安全计算的差异化营销平台部署在阿里云上，阿里云已通过等保测评，另申请机构具有同环境的个人反欺诈评估服务系统等级保护测评报告，但是暂未有基于多方安全计算的差异化营销平台的等级保护测评报告。	不符合	BJKJ-003

4.6.2 安全防护要求

测评对象	测评指标	结果记录	结果判定	问题编号
仿冒钓鱼	APP 安装、启动、更新时应对自身的完整性和真实性进行校验，具备抵御篡改、替换或劫持的能力。	申请机构不涉及客户端应用软件，故此项不适用。	不适用	
	APP 应具备基本的抗攻击能力，能抵御静态分析、动态调试等操作。	申请机构不涉及客户端应用软件，故此项不适用。	不适用	
	申请机构的客户端代码应使用代码加壳、代码混淆、检测调试器等手段对客户端应用软件进行安全保护。	申请机构不涉及客户端应用软件，故此项不适用。	不适用	
	申请机构应采取渠道监控等措施对仿冒客户端程序进行监测	申请机构不涉及客户端应用软件，故此项不适用。	不适用	
	申请机构网站应具有防网络钓鱼的安全提示功能，例	基于多方安全计算的差异化营销平台采用	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
	如显示客户预留信息、客户自定义个性化界面等。	HTTPS 安全加密通道，平台部署在阿里云上，采用了阿里云的web应用防护（WAF）高级版，对平台业务流量进行多维度检测和防护，阻挡诸如SQL注入或跨站脚本等常见攻击，避免这些攻击影响平台的可用性、安全性或过度消耗资源，降低数据被篡改、失窃的风险，同时带有网页防篡改的功能，对网页发生篡改时提供报警，并利用网页镜像进行及时恢复。		
	申请机构应具备钓鱼攻击监测能力，例如增加客户端提交的页面来源地址信息的校验、设置转账白名单等。	基于多方安全计算的差异化营销平台采用HTTPS 安全加密通道，平台部署在阿里云上，采用了阿里云的web应用防护（WAF）高级版，对平台业务流量进行多维度检测和防护，阻挡诸如SQL注入或跨站脚本等常见攻击，避免这些攻击影响平台的可用性、安全性或过度消耗资源，降低数据被篡改、失窃的风险，同时带有网页防篡改的功能，对网页发生篡改时提供报警，并利用网页镜像进行及时恢复。	符合	
	申请机构应采取防钓鱼网站控件、钓鱼网站监控工具、钓鱼网站发现服务等技术措施，及时监测发现钓鱼网站，并建立钓鱼网站案件报告及快速关闭钓鱼网站的处置机制	基于多方安全计算的差异化营销平台部署在阿里云上，阿里云运维平台可以对系统业务量、资源、异常行为、攻击行为进行监控和预警，当存在风险和异	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
		常情况时阿里云平台会发送预警邮件。		
安全漏洞管理	申请机构应考虑交易处理功能逻辑设计的合理性，避免逻辑漏洞。	申请机构对系统交易处理功能逻辑设计的合理性进行了内部评审，并具有《冰鉴科技-技术选型报告》。	符合	
	申请机构应避免调用存在安全漏洞的函数、组件。	申请机构对调用的函数库、组件进行了评估，具有《冰鉴科技-技术选型报告》。	符合	
	申请机构应进行开源系统或组件的安全评估，及时进行漏洞修复和加固处理。	申请机构会定期对开源系统或组件开展漏洞扫描，具有《冰鉴科技-网络安全漏洞定期扫描记录》。	符合	
