

《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	911200007773294627-2025-0001	
	创新应用名称	基于大数据技术的反诈交易监测服务	
	创新应用类型	金融服务	
	机构信息	统一社会信用代码	911200007773294627
		全球法人识别编码	无
		机构名称	天津农村商业银行股份有限公司
		持有金融牌照信息	牌照名称：中华人民共和国金融许可证 牌照编号：B1083H212000001 发证机关：中国银行保险监督管理委员会天津监管局
	拟正式运营时间	2025 年 10 月 22 日	
	技术应用	<p>1. 利用大数据的实时数据采集技术，采用数据库 CDC（变化数据捕获）技术，对交易系统源数据进行实时采集，确保核心系统、支付系统等关键数据源的每笔交易更新能在毫秒级同步至大数据平台，实现响应速度毫秒级。</p> <p>2. 利用大数据 Apache Hudi 数据湖技术，完整保存各源系统原始格式的历史数据，还能确保随时调用当前时点最新数据，解决了传统数据仓库“历史数据与实时数据割裂”的痛点，构建了“全量历史+实时鲜活”的数据底座。</p> <p>3. 利用大数据流批一体计算引擎技术，Spark 批量计算和 Flink 流处理，两者协同形成“批量建模-实时应用-批量优化”闭环模式，实现“全域风险筛查”。</p>	
	功能服务	<p>本应用通过大数据、机器学习、RPA 数字员工、AI 大模型等先进技术与反诈工作深度融合，推动风控关口不断前置，建立起基于大数据技术的反诈交易监测智能体，从大量交易数据中挖掘未知的可疑交易行为，助力可疑交易账户分析，从数字金融、科技金融、养老金融、普惠金融四个方面，为人民群众筑牢安全防护网。</p> <p>本应用由天津农村商业银行股份有限公司负责系统研发运维并提供金融应用场景，此外无其他第三方机构参</p>	

		与。
	创新性说明	<p>1. 数据应用方面，利用大数据技术，深度整合行内海量多元的客户基础信息，筛选潜在异常高危涉诈账户特征的可疑数据，联动推送至反诈模型监测。大数据技术与反诈规则模型协同应用，依据风险等级构建差异化风险数据池，达成大数据与反诈模型双向互补、精准识别的效能升级。</p> <p>2. 模型创新方面，利用行内自有资源，充分整合数据和业务系统关联，搭建起集“事前预警+事中拦截+事后监测”于一体的反诈模型智能体。自主研发“陌生入账对手新入库”模型，革新模型研发思路，弥补监测盲区，将交易监测及风控关口前置，为涉诈账户源头治理提供关联分析与风险拦截的创新范式。</p> <p>3. 账户管控方面，依托反欺诈平台，构建分层分级风控体系。分别在 T+0 日入账和出账环节布控交易阻断、暂停非柜面、临时止付、账户止付等不同的风控措施，避免“一刀切”式管控，精准防控风险，提升反诈效能。</p>
	预期效果	提升金融机构反诈模型科技创新能力，提高风控模型监测识别可疑账户的精准性，加强金融服务能力。
	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，预计对银行全量个人客户进行交易风险监测，年监测交易笔数约 1 万笔。
创新应用 服务信息	服务渠道	线上渠道
	服务时间	7 × 24 小时
	服务用户	天津农商银行个人客户
	服务协议书	《服务协议书-基于大数据技术的反诈交易监测服务》（见附件 1-1）
合法合规 性评估	评估机构	天津农村商业银行股份有限公司
	评估时间	2025 年 9 月 19 日
	有效期限	3 年
	评估结论	本应用严格按照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，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诈交易监测服务》(见附件 1-2)		
技术安全性评估	评估机构	天津农村商业银行股份有限公司		
	评估时间	2025 年 9 月 19 日		
	有效期限	3 年		
	评估结论	本应用严格按照《个人信息信息保护技术规范》(JR/T0171—2020)、《金融科技创新安全通用规范》(JR/T 0199—2020)、《金融数据安全 数据安全分级指南》(JR/T0197—2020)、《基于大数据的支付风险智能防控技术规范》(JR/T0202—2020)、《金融业数据能力建设指引》(JR/T0218—2021)、《金融数据安全 数据生命周期安全规范》(JR/T0223—2021)、《金融大数据平台总体技术要求》(JR/T0237—2021)等相关金融行业技术标准规范要求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。		
	评估材料	《技术安全性评估报告-基于大数据技术的反诈交易监测服务》(见附件 1-3)		
风险防控	风控措施	1	风险点	模型缺陷风险:包括模型设计、开发、及 IT 实施时产生的各类问题或操作错误;模型误用,当市场环境发生重大变化或行内原有产品、业务、管理环节发生重大变更,模型已不适合在当前情况时继续应用原模型,未及时作出调整。
			防范措施	通过搭建科学有效的治理框架,建立全生命周期管理机制和清单管理机制,不断完善资源管控,为模型风险管理工作提供支持;通过模型验证工作检验模型是否按预期运行,是否符合其设计目标和业务用途,定期开展模型有效性评估,模型验证工作由专业人员完成。开展模型投产后评估工作,关注模型准确率等关键指标及特征偏移、误差情况,当监测值出现过高或过低等异动时,自动触发警告,由业务专家及技术专家联合进行问题研判并进行问题修复。
		2	风险点	数据安全与隐私风险:反诈模型需采集客户账户信息、交易记录、身份信息、设备信息等敏感数据,如加密存储或访问控制不足,易引发

