《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	9131000010000595XD-2020-0003	
	创新应用名称	远程视频银行服务	
	创新应用类型	金融服务	
	机构信息 1	统一社会信用代码	9131000010000595XD
		全球法人识别编码	549300AX1UM10U30HK09
		机构名称	交通银行股份有限公司
		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：B0005H131000001 发证机关：中国银行业监督管理委员会
	机构信息 2	统一社会信用代码	911101085636549482
		全球法人识别编码	无
		机构名称	腾讯云计算(北京)有限责任公司
		持有金融牌照信息	无
	拟正式运营时间	2021 年 01 月 29 日	
	技术应用	1.基于音视频技术，搭建交通银行音视频平台，采用智能选路策略在交通银行与客户之间建立音视频加速通道，通过实时监控全网传输节点的业务高峰、网络抢占等情况来自动选择最优传输链路，实现交通银行与客户间跨运营商、跨区域链路的高质量实时音视频通讯，打造远程视频银行。 2.运用音频 3A 处理（回声消除 AEC、噪声抑制 ANS、自动增益控制 AGC）、音视频对抗弱网（抗丢包、网络自适应）等底层音视频技术，依托音视频平台使用算法对音视频数据源码进行消除回声、降噪、防丢包等处理，提高音视频数据的质量。 3.采用端到端加密模式将银行与客户远程交互音视频数据与业务数据分层加密传输（密钥由交通银行生成并管理）、分散存储，并在平台上自动完成音视频的录制存储，严控数据访问权限，有效防范数据泄露风险，提升远程银行业务的安全性。 4.利用图像识别、光学字符识别（OCR）等人工智能技术，提取用户的身份证件信息和图像特征，并向公安联网核查系统进行用户身份“实名实人”验证，提升客户身份认证的准确性，提高远程银行业务办理的效率。	
	功能服务	本项目综合运用 3A 处理、对抗弱网等音视频技术打造远程视频银行服务，通过“一对一”交互式服务，辅助用户更好办理银行高柜、低柜、移动场景业务，突破物理与空间限制，打造无障碍线上线下一体化金融服务。本项目此次试点用于对公开户，用户通过交通银行手机 APP 与客户经理进行音视频交互，	

		在客户经理的远程协助下，提前准备充足的业务办理资料，有效提高线下柜台开户业务办理效率。 本项目由交通银行股份有限公司提供金融应用场景、业务系统对接并负责平台运营，腾讯云计算（北京）有限责任公司提供技术支持和音视频平台搭建，此外无其他第三方机构参与。
	创新性说明	1.渠道创新方面，本项目将音视频技术与银行业务办理相结合，创新银行对客服务渠道，将客户原本需要全程线下网点办理的业务，通过移动 APP 远程视频互动的形式辅助业务办理，协助解决银行网点运营成本高的困局，提升了银行对客服务的广度和深度。 2.便民服务方面，结合音视频实时协作沟通，银行工作人员可以远程辅助客户进行业务办理，同时协助客户在其移动终端处理复杂的业务要素录入，降低客户在线上渠道的操作复杂度，提升银行移动 APP 产品的易用性，使客户不受物理位置限制、不受知识背景局限，随时随地享受标准化、无差别化金融服务，在后疫情时代，给客户更好的体验。 3.数据保护方面，通过数据传输端到端加密、音视频传输私有协议、银行数据本地化存储、重要信息显示脱敏等多种技术手段，全方位加强了数据安全和个人隐私保护。 4.身份验证方面，通过将视频交互过程中抽取的视频帧数据与 OCR 识别的身份证信息进行图像比对，并与公安联网核查系统进行身份认证，增加了客户端数据篡改和伪造的难度，提升对客户身份认证的准确性和高效性。
	预期效果	通过远程音视频金融服务的形式，扩大银行的金融服务半径，在后疫情时代，为客户提供更便捷的“非接触式”金融服务，为小微企业在办理对公开户业务时，提供更灵活的交互渠道，提升客户在移动端办理业务的用户体验。
	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，预计每年辅助对公开户 1.5 万户。
创新应用服务信息	服务渠道	线上渠道：交通银行企业手机银行 APP 等
	服务时间	5×8 小时
	服务用户	交通银行企业客户
	服务协议书	《服务协议书-远程视频银行服务》（见附件 1-1）
合法合规性评估	评估机构	北京德和衡（上海）律师事务所
	评估时间	2020 年 12 月 28 日
	有效期限	1 年
	评估结论	本项目涉及个人客户前端数据授权、用户身份验证（KYC）、