	申请机构应在设计和开发阶段避免网站、客户端、SDK、API 等存在常见漏洞，包括但不限于穷举尝试漏洞、重放漏洞、注入漏洞、跨站脚本漏洞、文件上传下载漏洞、缓冲区溢出漏洞、非法提权漏洞、逆向工程漏洞等。	申请机构在设计和开发阶段会进行程序代码的源码审计和应用漏洞扫描，具有《冰鉴科技-系统源代码安全审计报告》和《华为云漏洞扫描服务安全报告》。	符合	
	申请机构应在金融科技创新应用上线前进行源代码安全审计、渗透测试，及时处理安全漏洞，有效控制安全风险。	申请机构在金融科技创新应用上线前进行源代码安全审计，具有《冰鉴科技-系统源代码安全审计报告》，但暂未进行渗透测试。	部分符合	BJKJ-004
	申请机构应对金融科技创新应用进行定期及变更时的漏洞扫描，及时修补发现的系统安全漏洞。	申请机构对金融科技创新应用定期及变更时会通过工具对系统开展漏洞扫描，具有《华为云漏洞扫描服务安全报告》。	符合	
	申请机构应建立紧急补丁（应急方案）的开发、发布流程，以备必要时提供紧急补丁或应急方案进行处理，	申请机构建立了紧急补丁（应急方案）的开发、发布流程《冰鉴科技-安全补丁管理流	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
	以修补重要安全漏洞。	程》。		
网络攻击防护	申请机构应对客户端软件、网站、API 和 SDK 的常见网络攻击，包括但不限于穷举登录尝试、重放攻击、注入攻击、跨站脚本攻击、文件上传下载攻击、非法提权、逆向工程等，进行监测、识别和阻断。	基于多方安全计算的差异化营销平台部署在阿里云上，采用了阿里云的 web 应用防护（WAF）高级版，对平台业务流量进行多维度检测和防护 。	符合	
	申请机构宜针对设备、IP、账号等建立关联关系，利用社群发现、风险传播等方式精准防御团伙欺诈行为。	基于多方安全计算的差异化营销平台部署在阿里云上，阿里云云安全中心配置设备常用登录地、常用登录账号策略，防止异地异账号登录。	符合	
	申请机构宜基于用户行为频率、属性聚集等特征，针对批量或高频登录等异常行为，例如异常登录、注册、邀请好友、提现下单，利用 IP 地址、终端设备标识等信息进行综合识别，及时采取附加验证、拒绝请求等手段降低安全隐患。	基于多方安全计算的差异化营销平台部署在阿里云上， 并基于 IP、用户账号、登录时间、登录行为的分析系统能准确判断是否爬虫还是正常用户登录，对非正常 IP 进行短时间封禁。 目前平台没有账户登录失败处理功能，建议增加登录失败次数锁定功能。	部分符合	BJKJ-005
安全事件管理	申请机构对于重大信息安全事件，相关人员应注意保护事件现场，采取必要的控制措施。	申请机构具备重大信息安全事件的处置措施，在《冰鉴科技-数据安全管理文档》1.9 安全事件管理制度章节明确了相关人员应注意保护事件现场，采取必要的控制措施。	符合	
	申请机构应定期对本机构及同业发生的信息安全事件及风险进行深入研判、分析，评估现有控制措施的脆	申请机构定期对本机构及同业发生的信息安全事件及风险进行深入研判、分析，评估	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
	弱性，及时整改发现的问题。	现有控制措施的脆弱性，及时整改发现的问题，在《冰鉴科技-数据安全管理文档》进行了阐述，并具有《信息安全事件风险研判记录》		

