《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	914100001699995779-2023-0001	
	创新应用名称	基于大数据技术的反电信网络诈骗服务	
	创新应用类型	金融服务	
	机构信息	统一社会信用代码	914100001699995779
		全球法人识别编码	300300C1085141000016
		机构名称	郑州银行股份有限公司
		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：B1036H241010001 发证机关：国家金融监督管理总局河南监管局
	拟正式运营时间	2024 年 03 月 14 日	
	技术应用	1. 运用大数据技术，依托客户充分授权的行内数据（客户信息、账户信息、交易数据、黑名单数据）以及来源合规的第三方数据（制裁类、通缉类名单数据），建立对私、对公渠道反电信网络诈骗规则和模型，形成了事中和事后监控的全方位风险防御能力。 2. 运用流式计算技术，对实时交易数据进行分析处理，事中规则实时识别可疑交易，提高风险预警的时效性。 3. 基于分布式微服务架构，将数据处理、规则分析、模型计算、名单管理、账户核查等功能模块独立部署、运行及维护，有效降低各功能服务间的耦合性，提升维护效率。	
	功能服务	本应用综合运用大数据、流式计算、分布式微服务等技术，通过建立事中风控规则，实时识别可疑账户，下发分支行排查。并通过建立事后风控模型，每日对账户进行跑批，实现事后识别可疑账户下发分支行排查，事中和事后监控相辅相成，全方位识别电信网络诈骗风险，与分支机构快速有效的进行账户核查及管控。 本应用由郑州银行股份有限公司负责研发及运维，并提供金融应用场景，此外无第三方机构参与。	
	创新性说明	1. 数据融合应用方面，在行内客户信息、交易数据等基础上，通过引入外部名单类数据，丰富银行对账户的电信网络诈骗风	

		险评估的数据维度。 2. 风控能力方面，通过建立风控规则和模型的方式，形成事中和事后两种风控模式，全面提升银行对电信网络诈骗风险的监测能力，精准识别涉诈账户。 3. 业务效率方面，对识别出的疑似涉诈风险账户提供排查-管控-反馈的一站式服务，提升行内对风险账户管控效率。 4. 运行维护方面，基于分布式微服务架构灵活部署优势，可以对单个微服务进行快速维护部署，而不会影响其它微服务运行使用，有效降低升级维护带来的影响。
	预期效果	涉诈风险的排查效率得到提升，降低需要人工排查介入的工作量，涉诈风险类账户从挖掘、确认、再到处置的时间周期明显缩短，识别精确度有所提升。
	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，预计平台每天对约 33 万账户进行监测。
创新应用服务信息	服务渠道	线下渠道：ATM 线上渠道：PC 端服务平台、移动端 App、其他支付平台
	服务时间	7×24 小时
	服务用户	郑州银行个人和企业客户
	服务协议书	《郑州银行办理“企业对公账户、银行卡”承诺书》（见附件 1-1）
合法合规性评估	评估机构	郑州银行股份有限公司法律合规部
	评估时间	2023 年 11 月 13 日
	有效期限	3 年
	评估结论	本应用严格按照《中华人民共和国网络安全法》《中华人民共和国反洗钱法》《中华人民共和国数据安全法》《中华人民共和国反电信网络诈骗法》《中华人民共和国个人信息保护法》《中华人民共和国消费者权益保护法》《金融机构大额交易和可疑交易报告管理办法》（中国人民银行令〔2016〕第 3 号发布）、《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）、《金融机构反洗钱和反恐怖融资监督管理办法》（中国人民银行令〔2021〕第 3 号发布）、《中国人民银行关于加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》（银发〔2016〕261 号）、《中国银保监会办公厅关于印发银行保险机构信息科技外包风险监管办法的通知》（银保监办发〔2021〕141 号）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。