			敏感信息泄露风险。
		防范措施	敏感信息保护。建立应急响应机制，参照《数据安全法》定期开展信息渗透测试与漏洞扫描。实施数据分级分类管理，对生物特征等核心数据采用硬件加密模块（HSM）存储。部署动态访问控制，加强数据调取审批，基于角色最小权限原则限制数据调取；采用隐私增强技术（PETs）。建立数据脱敏审计机制，自动检测未脱敏字段并告警。
	风险补偿机制	本应用按照风险补偿方案（见附件 1-4），建立健全风险补偿机制，驱动风控模型迭代优化及构建多维度的补偿体系，确保可疑交易监测持续有效。	
	退出机制	本应用按照退出机制（见附件 1-5），在确保可疑交易监测覆盖面和有效性的前提下，执行下线操作。在业务方面，按照退出方案关停相关服务，同时做好相关技术文档的留存。在技术方面，对功能进行下线。涉及数据的，做好数据备份，同时按照国家及金融行业相关规范要求做好数据清理、隐私保护等工作。	
	应急预案	本应用按照应急处置预案（见附件 1-6），切实保障业务稳定运行，确保在反诈模型失效、误判率激增、遭遇新型诈骗攻击或系统故障时，快速启动应急机制，最大限度降低用户损失，保障业务安全。在模型上线前进行全链路压测、容灾演练、应急演练，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，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。	
投诉响应机制	机构投诉	投诉渠道	1. 营业网点 向天津农商银行营业网点业务人员反馈问题。 2. 客服电话 致电客户服务热线“96155”，通过选择人工服务联系客服代表进行投诉反馈。
		投诉受理与处理机制	受理部门：天津农商银行营运管理部 受理时间：1 个工作日

			<p>受理流程：收到客户投诉后，向相关团队核实情况，客服人员跟进并告知客户投诉进展。</p> <p>处理时限：1-3 个工作日处理完成</p>
	自律投诉	投诉渠道	<p>受理机构：中国互联网金融协会</p> <p>投诉网站： https://tousu.nifa.org.cn</p> <p>投诉电话：400-800-9616</p> <p>投诉邮箱： fintech-support@nifa.org.cn</p>
		投诉受理与处理机制	<p>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。</p> <p>对于涉及相关地区的金融科技创新应用项目的争议、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。</p> <p>联系方式：400-800-9616</p> <p>对外办公时间：周一至周五 上午 8:30-11:30 下午 13:30-17:00</p>
备注	无		