		远程视频公证、电子签名等情景以及实时音视频、智能选路、身份认证安全加密、双录存储等技术环节，整体符合《中华人民共和国网络安全法》、《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）、《中国人民银行关于取消企业银行账户许可的通知》（银发〔2019〕41号）等国家及金融领域相关法律法规和政策文件要求，可以依法开展进一步的研发和实施。		
	评估材料	《合法合规性评估报告—远程视频银行服务》（见附件1-2）		
技术安全性评估	评估机构	腾讯云计算（北京）有限责任公司		
	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《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）、《网上银行系统信息安全通用规范》（JR/T 0068—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，并从技术架构、应用场景、安全机制、运维容灾、权限控制和隐私保护等方面进行全面安全评估，采取了有效的技术和管理手段进行针对性安全增强，方案合理有效。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—远程视频银行服务》（见附件1-3）		
风险防控	风控措施		风险点	在实时音视频数据传输和存储过程中，可能存在隐私数据被超范围使用和泄露的风险问题。
		1	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。数据传输时，采用端到端加密的方式，通过音视频加密、密钥自管理等方式确保数据不会被第三方破解。数据存储时，在外网不落地，双录文件在银行内网安全隔离、分散存储，严控访问权限，降低数据泄露风险。数据使用时，明确告知客户数据使用范围，不归集、不共享原始数据前提下，控制在行方业务渠道范围内。
		2	风险点	实时音视频技术对网络依赖性强，消耗网络资源大，可能面临业务量高并发时系统中断等风险，需加强网络实时监控预警和管理。

			防范措施	在项目设计中，考虑业务并发量，并给出冗余带宽，同时使用音视频双通道备份等方式建立通道切换机制，保障业务安全稳定运行。
		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建立的风险补偿方案（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建立的退出机制（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建立的应急处置预案（附件 1-6），针对不同的问题提供相应的解决方案，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。包括但不限于以下内容: 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，而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。	
投诉 响应机制	机构投诉	投诉渠道	1.致电交通银行客服热线 95559，选择人工服务联系客服代表; 2.通过登录交通银行官方网站 www.bankcomm.com，选择在线客服联系客服代表。
		投诉受理 与处理机制	交通银行接受投诉后，将指派专职人员核实情况，并及时告知客户投诉处理进展，项目团队也将及时协助相关问题的解决。
	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）

附件 1-1

远程视频银行服务
服务协议书

人民币单位银行结算账户管理协议

（2019 版）

重要提示
请甲方认真阅读本协议全文，尤其是带有▲▲标记的条款。如有疑义，请及时提请乙方予以说明。

鉴于:

甲方向乙方申请开立人民币单位银行结算账户（下称“账户”）。

为明确双方权利义务，根据有关法律法规及监管规定，甲方与乙方经协商一致，订立本协议。

第一条　定义

1.1 本协议所称“账户”，指乙方为甲方开立的用于办理资金收付结算的账户。

1.2 本协议所称“停止支付”，指停止账户的资金支付功能，账户只收不付，签约缴纳税款、社会保险费用以及水、电、燃气、暖气、通信等公共事业费用的资金支付除外。

1.3 本协议所称“中止账户业务”，指停止账户资金收付功能，账户不收不付，签约缴纳税款、社会保险费用以及水、电、燃气、暖气、通信等公共事业费用的资金支付除外。

1.4 本协议所称“收付活动”不包括有权机关扣划资金以及账户结息、银行扣收管理费等因账户管理本身形成的资金收付。

第二条　账户的开立和使用

2.1 根据甲方向乙方提交的开立账户申请及所提供的《交通银行开立单位银行结算账户申请书》（以下简称“《开户申请书》”）和根据乙方要求提供的文件、资料及相关信息，乙方为甲方开立账户，账户户名、账号和账户类型以第 19.1 条约定为准。

2.2 甲方为境内依法设立的企业法人、非法人企业、个体工商户的，所开立账户自开立之日即可办理收付款业务，如甲方所开立账户为基本存款账户，乙方在完成基本存款账户信息备案后，将为甲方打印《基本存款账户信息》和存款人查询密码并交付甲方。甲方为机关、事业单位等其他单位的，如所开立账户为因借款转存开立的一般存款账户，所开立账户自开立之日即可办理收付款业务，如所开立账户为因借款转存开立的一般存款账户以外的其他账户，所开立账户自开立之日即可办理收款业务，但付款业务需自所开立账户开立之日起 3 个