		经评估，本应用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-基于大数据技术的反电信网络诈骗服务》（见附件 1-2）		
技术安全性评估	评估机构	郑州银行股份有限公司信息科技部		
	评估时间	2023 年 11 月 8 日		
	有效期限	2 年		
	评估结论	本应用严格按照《计算机软件检测规范》(GB/T 15532-2008)、《信息安全技术信息安全漏洞管理规范》(GB/T 30276-2013)、《信息安全技术网络安全漏洞分类分级指南》(GB/T 30279-2020)、《信息安全技术应用软件安全编程指南》(GB/T 38674-2020)、《信息安全技术信息系统密码应用基本要求》(GB/T 39786-2021)、《银行业软件测试文档规范》(JR/T 0101-2013)、《网上银行系统信息安全通用规范》(JR/T 0068-2020)、《金融网络安全 Web 应用服务安全测试通用规范》(JR/T 0213-2021)、《银行互联网渗透测试指南》(JR/T 0232-2021)、《移动金融客户端应用软件安全检测规范》(TPCAC 0007-2020)、《PTES-渗透测试执行标准》、《金融领域科技伦理指引》（JR/T 0258—2022）等相关金融行业技术标准规范要求进行设计开发并进行全面安全评估。 经评估，本应用符合现有相关行业标准要求。		
	评估材料	《技术安全性评估报告-基于大数据技术的反电信网络诈骗服务》（见附件 1-3）		
风险防控	风控措施	1	风险点	在数据采集、存储、传输、使用等过程，由于技术缺陷或业务管理漏洞可能会造成数据的泄露风险。
			防范措施	确保数据安全管理和使用。基于国家法律法规对于公民隐私权和数据使用的规定，对系统管理员进行培训，对权限严格控制，保障客户合法权益不受侵害，防止发生客户信息泄露事件。
		2	风险点	创新应用上线运行后，可能面临网络攻击，系统宕机，亟需采取措施加强风险监控预警与处置。
			防范措施	在实施过程中，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，保障系统安全稳定运行，保护金融消费者合法权益。
		3	风险点	随着时间的推移，新的欺诈手段会出现，涉诈账户的风险特征发生变化，当前风控模型的欺诈识别效果可能会降低。
			防范	一是对规则模型进行监控，模型效果定时进行分析，及时进行模型迭代，避免模型准确性问题影响

			措施	风险识别效果。二是对客户可能造成的影响做好解释工作，在有效保障客户合法权益的前提下，完成风险交易的核查处置。
	风险补偿机制	本应用建立风险补偿方案（见附件 1-4），建立健全风险补偿机制，客户可通过营业网点、客服电话、门户网站等渠道提出投诉意见及诉求。郑州银行股份有限公司将积极受理，核实情况，确认银行所承担责任，及时联系客户，与客户进行沟通调解，最大程度保障消费者的合法权益。		
	退出机制	本应用建立退出机制（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。郑州银行股份有限公司按照预定退出方案进行平稳终止，对平台相关数据进行处理，切实保障金融用户数据安全。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。切实保障消费者权益。		
	应急预案	本应用建立应急处置预案（见附件 1-6），妥善处理突发安全事件，切实保障系统稳定运行。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。		
投诉响应机制	机构投诉	投诉渠道	1. 营业网点：向郑州银行辖内各营业网点客户经理、网点负责人反映问题和诉求。 2. 客服电话：请致电郑州银行客户服务热线（95097），选择人工服务联系客服代表。 3. 门户网站：可在郑州银行门户网站（www.zzbank.cn）在线客服进行在线留言。	
		投诉受理与处理机制	受理部门：郑州银行股份有限公司反洗钱与反诈中心 受理时间：周一至周五（工作日） 上午 8:30-11:30 下午 14:00-17:30 处理流程：在接到投诉事件后，受理人员负责对事件进行了解和分析，在确认投诉原因和相关问题后，协调相关业务或技术部门进行处理解决。 处理时限：7 个工作日	
	自律投诉	投诉渠道	受理机构：中国互联网金融协会 投诉网站： https://tousu.nifa.org.cn 投诉电话：400-800-9616	