附件 1-1

基于大数据技术的反诈交易监测服务协议书

本项目服务协议包括《天津农商银行人民币个人银行结算账户管理协议》，具体内容详见附件 1-1-1：

天津农商银行人民币个人银行结算账户 管理协议

为保证合法、规范使用个人银行结算账户，开户申请人（甲方）与天津农商银行（乙方）在平等自愿的基础上，根据中国人民银行《人民币银行结算账户管理办法》、《关于改进个人银行结算账户服务 加强账户管理的通知》、《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》、《关于落实个人银行结算账户分类管理制度的通知》、《关于改进个人银行结算账户分类管理有关事项的通知》、《关于贯彻落实电信网络诈骗及其关联违法犯罪联合惩戒办法有关事项的通知》及相关法律法规和规范性文件规定，签订本协议并共同遵守。

第一条 本协议所称个人银行结算账户（含Ⅰ、Ⅱ、Ⅲ类个人银行结算账户）是指甲方凭个人有效身份证件以自然人名称在乙方开立的，办理资金收付结算的人民币活期账户。

第二条 甲方自愿选择在乙方开立人民币个人银行结算账户。乙方同意为甲方开立个人银行结算账户，并为甲方提供个人银行结算账户服务。

第三条 甲方在乙方开立、使用和撤销个人银行结算账户应遵守《人民币银行结算账户管理办法》及相关法律。甲方

使用在乙方开立的个人银行结算账户办理各项业务时，还应遵守乙方的相关制度规定。

第四条 甲方在乙方开立个人银行结算账户，需向乙方提交相应的证明文件，并接受乙方的审核。甲方承诺所提供的开户资料真实、有效，如有伪造、欺诈，承担法律责任。

第五条 甲方在乙方只能开立一个Ⅰ类户，已开立Ⅰ类户，再新开户的，可开立Ⅱ类户。甲方于2016年11月30日前在乙方开立多个Ⅰ类户的，甲方同意按要求向乙方说明其开户合理性。对于无法核实开户合理性的，甲方同意撤销个人银行结算账户，或采取降低账户类别等措施。乙方有权对甲方不符合政策的账户采取限制交易等控制措施。乙方为甲方开立Ⅱ类户的数量原则上不超过5个。

第六条 甲方在乙方开立、使用和撤销个人银行结算账户过程中，甲方授权同意乙方收集使用甲方在乙方产品或服务过程中主动提供、或因使用产品或服务而产生的个人信息。个人信息包括身份证件信息、姓名、性别、民族、国籍、职业、个人电话号码、面部图像信息、通信通讯联系方式、住址、账户信息。

第七条 为了保障服务的安全性，乙方会通过人脸识别等技术手段将甲方的真实面部信息与权威数据源进行比对，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。

第八条 对于预留密码的账户，凡使用正确密码进行的交易均视为甲方本人行为，甲方应妥善保管账户介质、密码、本人有效身份证件及有关业务凭证等，因甲方保管不善或自愿使用账户造成的损失由甲方自行承担。

第九条 甲方申请在乙方开立个人银行结算账户时应填写开户申请书。符合乙方受理个人票据业务开办条件的客户，在申请办理票据业务时还需要预留签章。乙方受理后，甲方应确认开立个人银行结算账户申请书中填写的内容。

第十条 甲方应配合乙方按照法律、行政法规及有关规定开展的客户尽职调查工作；乙方有权采取合理方式在与甲方建立业务关系和业务关系存续期间对甲方进行尽职调查等工作。

第十一条 甲方不得利用在乙方开立的个人银行结算账户进行偷逃税款、逃废债务、套取现金、洗钱及其他违法犯罪活动。

第十二条 甲方申请开立的个人银行结算账户仅限本人使用，甲方不得出租、出借、转借、出售或购买在乙方开立的个人银行结算账户，不得利用在乙方开立的个人银行结算账户套取银行信用。