工作日后方可办理。

2.3 本协议项下账户开立后，甲方可通过柜面渠道使用账户，如甲方需通过交通银行企业网上银行、企业手机银行等电子渠道使用账户，应按照乙方要求与乙方另行签订协议后使用。

2.4 甲方开立账户项下部分业务/功能需另行签署相关业务协议、开通相关业务/功能后方可办理，具体业务/功能以乙方规定为准。

2.5 甲方使用账户过程中选择使用支付结算工具的，应以符合相关支付结算工具适用的法律法规、监管规定及乙方规定的使用条件为前提。

2.6 如账户开立后，乙方发现甲方账户资料不完整、不合规或者提供的信息有错漏，乙方将通知甲方于 2 个工作日内予以更正，甲方应按乙方要求办理更正手续。如甲方未按时办理更正手续或办理更正手续时提供的资料及/或信息不符合乙方要求，乙方有权对甲方账户停止支付。

2.7 为保障甲方账户的资金安全，对于新开户前十笔业务及大额支付业务（前述“大额支付”的金额标准由乙方确定并作适时调整）乙方提供事后核实服务，如在乙方提供核实服务过程中甲方拒绝核实，视同放弃此项服务的权利。

第三条　账户的变更

3.1 甲方变更名称、法定代表人/负责人的，应自变更之日起 5 个工作日内就其变更事项向乙方提交《交通银行变更单位银行结算账户内容申请书》（以下简称“《变更申请书》”）及乙方规定的文件、资料及相关信息。变更事项以《变更申请书》的记载为准。

因甲方未按上述时间要求提交材料或提供的文件、资料及相关信息不符合乙方规定，导致乙方未在甲方指定的账户信息变更日完成变更，由此导致的乙方无法按规定程序和时间与甲方对账、账户往来的差错无法及时纠正等损失由甲方自行承担。

▲▲3.2 如甲方的名称、法定代表人或单位负责人发生变更，且甲方未按前款规定办理相关手续，乙方知晓该等情况后，乙方将通知甲方办理变更手续。甲方应自乙方通知中载明的期限内办理变更手续，如甲方未按前述规定办理变更手续，且未提出合理理由，乙方有权将甲方账户停止支付。

▲▲3.3 甲方提供的证明甲方系依法设立或者可依法开展经营、社会活动的执照、证件等文件、法定代表人或单位负责人有效身份证件（以下简称“证件”）到期日前，乙方将提前通知甲方办理证件更换手续，并根据法律法规、监管规定要求甲方于证件更换后按乙方通知中规定的要求和期限向乙方办理证件到期日更新手续。甲方应按照乙方通知中规定的要求和期限向乙方办理证件到期日更新手续，如甲

方未按乙方通知中规定的要求和期限向乙方办理证件到期日更新手续，且未提出合理理由，乙方有权中止甲方账户业务。

第四条　账户撤销

4.1 甲方发生被撤销、解散、关闭、注销、宣告破产、证明甲方系依法设立或者可依法开展经营、社会活动的执照、证件等文件被吊销、第 19.2 条中约定的因其他原因需要撤销银行结算账户的情形等任一情形的，应于 5 个工作日内向乙方提出撤销账户的申请。

甲方申请撤销账户，应当与乙方核对账户存款余额，并根据乙方要求向乙方交回相关重要空白票据和结算凭证等资料（如涉及），如甲方无法交回，应向乙方出具无法交回的证明。因甲方未向乙方交回上述资料造成的甲方损失，由甲方自行承担，如甲方未向乙方交回上述资料致使乙方遭受损失的，甲方应向乙方承担赔偿责任。

如拟撤销账户涉及相关业务尚未处理完毕的，该账户需在相关业务全部处理完毕后方可撤销。

4.2 如甲方发生被撤销、解散、关闭、注销、宣告破产、证明甲方系依法设立或者可依法开展经营、社会活动的执照、证件等文件被吊销等任一情形，且甲方未按前款规定办理撤销账户手续，乙方知晓该等情况后，乙方将通知甲方办理相关手续。甲方应自乙方通知中载明的期限内办理撤销账户手续，如甲方未按通知规定办理账户撤销手续，乙方有权将甲方账户停止支付。

▲▲第五条　预留签章

5.1 甲方应就所开立账户在乙方留存预留签章。凡甲方使用预留签章签发的支付结算凭证，均视为甲方发出的支付结算指令，乙方根据甲方使用预留签章签发的支付结算凭证为甲方办理的支付结算业务，相应的后果均由甲方承担。