4.7 内控管理

测评对象	测评指标	结果记录	结果判定	问题编号
技术管理	申请机构应有效研判新技术在金融业务的应用价值，正确进行新技术选型。	申请机构提供了《冰鉴科技-技术选型报告》，报告中第一章节描述了多方安全计算在业务的价值，正确进行了新技术选型。	符合	
	申请机构应审慎选择新技术，进行新技术应用风险评估，避免过度采用未成熟的新技术。	申请机构提供了《冰鉴科技-技术选型报告》，文档中对新技术应用风险进行了描述，并对多方安全计算的必要性和可行性进行了描述。	符合	
	申请机构应对技术复杂性与金融业务复杂性进行关联分析，提高缺陷及时识别的能力。	申请机构提供了《冰鉴科技-技术选型报告》，文档中对技术复杂性与金融业务复杂性进行了关联分析，并提供了解决方案-流式通信机制，提高了缺陷及时识别的能力。	符合	
	申请机构应建立第三方技术、组件或产品的管理清单，明确记录提供方、版本等信息。	申请机构提供了第三方产品清单及更新记录，明确了提供方、产品、日期等信息。	符合	
	申请机构应跟踪第三方技术、组件或产品的更新情况，及时甄别版本变化带来的影响。	申请机构提供了第三方产品清单及更新记录，包含提供方、更新日期及更新记录等信	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
		息。		
	申请机构应与第三方技术、组件或产品的供应商明确安全责任，建立有效的风险联动机制。	申请机构与第三方供应商签订了合同协议，协议中明确了各方的责任和义务；经访谈技术主管，申请机构与第三方建立了有效的风险联动机制，发生风险时，双方会共同进行风险处置。	符合	
	申请机构应结合当前的法规政策、标准规范、应用模式、服务产品、信息系统支撑等方面，结合自身工作基础，说明金融科技创新应用的必要性、可行性。	申请机构提供了《冰鉴科技-技术选型报告》，第二章节描述了多方安全计算的必要性与可行性；申请机构提供了《金融科技创新应用声明书》，文档中对多方安全计算的创新性进行了描述。	符合	
	申请机构应对金融科技创新应用的具体目标、预期效果提出可量化的指标。	申请机构提供了《金融科技创新应用声明书》，预期规模章节包含了“按照风险可控原则合理确定用户范围和服务规模，预计年营销查询达到 5 万次。”的描述。	符合	
	申请机构应明确金融科技创新应用的业务功能、服务对象、预期用户规模和应用模式，说明金融科技应用采用的主要技术。	申请机构提供了《金融科技创新应用声明书》，技术应用章节描述了金融科技应用采用的主要技术。	符合	
	申请机构应监控金融科技创新应用运行的状态、资源耗用情况、异常报警情况等。	经访谈申请机构技术负责人，申请机构使用云厂商自带的监控插件及机构搭建的 Prometheus+grafana 对服务器资源利用情况进行监控，使用 elasticsearch+flume +kibana 对应用运行状	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
		态进行监控；服务器状态异常或应用状态异常时，会通过钉钉和企业微信进行告警。		
	申请机构应在监控管理、日志管理等方面提供相应的功能，保障新技术应用过程可回溯、可监控、可审计。	申请机构使用 elasticsearch+flume+kibana 对应用运行状态进行监控，该 EFK 采集系统和应用日志，具有监控管理、日志管理功能，可进行日志审计。	符合	
	申请机构应制定可行有效的新技术回退、中止方案。	申请机构提供了《冰鉴科技-技术选型报告》，“新技术回退、中止方案”章节描述了回退、中止方案，经访谈技术主管，技术回退、中止方案可以有效执行。	符合	
风险控制	申请机构应采用科学的风险管理技术和方法，充分识别和评估金融科技创新应用面临的风险，对各类主要风险进行持续监控。	申请机构提供了《冰鉴科技-技术选型报告》，文档对应用风险评估与监控方案进行了描述；经访谈申请机构技术负责人，申请机构使用云厂商自带的监控插件及机构搭建的 Prometheus+grafana 对服务器资源利用情况进行监控，使用 elasticsearch+flume+kibana 对应用运行状态进行监控。	符合	
	申请机构应做好新技术金融应用风险防范，建立健全试错容错机制，完善风险拨备资金、保险计划、应急处置等风险补偿措施。	申请机构提供了《基于多方安全计算的差异化营销平台风险补偿机制》、《基于多方安全计算的差异化营销平台退出机制》、《基于多方安全计算的差异化营销平台应急预	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
		案》，建立建全了试错容错机制，完善了风险拨备资金、保险计划、应急处置等风险补偿措施。		
	申请机构应建立健全客户投诉处理机制，制定金融科技创新应用的投诉处理工作流程，定期汇总分析投诉反映事项，查找问题，有效改进服务和管理。	申请机构提供了《冰鉴科技-客户投诉及申诉制度》，包含了客户投诉处理机制及投诉处理工作流程，申请机构及其各级分支机构做好金融消费者投诉统计、分析工作，并每半年形成报告。	符合	
内控保障	申请机构应建立健全内部控制制度体系，为金融科技创新应用制定全面、系统、规范的管理制度和业务流程，并定期进行评估。	申请机构制定了《金融科技创新应用管理制度及工作组织机制》，制度对金融科技应用创新、实施、管理过程进行了描述，但暂未制定定期评估相关流程。	部分符合	BJKJ-006
	申请机构应明确金融科技创新应用的工作组织机制，明确工作负责人。金融科技创新应用由多个机构共同开发、运营时，应指定牵头负责单位，建立工作协调机制、联合运营机制、问题协同处理机制等控制措施。	申请机构制定了《金融科技创新应用管理制度及工作组织机制》，制度中对各部门职责进行了说明，但未指定牵头负责部门，且未建立工作协调机制、联合运营机制、问题协同处理机制等控制措施。	部分符合	BJKJ-007
	申请机构应定期开展金融科技应用内部审计	申请机构制定了《金融科技应用内部审计制度》，制度中明确内部审计原则上每年进行一次，由内部审计管理小组制定《内部审计计划》，经 CEO 批准后实施；申请机构金融科技应用上线前进行了内部审计，并提供了《冰鉴科技-金融科技应用	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
		内部审计报告》。		
	应当建立内部控制问题整改机制，明确整改责任部门，规范整改工作流程，确保整改措施落实到位。	申请机构提供了《冰鉴科技-内部控制问题整改机制》，人事行政部负责归口管理纠正/预防措施实施，组织相关部门制定纠正/预防措施，并负责跟踪验证，确保整改措施落实到位。	符合	