第十三条 如甲方违规使用个人银行结算账户，乙方有权停止其使用个人银行结算账户。

第十四条 为有效防范电信网络诈骗风险，保障资金安全，根据相关规定，乙方有权结合甲方账户使用情况，采取

包括但不限于动态调整账户非柜面业务限额（包括网上银行、手机银行、第三方支付、自助设备、POS等）、暂停非柜面业务、只收不付、不收不付等措施。

第十五条 甲方因非法买卖、出租、出借银行账户经设区的市级以上公安机关认定为惩戒对象的，乙方有权按照《电信网络诈骗及其关联违法犯罪联合惩戒办法》及相关法律法规和规范性文件对其个人银行结算账户采取管控措施。

第十六条 甲方承诺不冒用他人身份或者虚构代理关系开立个人银行结算账户。

第十七条 甲方应知悉，依据《中华人民共和国刑法》第二百八十七条规定，“明知他人利用信息网络实施犯罪，为其他犯罪提供互联网接入、服务器托管、网络储存、通讯传输等技术支持，或者提供广告推广、支付结算等帮助，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金”。

第十八条 甲方在证件到期后三个月内，仍未向乙方提供最新证件，且未提出合理理由的，乙方有权中止为甲方办理业务，视情况对甲方账户采取账户限制措施，由此造成的后果由甲方承担。

第十九条 根据人民银行相关规定，甲方在乙方开立的个人银行结算账户自开户之日起6个月未发生业务的（不含计息），乙方将对受控账户发送通知短信，该账户将被采取限制措施，由此造成的后果由甲方承担。甲方重新完成身份核验后，可以恢复相关业务。

第二十条 根据人民银行相关规定，甲方预留的电话号码应当与个人身份证件号码一一对应，对多人使用同一联系电话号码开立和使用账户的情况，甲方无法证明合理性的，乙方有权对相关银行账户暂停非柜面业务。

第二十一条 甲方须按支付结算法律法规使用支付结算工具，并按乙方有关规定支付服务费用，具体收费项目和收费标准以乙方官网公示或公告为准。

第二十二条 甲方使用在乙方开立的个人银行结算账户办理个人转账收付和大额现金存取时要遵守《人民币银行结算账户管理办法》的有关规定。

第二十三条 甲方同意乙方在个人银行结算账户存续期间向甲方发布营销等宣传短信。甲方可通过乙方发布的营销或宣传短信中提供的拒绝接收方式拒绝接收。

第二十四条 甲方撤销在乙方开立的个人银行结算账户，必须与乙方核对该账户存款余额，并交回各种重要空白票据及结算凭证，乙方核对无误后方可办理销户手续。甲方因故未交回各种重要空白票据及结算凭证的，须出具书面证明，由此而造成的损失由甲方承担。

第二十五条 甲方遗失或更换预留个人印章的，应按《人民币银行结算账户管理办法》及乙方的相关制度规定，向乙方提供经签名确认的书面申请及相关证明文件。

第二十六条 甲方须定期与乙方核对账务。

第二十七条 乙方应依法为甲方在乙方开立的个人银行结算账户的存款和有关资料保密。除国家法律另有规定外，乙方有权拒绝任何单位或个人查询。

第二十八条 甲方账户自开户之日或上一次交易日起满一年（含）以上未发生交易（不含结息），甲方同意乙方对该账户采取长期不动账户措施管理。

第二十九条 本协议以双方签名或盖章后生效，于甲方在乙方开立的个人银行结算账户存续期间有效，如甲方撤销在乙方开立的个人银行结算账户，自正式销户之日起，本协议自动终止。

第三十条 因法律、行政法规及有关规定调整导致协议条款不再适用，或因乙方管理需要调整本协议条款，乙方通过营业网点对更新后的协议条款进行公告，公告期为三十个自然日，公告期内，甲方如不同意有关变更，可按照规定进行销户，继续使用个人银行结算账户的，视为甲方同意有关变更，公告期满后，新协议条款即为生效。

第三十一条 本协议生效后施行的法律法规和监管规章的有关规定与本协议内容冲突的，以有关法律法规和监管规章规定为准。

第三十二条 若本协议发生争议，双方应协商解决，或向我行官方客服 022-96155 反馈；协商不成，任何一方有权向乙方所在地人民法院提起诉讼。在诉讼期间，本协议不涉及争议部分的条款仍需履行。