5.2 甲方如需更换预留签章，应按照乙方的相关要求提供相关资料，办理预留签章变更手续。乙方收到甲方提交的资料并审核通过后，将为甲方办理预留签章变更手续。预留签章变更手续办理完毕后，乙方无法使用原预留签章办理业务，乙方在甲方办理预留签章变更手续前，根据甲方使用原预留签章签发的支付结算凭证为甲方办理的支付结算业务的后果由甲方承担。

5.3 甲方应妥善管理预留签章，如遇预留签章遗失，甲方应及时向乙方办理预留签章变更手续。否则由此发生的损失由甲方自行承担，如因此致使乙方遭受损失的，甲方应向乙方承担赔偿责任。

第六条　查询账户信息

6.1 甲方有权向乙方申请查询所开立账户的相关账户信息，甲方向乙方查询时应出具加盖甲方预留签章的查询申请书，乙方核验预留

签章后，根据甲方查询申请书内容为甲方查询账户信息。

6.2 如甲方为境内依法设立的企业法人、非法人企业、个体工商户，且所开立账户为基本存款账户，甲方有权向乙方申请重新打印《基本存款账户信息》、重置存款人查询密码，甲方向乙方申请重新打印《基本存款账户信息》、重置存款人查询密码应出具企业法定代表人或单位负责人有效身份证件；授权他人办理，应出具法定代表人或单位负责人的授权书及被授权人的有效身份证件，授权书须加盖甲方预留签章。

第七条　银企余额对账

▲▲7.1 甲方账户开立后，乙方将根据法律法规、监管规定定期向甲方发送账户余额对账单进行账户余额对账，甲方收到乙方发送的对账单后，应根据乙方要求向乙方反馈对账结果，如甲方未作反馈或者反馈核对结果不一致，乙方将查明原因，并有权将甲方账户停止支付，直至对账相符后再予恢复。乙方向甲方发送账户余额对账单的具体频率由乙方确定并作适时调整。

7.2 甲方所开立账户未开通企业网上银行、企业手机银行等电子渠道的，乙方向甲方发送的账户余额对账单将以纸质形式提供。甲方所开立账户开通企业网上银行、企业手机银行等电子渠道中任意一种或多种渠道的，乙方将不再以纸质形式向甲方提供账户余额对账单，相应账户余额对账单将通过甲方所开立电子渠道以电子形式提供。

▲▲第八条　账户异常处理

8.1 若甲方存在异常账户开立与使用情况，乙方可根据法律法规和监管要求对甲方采取账户控制措施，控制措施包含但不限于控制交易频次、控制交易金额、限制非柜面交易、限制柜面交易、停止支付和中止账户业务等。

8.2 新开户不动户处理

甲方所开立账户自开立之日起 6 个月内无交易记录的，乙方将暂停该账户的非柜面业务。乙方暂停该账户的非柜面业务后，如甲方拟恢复该账户非柜面业务，甲方应向乙方提交身份核实文件重新进行身份核实，乙方对甲方提交的身份核实文件进行审核并审核通过后为甲方恢复该账户的非柜面业务。

8.3 长期不动户处理

（1）甲方所开立账户连续 1 年未发生收付活动，乙方将通知甲方在 30 个自然日内确认账户是否继续使用。甲方逾期未确认且未提出合理理由，乙方有权中止甲方账户业务，并将该账户认定为久悬账户。甲方存在久悬账户情况，不得在乙方新开立账户。

（2）甲方账户被乙方认定为久悬账户满 5 年且甲方未主动撤销该账户，乙方将通知甲方在 30 个自然日内向乙方办理销户手续。甲

方逾期未向乙方办理撤销账户手续，乙方有权撤销该账户，账户内的资金由乙方进行专项管理，甲方可根据乙方规定持相关材料办理该等资金的划转手续。

8.4 违法失信处理

（1）甲方被全国企业信用信息公示系统列入“严重违法失信企业名单”，乙方经核实后有权中止甲方账户业务。

（2）甲方经公安机关认定存在出租、出借、出售、购买银行账户，或假冒他人身份或者虚构代理关系开立银行账户等情形，乙方将在 5 年内暂停甲方银行账户非柜面业务，3 年内不为甲方新开立账户。

▲▲第九条　账户收费

9.1 甲方开立及使用账户过程中，应按相关法律、法规、规章、监管规定及乙方公布的当时有效的《交通银行服务收费名录》按时足额向乙方支付相关费用。甲方授权，乙方有权直接从所涉账户中扣收相关费用。