5. 评估总结

5.1 评估过程描述

针对上海冰鉴信息科技有限公司基于多方安全计算的差异化营销平台产品，按照 JR/T 0199-2020《金融科技创新安全通用规范》要求，在上海冰鉴信息科技有限公司搭建的检测环境中进行了全面的检测，此次检测内容主要包括交易安全、服务质量、业务连续性、算法安全、数据安全、网络安全、内控管理等七个方面，并得出了相关的检测结果，但对于升级、与软硬件环境关系密切和没有检测到的业务等不在此次检测说明范围内。

5.2 评估总结

根据 JR/T 0199-2020《金融科技创新安全通用规范》判定结果如下：

交易安全检测：共包含 22 个检测项，不存在判定结果为“符合”、“部分符合”、“不符合”的项，判定结果为“不适用”的有 22 项。

服务质量检测：共包含 5 个检测项，实际检测 5 个检测项，判定结果为“符合”的有 5 项，不存在判定结果为“部分符合”、“不符合”、“不适用”的项。

业务连续性检测：共包含 27 个检测项，实际检测 27 个检测项，判定结果为“符合”的有 27 项，不存在判定结果为“部分符合”、“不符合”、“不适用”的项。

算法安全检测：共包含 26 个检测项，实际检测 26 个检测项，判定结果为“符

合”的有 26 项，不存在判定结果为“部分符合”、“不符合”、“不适用”的项。

数据安全检测：共包含 42 个检测项，实际检测 24 个检测项，判定结果为“符合”的有 22 项，判定结果为“部分符合”的有 1 项，判定结果为“不符合”的有 1 项，判定结果为“不适用”的有 18 项。

网络安全检测：共包含 20 个检测项，实际检测 16 个检测项，判定结果为“符合”的有 13 项，判定结果为“部分符合”的有 2 项，判定结果为“不符合”的有 1 项，判定结果为“不适用”的有 4 项。

内控管理检测：共包含 19 个检测项，实际检测 19 个检测项，判定结果为“符合”的有 17 项， 判定结果为“部分符合”的有 2 项，不存在判定结果为“不符合”、“不适用”的项。

本次技术性安全评估共包含 161 个检测项，实际检测 117 个检测项，其中判定结果为“符合”的有 110 项，判定结果为“部分符合”的有 5 项，判定结果为“不符合”的有 2 项，判定结果为“不适用”的有 44 项。

具体检测情况及结果如下表所示：

序号	检测项						
	名称	检测项	实际检测项	符合项	部分符合项	不符合项	不适用项
1	交易安全	22	0	0	0	0	22
2	服务质量	5	5	5	0	0	0
3	业务连续性	27	27	27	0	0	0
4	算法安全	26	26	26	0	0	0
5	数据安全	42	24	22	1	1	18
6	网络安全	20	16	13	2	1	4
7	内控管理	19	19	17	2	0	0
综合		161	117	110	5	2	44