天津农村商业银行股份有限公司

2025 年 9 月 26 日

基于大数据技术的反诈交易监测服务 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》、《中华人民共和国反洗钱法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《中华人民共和国消费者权益保护法》、《中华人民共和国反电信网络诈骗法》、《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）、《中华人民共和国消费者权益保护法实施条例》（中华人民共和国国务院令 第778号）、《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）、《征信业务管理办法》（中国人民银行令〔2021〕第4号发布）、《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》（中国人民银行、银监会、证监会、保监会令〔2007〕第2号发布）、《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）、《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），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，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。

天津农村商业银行股份有限公司

2025 年 9 月 26 日

基于大数据技术的反诈交易监测服务 技术安全性评估报告

本项目严格按照《个人信息信息保护技术规范》(JR/T0171—2020)、《金融数据安全 数据安全分级指南》(JR/T0197—2020)、《基于大数据的支付风险智能防控技术规范》(JR/T0202—2020)、《金融业数据能力建设指引》(JR/T0218—2021)、《金融数据安全 数据生命周期安全规范》(JR/T0223—2021)、《金融大数据平台总体技术要求》(JR/T0237—2021)等相关金融行业技术标准规范要求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。

天津农村商业银行股份有限公司

2025 年 9 月 26 日

基于大数据技术的反诈交易监测服务 风险补偿机制

一、建立风险补偿机制的必要性

建立风险补偿机制，其重要性主要体现在以下几个方面：

1. 模型虽然能够有效识别可疑交易，但仍然存在一定的误判率，例如，合法交易可能因为某些特征与可疑交易相似被误判而遭到拦截、冻结账户或限制交易。

2. 电诈分子不断研究、破译银行风控规则，采用新型作案手法进行交易，导致出现模型漏判，涉诈账户被模型监测识别的精准性降低。

二、风险补偿机制建设

为进一步提升和优化可疑交易账户监测模型的精准性，建立相关风险补偿机制，确保可疑交易监测持续有效。具体如下：

1. 驱动风控模型迭代优化。根据补偿机制所产生的数据和案例反哺风控模型，帮助数据分析人员精准定位模型缺陷，优化特征变量和规则逻辑，持续优化风控模型。

2. 构建多维度的补偿体系。如：提供紧急客服热线、优先处理通道，加速误报解冻，优化流程实现更快的调查响应速度，减少客户等待时间。

3. 建立长效风险拓展机制。让风控模型具有“迭代进化”能力，将人行下发风险提示、风险指引等信息转化为外部风险信号库，确保风控系统能够主动适应日益变化的外部风险环境，实现自我迭代和升级，避免模型性能衰减和失效。