▲▲9.2 协议履行期间，乙方有权调整收费项目、收费标准。乙方下调收费标准，将于执行前 10 个银行工作日在交通银行门户网站、企业电子银行或乙方营业网点公告；乙方设立新的收费项目或提高收费标准，在不违反法律、法规、规章和监管规定的强制性规范的前提下，乙方有权提前在交通银行门户网站、企业电子银行或乙方营业网点公告。甲方不同意公告内容的，有权在公告执行前依本协议的约定办理账户撤销手续。甲方在公告执行后继续办理相关业务的，视同接受公告内容。

▲▲第十条　甲方的陈述与保证

10.1 甲方是依法设立、根据法律法规及监管规定可以开立人民币单位银行结算账户的主体，具备所有必要的权利能力，能以自身名义履行本协议的义务并承担民事责任。

10.2 签署和履行本协议是甲方真实的意思表示，并取得签署和履行本协议所必须的同意、批准和授权，不存在任何法律上的瑕疵。

10.3 甲方在申请开立、变更和撤销账户时以及在履行本协议过程中向乙方提交的所有文件、资料及在各申请书中填写的信息真实、合法、有效。

10.4 如甲方在本协议项下开立账户为基本存款账户，甲方应确保该基本存款账户的唯一性，如本协议项下基本存款账户开立后，乙方发现甲方在本协议项下基本存款账户开立前已开立基本存款账户，乙方有权撤销本协议项下开立的基本存款账户。

▲▲10.5 甲方充分了解并清楚知晓出租、出借、出售、购买账户的相关法律责任和惩戒措施，承诺依法依规开立和使用本账户。

10.6 甲方及其关联方均不属于联合国、欧盟或美国等制裁名单，

及中国政府部门或有权机关发布的涉恐及反洗钱相关风险名单内的企业或个人；不位于被联合国、欧盟或美国等制裁的国家和地区。

10.7 甲方保证遵守国家反洗钱法律、法规及相关政策要求，不从事协助他人进行洗钱、恐怖融资、逃税、逃废银行债务、套取现金、电信诈骗、非法集资等违法违规活动，积极配合乙方开展客户开户意愿核实、身份识别、交易记录保存、客户身份及交易背景尽职调查、大额和可疑交易报告等各项反洗钱工作，并按乙方要求提供相关证明材料。

第十一条　双方权利义务

11.1 甲方权利义务

（1）甲方开立及使用账户应符合法律法规和监管规定，并遵守乙方的相关规定及操作惯例。

▲▲（2）甲方应对账户交易的合法性和结算收付资金的合法性负责。不得利用开立银行结算账户进行或协助他人进行洗钱、恐怖融资、逃税、逃废银行债务、套取现金、电信诈骗、非法集资等各类违法违规活动。

11.2 乙方权利义务

▲▲（1）乙方有权依据法律法规和监管要求，针对甲方的异常账户开立与使用情况采取账户控制措施，控制措施包含但不限于控制交易频次、控制交易金额、限制非柜面交易、限制柜面交易、停止支付和中止账户业务等。

▲▲（2）乙方有权通过面对面、视频等方式向企业法定代表人或单位负责人核实开户意愿。如甲方存在异常开户情形的，乙方有权按照反洗钱等规定采取延长开户审查期限、强化客户尽职调查等措施，必要时有权拒绝开户受理。

（3）乙方在本协议项下为向甲方提供的账号在甲方账户存续期间具有专属性，仅限于为甲方办理支付结算业务时使用。

（4）乙方应按照法律法规、监管规定为甲方提供账户服务。

▲▲（5）乙方应及时、准确地完成甲方按照相关法律法规、规章及本协议的约定发出的收付结算指令，乙方因执行甲方支付结算指令而造成的甲方经济损失，乙方不承担责任。但对于不符合法律法规、监管部门规定的收付结算指令，乙方没有义务执行，亦不承担责任，但因乙方过错依法应当由乙方承担的责任除外。

▲▲（6）如因乙方操作失误，将不属于甲方的款项误入甲方账户，乙方有权自行划回。

▲▲第十二条　信息披露与保密

12.1 对于在本协议签署和履行过程中获取和知悉的甲方的未公开信息和资料，乙方对相关信息和资料的使用不得违反法律法规和监

管要求，并应依法承担保密责任，不向第三方披露该等信息和资料，但下列情形除外:

（1）适用法律法规要求披露的;

（2）司法部门或监管机构依法要求披露的;