			投诉邮箱： fintech_support@nifa.org.cn
		投诉受理 与处理机制	中国互联网金融协会是经党中央、国务院同意，按照人民银行、银监会、证监会、保监会、工信部、公安部、工商总局等 10 部委联合发布的《关于促进互联网金融健康发展的指导意见》（银发〔2015〕221 号）要求， 由中国人民银行会同银监会、证监会、保监会等国家有关部委组织建立的国家级互联网金融行业自律组织。为保护金融消费者合法权益，营造守正、安全、普惠、开放的金融科技创新发展环境，协会按照金融管理部门相关要求建立健全消费者投诉处理机制。 对于涉及相关地区的金融科技创新应用的争议、投诉事项，协会接收投诉意见后，由相关部门依程序进行处置，并接受金融管理部门监督审查。 联系方式：400-800-9616 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[1]	本机构承诺所提交的材料真实有效，遵守国家相关法律法规规定和社会公序良俗，严格落实金融管理部门相关监管要求，认真执行行业相关规则规范，强化全流程风控管理体系建设，有效识别、评估、监测和控制风险，并做出以下声明： 1.守正创新。忠实履行金融天职和使命，着力解决实体经济痛点难点，确保科技创新不偏离正确的发展方向，严防技术滥用，切实通过技术创新满足人民群众对美好生活的期待与向往。 2.以人为本。始终坚持以人民为中心的发展思想，坚持金融科技创新行为从人民群众实际需求出发，以增进社会共同福祉为目标，尊重并维护人民群众尊严		

[1] 科技产品类创新应用，若未能在公示前获得外部权威专业机构出具的标准符合性证明材料，还应承诺“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。”

	和利益，致力促进社会和谐与文明进步。 3. 诚实守信。恪守社会主义核心价值观，将求真务实作为金融科技从业人员的基本素养，将履约践诺作为从事金融科技活动的基本要求，强化诚信道德自律，积极倡导诚实守信的良好社会风尚。 4. 公开透明。使用简明清晰、通俗易懂的方式，及时、真实、准确、完整地主动对外披露金融科技创新的功能实质和潜在风险，不隐瞒不利信息、不“劝诱”销售产品，让社会公众看得到、读得懂、能监督。 5. 权益保护。充分尊重和保障人民群众隐私权、自主选择权、依法求偿权等合法权益，严格履行适当性义务，严防过度采集、违规使用、非法交易和泄露用户隐私数据行为，采取风险拨备资金、保险计划等补偿机制，切实保护用户资金和信息安全。 6. 安全合规。把遵守法律法规和维护金融稳定作为开展金融科技创新活动的前提条 件，已通过业务合规性和技术安全性评估审计等措施保障新技术应用风险可控，避免新技术应用带来的数据泄露、算法黑箱、信息茧房等问题，切实防范技术和数据滥用可能导致的人民群众信息与资金失窃风险。 7. 公平普惠。应用新一代信息技术优化金融服务供给结构，持续增强金融服务的普适性、可得性和满意度。重点关注特殊人群、弱势群体需求，努力消除因使用成本、文化程度、地域限制等造成的“数字鸿沟”，不断提升人民群众的获得感、幸福感、安全感。 8. 社会责任。贯彻落实国家战略部署，围绕新时代经济社会发展的战略目标、战略重点，始终把社会效益放在首位，坚持社会效益和经济效益相统一，开展“负责任的创新”，打造“值得信赖的技术”，切实服务经济社会健康可持续发展。 本声明书正文与附件表述不一致的，以正文为准。 以上承诺如有违反，愿承担相应责任与后果。 法定代表人或其授权人（签字）：2023 年 11 月 13 日（盖章）

附件 1-1

办理“企业对公账户、银行卡”承诺书（模板）

电信网络诈骗犯罪是严重影响人民群众合法权益、破坏社会和谐稳定的社会毒瘤，必须坚决依法严惩。利用非法收购的对公账户、个人银行卡获取和转移诈骗所得的财产是犯罪分子常用的手段。为配合公安机关严厉打击治理电信网络诈骗犯罪，我承诺如下：