4. 完善人工干预流程。当模型未监测到涉诈风险时，及时启动人工筛查机制，组织相关人员开展风险排查，并及时对异常账户采取管控措施。

天津农村商业银行股份有限公司

2025 年 9 月 26 日

基于大数据技术的反诈交易监测服务 退出机制

一、退出机制的定义

反诈模型退出机制指终止模型服务的过程，确保在模型因效果、策略、合规或技术原因需停用时，业务风险可控。

核心目标：

1. 防风险：避免退出后欺诈率飙升或误伤用户。
2. 保连续：维持风控体系无缝衔接。
3. 合规范：满足数据清理及监管报备要求。

二、退出机制的触发条件

1. 效果不达标，策略迭代，业务场景下线。本应用涉及的交易监测模型已不满足我行反诈业务需求，或我行研发出有效性更高的反诈模型进行替代。

2. 相关法律法规或监管要求发生变化，导致当前的风控服务无法满足新的合规标准，或者继续运行可能面临合规风险，需要及时退出并调整服务。

3. 技术/成本问题，模型数据存在严重问题，维护成本过高。

三、退出机制的具体步骤

（一）退出评估与决策

1、业务影响评估：分析停止该服务后，对客户交易的影响。

2、技术依赖性评估：梳理该服务与其他核心系统（如交易系统、数据库）的耦合度。退出是否会对其他系统造成影响。

3. 将评估报告提交至相关决策机构进行最终审批，获得正式批准后，启动退出程序。

（二）通知与沟通

1. 通知相关方，明确退出决定、原因、时间表及其职责变化。

2. 做好退出原因解释并说明已采取的后续风险保障措施，确保符合监管规定。

（三）数据清理与备份

1. 数据资产盘点和分类

全面盘点该服务涉及的所有数据资产，包括：生产数据库、备份数据库、日志文件等。根据法律法规和合规要求，将数据严格分类：

必须依法保留的数据：例如，可疑交易报告记录、相关审计日志等，需根据《反电信网络诈骗法》等法律法规要求进行保存。

必须彻底删除的数据：包含个人敏感信息且无保留必要的信息，进行删除。

2. 执行数据迁移与备份

将必须依法保留的数据从生产环境中迁移至专用的、安全的长期归档存储系统，并设置严格的访问权限。

3. 执行数据清理与销毁

对必须彻底删除的数据，使用技术手段进行不可恢复的销毁。

（四）系统关闭与资源回收

制定详细的系统停机计划，将该服务的所有代码、配置文档、技术设计文档、用户手册等进行最终版本的归档保存，以备审计或查询需求。

（五）后续跟进与评估

在服务关闭后的一段时间内密切监控关键风险指标变化。评估退出该服务后对整体业务风险的影响是否在预期范围内。

天津农村商业银行股份有限公司

2025 年 9 月 26 日

基于大数据技术的反诈交易监测服务 应急预案

一、应急预案的基本介绍

（一）目标

本应用按照应急处置预案妥善处理突发事件，切实保障业务稳定运行，确保在反诈模型失效、误判率激增、遭遇新型诈骗攻击或系统故障时，快速启动应急机制，最大限度降低用户损失，保障业务安全。

（二）适用范围

1. 模型误拦截率/漏拦截率异常上升。
2. 新型诈骗手法突破现有模型防御。
3. 模型服务宕机或数据源异常。
4. 监管紧急风险通报。

二、应急预案的处理原则

在模型上线前进行全链路压测、容灾演练，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，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。

（一）分级响应

按影响范围分级启动预案：

1. 对于影响较小的一般风险,通过技术手段敏捷化处理完善。

2. 对于重大风险,首先暂停模型监测,然后有效处理恢复至服务正常运作。

3. 就责、权、利参照风险补偿机制相关内容进行善后处理。

（二）最小化用户影响

误管控账户提供快速解管控服务,人工审核后恢复账户使用。

三、应急预案的具体安排

（一）应急组织架构

1. 应急指挥组:决策预案启动、资源协调、对外沟通。

2. 技术响应组:修复系统故障。

3. 风险运营组:人工审核交易、投诉处理。

（二）关键流程安排

阶段 1：监测与告警

监控指标：建立日常生产运行监控机制，7×24 小时检测模型性能（漏判率、误判率、服务可用性）。定期审查模型决策是否符合监管要求。

服务告警：核心链路、接口、功能模块、硬件资源等发生异常，预警量出现明显下降或上升。

服务宕机：自动暂停管控机制。

阶段 2：应急响应

1. 确认问题：

技术组定位原因，识别链路、硬件资源、模型 BUG、数据污染、新型攻击或其他问题，并触发数据回补或模型降级。

2. 启动预案：

一般风险：通过技术手段敏捷化处理完善。

重大风险：首先暂停模型监测，然后有效处理恢复至服务正常运作。

阶段 3：恢复与复盘

1. 恢复标准：

主模型修复且测试通过，或新型诈骗防御规则已上线。上线后保留历史版本，若新模型引发问题，支持一键回退至稳定版本。

2. 事后复盘：

输出故障报告：根因分析、损失统计（如用户资金损失量）、模型优化计划。

天津农村商业银行股份有限公司

2025 年 9 月 26 日