（3）乙方为行使本协议项下权利、履行本协议项下义务需向乙方的外部专业顾问披露和允许乙方的外部专业顾问在保密的基础上使用的;

（4）甲方同意或授权乙方进行披露的。

12.2 在本协议第 12.1 条规定的情形外，甲方进一步同意乙方在如下情形可以使用或披露甲方的信息和资料，包括但不限于甲方的基本信息及其他相关信息，愿意承担由此产生的一切后果:

为下列目的向业务外包机构、第三方服务供应商、其他金融机构及乙方认为必要的其他机构或个人，包括但不限于交通银行股份有限公司的其他分支机构，或者交通银行股份有限公司完全或部分拥有的子公司，披露和允许其在保密的基础上使用该等信息和资料:

（1）为开展人民币单位银行结算账户管理业务或与人民币单位银行结算账户管理业务有关;

（2）乙方为向甲方提供或可能提供新产品或服务或进一步提供服务。

本协议第 12.2 条是否适用，以双方在第 19.3 条约定为准。

▲▲第十三条　通知

13.1 甲方在本协议中填写的联系方式(包括通讯地址、联系电话、传真号码等）均真实有效。任一联系方式发生变更，甲方应立即以书面方式将变更信息寄/送至乙方在本协议填写的通讯地址。该等信息变更在乙方收到更改通知后生效。

13.2 除本协议另有明确约定外，乙方对甲方的任何通知，乙方有权通过以下任一方式进行。乙方有权选择其认为合适的通知方式，且无需对邮递、传真、电话、电传、微信或任何其他通讯系统所出现的传送失误、缺漏或延迟承担责任。乙方同时选择多种通知方式的，以其中较快到达甲方者为准。就同一事项，乙方对甲方发出一份以上通知且通知内容不同的，除非在通知中另有明确说明，以通知发出时间在后的为准。

（1）公告，以乙方在其网站、网上银行、电话银行或营业网点发布公告之日视为送达日;

（2）专人送达，以甲方签收之日视为送达日;

（3）邮递（包括特快专递、平信邮寄、挂号邮寄）送达于乙方最近所知的甲方通讯地址，以邮寄之日后的第 3 日（同城）/第 5 日（异地）视为送达日;

（4）传真、移动电话短信、微信或其他电子通讯方式送达于乙方最近所知的甲方传真号码、甲方指定的移动电话号码或电子邮件地址、微信号，以发送之日视为送达日，前述送达指相关信息进入服务商的服务器终端而不以相关信息实际在客户终端显示为标准。

13.3 甲方确认并同意，除非乙方收到甲方关于变更通讯地址的书面通知，甲方在本协议填写的通讯地址是法院向甲方送达司法文书及其他书面文件的地址。上述送达地址适用的范围包括但不限于民事诉讼一审、二审、再审和执行程序等。如甲方应诉并直接向法院提交送达地址确认书，该确认地址与乙方最近所知的通讯地址不一致的，法院有权以送达地址确认书上的地址为准进行送达。

本合同争议解决过程中，法院可通过以下任一方式将判决书、裁定书、调解书送达于甲方:

（1）邮寄送达（包括特快专递、平信邮寄、挂号邮寄），以甲方在送达回证上的签收日为送达之日;

（2）专人送达，以甲方在送达回证上的签收之日视为送达之日。

法院采用邮寄送达（包括特快专递、平信邮寄、挂号邮寄）方式的，如甲方未在送达回证上签收或甲方所填写的通讯地址不准确或通讯地址实际发生变更但乙方未收到甲方关于变更通讯地址的书面通知导致判决书、裁定书、调解书被退回的，以文书被退回之日视为送达之日。

法院采用专人送达方式的，如甲方未在送达回证上签收，以送达人当场在送达回证上记明情况之日为送达之日。

除判决书、裁定书、调解书外，法院对甲方的任何通知，法院有权通过第 13.2 条约定的任一通讯方式进行。法院有权选择其认为合适的通讯方式，且无需对邮递、传真、电话、电传、微信或任何其他通讯系统所出现的传送失误、缺漏或延迟承担责任。法院同时选择多种通讯方式的，以其中较快到达甲方者为准。

13.4 本条约定属于协议中独立存在的解决争议条款，本协议无效、被撤销或者终止的，不影响本条款的效力。

▲▲第十四条　违约

14.1 甲方出现下列任一情形时，乙方有权对账户采取停止支付、中止账户业务、撤销甲方账户等任一措施，并有权采取法律法规、监管规定规定的其它救济措施:

（1）使用虚假证明文件骗取乙方办理支付结算;

（2）在本协议第十条项下所做陈述与保证不真实;

（3）违反本协议约定的其他义务。

14.2 因甲方违约，造成乙方经济损失或导致乙方受到中国人民银行等监管部门处罚，甲方应承担赔偿责任。

▲▲第十五条　不可抗力

由于不可抗力及/或国家政策变化、IT 系统故障、通讯系统故障、电力系统故障、金融危机等非乙方所能控制的原因导致甲方损失的，乙方不承担责任，双方在补充协议中另有约定的除外。前述约定不免除因乙方过错依法应由乙方承担的责任。

第十六条　法律适用及争议解决

16.1 本协议适用中华人民共和国法律（为本协议目的不包括香港、澳门和台湾地区的法律）。

16.2 因本协议而发生的争议，应向乙方所在地有管辖权的法院提起诉讼。争议期间，各方仍应继续履行未涉争议的条款。

第十七条 协议生效与终止

17.1 本协议自甲方法定代表人/负责人或授权代表签字（或盖章）并加盖公章、乙方负责人或授权代表签字（或盖章）并加盖业务章后生效。

17.2 本协议自本协议约定的账户撤销之日终止。

17.3 除本协议另有约定外，在符合法律法规、监管规定的情况下，甲乙双方任意一方均可向对方提出撤销本协议项下账户，具体销户要求及销户流程以双方届时协商情况为准。

第十八条　其他条款

18.1 本协议未尽事宜，按照国家相关法律法规及相关监管要求执行。

18.2 本协议项下经甲乙双方签署的《交通银行开立单位银行结算账户申请书》、《交通银行变更单位银行结算账户内容申请书》、《交通银行撤销单位银行结算账户申请书》以及双方确认的相关文件、资料均为本协议不可分割的组成部分。

18.3 本协议正本壹式贰份，甲方持有壹份，乙方持有壹份，具有同等法律效力。

第十九条 其他约定事项

19.1 本协议第 2.1 条约定的账户信息如下:

（1）户名: _____

（2）账号: _____

（3）账户为_____存款账户。

19.2 本协议第 4.1 条约定的因其他原因需要撤销银行结算账户的情形为: _____

_____

19.3 甲方同意，本协议☐适用☐不适用本协议第 12.2 条。

19.4 联系方式

甲方的联系方式包括:
通讯地址: _____
收件人: _____
邮政编码: _____
电话: _____
移动电话号码: _____
传真: _____
电子邮件地址: _____
乙方的联系方式包括:
通讯地址: _____
收件人: _____
邮政编码: _____
电话: _____
移动电话号码: _____
传真: _____
电子邮件地址: _____

19.5 其他 _____

_____

_____

甲方: _____
法定代表人（负责人): _____
法定地址: _____
乙方: 交通银行_____
负责人: _____

甲方已通读协议全部条款，乙方已应甲方的要求作了详细说明，甲方签署本协议时对所有内容无疑问和异议，理解协议条款尤其是带▲▲标记条款的含义及其法律后果。

甲方（公章）　　乙方（业务章）

法定代表人（负责人）或授权代表　负责人或授权代表
（签字或盖章）　　（签字或盖章）

年　　月　　日　　年　　月　　日

附件 1-2

远程视频银行服务

合法合规性评估报告

北京德和衡律师事务所
BEIJING DHH LAW FIRM

德衡（沪）律审查（2020）第 108 号

北京德和衡（上海）律师事务所

关于远程视频银行服务的

合法合规性评估报告

北京德和衡（上海）律师事务所

二〇二〇年十二月二十八日

第一部分 项目背景

（一）项目背景概述

远程视频银行服务（以下简称“项目”或“应用”），是综合利用实时音视频、智能选路、生物识别、安全加密、双录存储等技术，从惠民服务、普惠金融场景切入，开展远程视频银行业务办理，结合金融级身份认证，运用视频柜员在线作业工具实现高柜、低柜、移动场景业务视频化办理，打造线上线下一体化的金融服务。

该项目将音视频技术与生物识别结合，探索打造远程视频银行，突破物理与空间限制，用户通过移动应用，一键呼叫视频柜员，办理原先到线下网点才能办理的业务，提升银行普惠金融的便捷性。

