**一、项目图例如下：**



**二、产品技术标准要求**

1.功能要求

（1）经办上传数据。经办人员按照统一指定模板填写需要处理的卡号数据，登陆系统进行上传，上传完成后自动发起流程，以待办任务的形式流转至复核人员，经办角色可以实时登录系统查看处理结果。

（2）复核处理功能。复核人员进入系统后，系统支持在线查看经办上传的文本内容，经核实后确认无误后，点击提交，修改处理状态为处理通过；若核实有误，修改处理状态为不通过，并填写不通过的原因，提交后该任务流转退回至经办人员，经办人员再次修改数据后可重新发起处理流程。

（3）处理限额设置。复核人员将待处理数据确认无误，审核通过后，系统后台通过调用总行7个接口逐笔完成相关数据的限额设置，分行特色系统根据总行相对应接口返回的数据完成更新操作。

注意：批转联处理文本支持的最大数据条数应做限制或拆包分批处理。

（4）查询功能及报表导出。系统经办角色、复核角色、管理员等用户角色可以查看文件处理当前节点，数据处理状态，支持按照日期、单一卡号等维度条件查询限额情况（是否限额、什么机构、什么时候限额、限了什么项目等），并针对查询结果支持报表导出功能。

2.性能要求

（1）数据保护：我行敏感信息的系统不得部署在我行网络环境之外的其他外部服务商环境上。接触我行信息时，遵守我行安全和保密相关条款的要求。如涉及处理我行数据，严格在合同允许范围内使用，不超范围使用我行数据。

（2）网络安全保障

（a）在发现提供的产品脆弱性和漏洞后，第一时间通知我行并协助我行进行漏洞整改与修复。对我行的安全漏洞信息严格进行保密，不在任何场合以任何方式提供给任何第三方。不使用安全漏洞信息攻击我行。

(b)针对网络安全风险事件（包括但不限于：源代码泄露、敏感数据泄露、产品出现安全漏洞等）制定应急响应方案，及时配合我行进行应急处置。

(c)系统上线和系统版本变更前必须经过网络安全测试，包括：渗透测试、漏洞扫描等，测试无中高风险方可投产上线。如无变更，网络安全测试也不少于1次/年。系统升级变更的应重新开展安全测试。安全测试报告（渗透测试、漏洞扫描）需由市场中具有相关测评服务的第三方网络安全公司出具。

(d)有义务向我行说明产品采集的信息、产品后台之间的连接情况和回传信息。不利用提供的产品和服务擅自获取我行数据、擅自控制和操纵我行设备，无正当理由不中断产品供应或必要的技术支持服务。

(e)做好源代码的安全管控，防止源代码外泄。涉及我行的源代码原则上不托管于第三方代码托管平台，如必须托管，应向我行报备，并使用高强度的访问控制措施。不擅自在互联网搭建含我行logo、品牌名和我行内部信息的系统。

(f)具备完善的客户信息及资产安全保障机制，具备完善的系统安全保障机制及数据备份机制。供应商应保守商业秘密，不向任何第三方透露合作方式、价格等内容，不得采集持卡人姓名、手机号码、不得留存交易卡号。供应商须承诺所提供的服务资源在合作有效期内保持有效。若因供应商提供的服务资源失效导致活动无法顺利进行或客户无法享受服务，供应商应承担相关赔偿责任。

3、可用性要求

反电诈个人账户反电诈限额管控支持省分行条线部门用户、二级分行、网点分级管理和使用，界面美观，操作便利，并支持多维度数据查询和动态统计分析。即网点经办人员按照统一要求的数据文本格式上传待处理数据，网点复核人员复核确认后，提交系统进行数据处理。系统会自动调用总行接口完成限额设置，经办及复核人员可查询数据处理结果及详情。二级分支行本部管理员可查询本行内各网点下传数据统计情况，省行管理员可查询全行数据统计情况，支持报表导出。根据行方反诈工作最新要求，可结合新形势，维保期内对上述限额管控功能（包括但不限于页面展示、限额管控接口）升级调整。