5.3 问题列表

问题编号	问题描述	测评对象	整改情况
BJKJ-001	申请机构基于多方安全计算的差异化营销平台只涉及后台操作人员、管理人员的手机号码个人金融信息展示，但目前系统上暂未对上述手机号码进行屏蔽展示。 补偿机制：申请机构承诺 6 个月内完成基于多方安全计算的差异化营销平台的手机号码屏蔽改造。	数据安全	限期整改
BJKJ-002	系统中暂未有日志管理功能，建议平台增加日志管理功能。 补偿措施：申请机构承诺 6 个月内完成日志管理功能的建设。	数据安全	限期整改
BJKJ-003	暂未有基于多方安全计算的差异化营销平台的等级保护测评报告。 补偿措施：申请机构承诺 6 个月内完成基于多方安全计算的差异化营销平台的等级保护测评。	网络安全	限期整改
BJKJ-004	暂未对基于多方安全计算的差异化营销平台进行渗透测试。 补偿措施：申请机构承诺在 6 个月内对产品进行渗透测试。	网络安全	限期整改
BJKJ-005	目前平台没有账户登录失败处理功能，建议增加登录失败次数锁定功能。 补偿措施：申请机构承诺在 6 个月内完成账户登录失败处理功能的建设。	网络安全	限期整改
BJKJ-006	申请机构制定了《金融科技创新应用管理制度及工作组织机制》，制度对金融科技应用创新、实施、管理过程进行了描述，但暂未制定定期评估相关流程。 补偿措施：申请机构承诺在 6 个月内补充金融科技应用创新、实施、管理制度，制定定期评估流程。	内控管理	限期整改
BJKJ-007	申请机构制定了《金融科技创新应用管理制度及工作组织机制》，制度中对各部门职责进行了说明，但未指定牵头负责部门，且未建立工作协调机制、联合运营机制、问题协同处理机制等控制措施。 补偿措施：申请机构承诺在 6 个月内完善《金融科技创新应用管理制度及工作组织机制》，指定牵头负责部门，建立工作协调机制、联合运营机制、问题协同处理机制等控制措施。	内控管理	限期整改

6. 附件

无。

附件 1-4

基于多方安全计算的差异化营销平台风险补偿机制

3AUVJ6GCPTZ4

本项目按照由上海冰鉴信息科技有限公司与南京银行股份有限公司上海分行双方联合制定的风险补偿方案，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，配套风险拨备资金、保险计划等补偿措施，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：

一、基于相关政府部门的监管要求进行综合评估，明确风险责任认定方式和流程。建立切实有效的客户风控补偿机制，基于项目中由参与各方共同提供的服务，建立相关方的权责认定、风险防范和处理机制，保障客户合法权益。

二、如相关业务出现违约风险，客户可通过南京银行上海分行官方网站公布的客服电话提出投诉意见或书面风险补偿诉求。

三、南京银行上海分行将按照国家法律法规及与客户的协议约定，在受理投诉意见后，迅速核实情况，与客户积极协商，确认所承担责任和应履行义务，形成反馈意见，主动联系客户，友好协商解决投诉或争端，积极主动对客户进行赔付，保障客户合法权益。

四、若因技术缺陷，导致客户合法权益面临损害的事项发生，

项目参与各方将依据相关法律法规积极协商，确定最为高效的问题解决方式，切实将客户合法权益面临的损害风险降至最低。

附件：1-5

基于多方安全计算的差异化营销平台退出机制

3AUVI6GCPTZ4

本项目按照由上海冰鉴信息科技有限公司与南京银行股份有限公司上海分行双方联合制定的退出机制，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、业务退出。冰鉴科技在南京银行上海分行暂停“基于多方安全计算的差异化营销平台”运营前，应当配合南京银行上海分行提前以书面、短信、电话等多种形式告知客户，并承担合作终止产生的风险和责任。

二、技术退出。回收“基于多方安全计算的差异化营销平台”的系统资源，平稳完成技术退出。

三、数据处理。完成“基于多方安全计算的差异化营销平台”的业务数据、交易数据等数据库归档备份，将数据同步到相关业务系统，确保用户其他业务不受影响。

附件 1-6

基于多方安全计算的差异化营销平台应急预案

3AUVJ66CPT74

本项目按照由上海冰鉴信息科技有限公司与南京银行股份有限公司上海分行双方联合制定的应急处置预案，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。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。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、在系统上线前进行测试及容灾演练，针对应急情况提前培训处置措施；在系统上线后定期开展突发事件处置演练。

二、上线前对系统运维情况开展全方位评估，上线后定期进行运维再评估，确保运维能力稳定。

三、建立监控预警，及时发现业务、技术的异常情况，并配

备应急事件处理工作组，按照应急事件特点，实时启动应急响应，保障平台安全稳定地为客户服务。

四、对于突发事件，根据其影响范围和危害程度，进行风险分级，及时启动应急预案，切实保障客户信息安全。