经公安机关、开户银行告知，我已知悉擅自将本人办理的企业对公账户、个人银行卡、绑定的手机卡、U 盾等无偿转让、有偿提供或买卖本人工商营业执照、企业对公账户、个人银行卡的行为被法律所禁止，任何人违反都将受到法律制裁。

我承诺，我办理的企业对公账户、个人银行卡、绑定的手机卡、U 盾真实地用于个人的公司经营和合法资金往来。本人已认真阅读且理解上述内容的含义，并愿意承担相关法律责任。

承诺人：

年　　月　　日

备注:承诺人签字并按压拇指手印

附件 1-2

基于大数据技术的反电信网络诈骗服务合法合规性评估报告

本应用严格按照《中华人民共和国网络安全法》《中华人民共和国反洗钱法》《中华人民共和国数据安全法》《中华人民共和国反电信网络诈骗法》《中华人民共和国个人信息保护法》《中华人民共和国消费者权益保护法》《金融机构大额交易和可疑交易报告管理办法》（中国人民银行令〔2016〕第 3 号发布）、《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）、《金融机构反洗钱和反恐怖融资监督管理办法》（中国人民银行令〔2021〕第 3 号发布）、《中国人民银行关于加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》（银发〔2016〕261 号）、《中国银保监会办公厅关于印发银行保险机构信息科技外包风险监管办法的通知》（银保监办发〔2021〕141 号）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。

经评估，本应用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。

郑州银行股份有限公司

2023 年 11 月 13 日

附件 1-3

基于大数据技术的反电信网络诈骗服务技术安全性评估报告

本应用严格按照《计算机软件检测规范》(GB/T 15532-2008)、《信息安全技术信息安全漏洞管理规范》(GB/T 30276-2013)、《信息安全技术网络安全漏洞分类分级指南》(GB/T 30279-2020)、《信息安全技术应用软件安全编程指南》(GB/T 38674-2020)、《信息安全技术信息系统密码应用基本要求》(GB/T 39786-2021)、《银行业软件测试文档规范》(JR/T 0101-2013)、《网上银行系统信息安全通用规范》(JR/T 0068-2020)、《金融网络安全 Web 应用服务安全测试通用规范》(JR/T 0213-2021)、《银行互联网渗透测试指南》(JR/T 0232-2021)、《移动金融客户端应用软件安全检测规范》(TPCAC 0007-2020)、《PTES-渗透测试执行标准》等相关金融行业技术标准规范要求进行设计开发并进行全面安全评估。

经评估，本应用符合现有相关行业标准要求。

郑州银行股份有限公司

2023 年 11 月 8 日

附件 1-4

基于大数据技术的反电信网络诈骗服务风险补偿机制

本应用建立风险补偿方案，建立健全风险补偿机制，充分保障消费者合法权益。

具体机制如下：

客户可通过营业网点、客服电话、门户网站等渠道提出投诉意见及诉求。郑州银行股份有限公司将积极受理，核实情况，确认银行所承担责任，及时联系客户，与客户进行沟通调解。如产生相关法律纠纷，将依程序仲裁、诉讼，最大程度保障消费者的合法权益。

郑州银行股份有限公司

2023 年 11 月 8 日

附件 1-5

基于大数据技术的反电信网络诈骗服务退出机制

本应用按照退出机制，在保障用户资金和信息安全的前提下进行系统平稳退出。

具体机制如下：

郑州银行股份有限公司按照预定退出方案进行应用平稳终止，停止上线，对平台相关数据进行处理，切实保障金融用户数据安全。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。切实保障消费者权益。

郑州银行股份有限公司

2023 年 11 月 8 日

附件 1-6

基于大数据技术的反电信网络诈骗服务应急预案

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

具体应急预案如下：

1、应急处置培训

系统及业务上线前，对涉及的相关操作人员进行操作流程及应急处置培训，确保发生突发事件时能够第一时间妥当处置，最大程度降低影响范围。

2、充分测试演练

系统及业务上线前进行全链路压测、容灾演练，确保上线投产后业务正常运行，系统可正常使用，并且确保模型准确，保障我行客户合法权益。