在本项目中，主要有两方共同参与，包括交通银行股份有限公司（以下简称“交行”或“交通银行”）、腾讯云计算（北京）有限责任公司（以下简称“腾讯云”）。其中，交通银行负责提供业务监管合规、业务系统对接、业务场景应用等能力，腾讯云提供技术支持、音视频平台搭建以及技术和网络安全能力。

（二）备案及许可情况

本项目技术服务方腾讯云计算（北京）有限责任公司的备案及许可情况如下:

1. 增值电信业务经营许可证
许可证编号：B1.B2-20130326

2. 电信与信息服务业务经营许可证
许可证编号：京 ICP 证 150476 号

以下将从技术方法论合规、创新应用场景合规、和服务方式合规三个方面对本金融科技创新应用的合法合规性进行评估分析。

第二部分 技术方法论合规

本项目运用实时音视频、智能选路、生物识别、安全加密、双录存储等技术为交通银行用户提供服务。

实时音视频技术。在客户使用即时视频通讯业务辅助系统与柜员进行音视频交互的过程中，对于音视频的稳定性，延迟方面的客户体验尤为关键，腾讯即时视频通讯业务辅助系统所使用的音视频通道与微信视频、QQ 视频使用同一个通道与技术（腾讯实时音视频

技术-TRTC），处于国际领先的地位。在强大的音视频通道的支持下，确保了优质的客户体验。同时，该技术具备良好的信令及传输协议设计，能满足在目前互联网网络环境下，实现多人视频的高效通话要求，满足包括但不限于：各类满足高画质、抗丢包、抗抖动、低延时、高并发等实时音视频交互要求。传输时对信令及实时音视频数据流进行端对端的安全加密。互联网音视频数据从公网到行内网传输路径复杂，使用不同的运营商网络效率较低，为了保障实时音视频通话效果，支持多节点部署的链路加速及智能路由能力。

智能选路技术。通过监控全网节点的业务高峰、网络抢占等情况，选择最优传输链路，以提升用户体验，保障远程银行业务的时效性。同时，在外网接入时，走经过链路优化的专属视频云通道，获得最佳的传输质量，保证数据的真实性和完整性。

生物识别技术。在与行内系统服务集成对接方面，提供成熟的集成框架和组件，能够实现与行内柜面系统、OCR 识别系统、人脸识别等系统快速集成。所涉及的身份认证服务包括但不限于：OCR 识别身份证、联网核查、人脸识别等。在外围系统集成能力（AI 能力）方面，远程音视频能力平台提供的 SDK 需包含标准 SIP 接口，灵活地与其他外围系统进行对接，并具备与当前主流厂商的 AI 原子能力进行对接的能力，支持对接人脸识别接口、身份证 OCR 识别接口、智能语音（TTS、NLP）交互接口、人脸在框检测接口、电子签名系统接口、对接虚拟人像等能力。平台支持敏感数据脱敏，保障业务信息安全。同时在进行生物识别前，也需通过用户授权等方式，依法合规地开展业务。

安全加密技术。在音视频平台安全能力要求方面，明确要求（1）支持视频媒体流传输加密，支持 RSA 和 AES 组合加密，加密强度达到 AES256，信令流加密支持国密；（2）支持 API 请求 HTTPS 加密；支持防 DDOS 功能，保障互动视频会话安全；（3）支持敏感数据脱敏，保障业务信息安全；（4）支持密钥行方自管理，端对端的严格的安全体系，行方控制加密密钥，满足监管要求；（5）支持小程序视频场景的加密视频通话，以及小程序场景与 APP 场景、PC 端之间的加密视频通话；（6）支持小程序视频场景上的、金融级密码键盘，支持国密。

双录存储技术。平台支持完整的融合双录能力，支持双录文件在服务器端安全录制，而非录制在本地设备，然后再上传，以防文件丢失；能够将互动视频媒体流、PPT 投屏媒体流、双向投屏媒体流完美融合，支持显示定位地址、时间戳，双录视频能够完整的还原整个会话过程，作为法律见证留存至行内存储设备；支持系统对接，将文件存储在行内指定文件平台，数据存储时，在外网不落地，双录文件在银行内网安全隔离、分散存储，严控访问权限，降低数据泄露风险。支持在视频客服管理平台便捷查询和下载相关视频、影像文件，支持查询下载的权限控制和操作审计。

此外，双录存储技术还综合考虑了合规性——可靠证据链（双路备份机制）问题。支持服务端录制的同时，可支持座席端本地录制功能，中央双录+本机双录双路备份，满足

99.99%的可靠证据链要求；在服务端录制文件出现问题时，可手工补录本地录制视频，保障证据链的可靠和数据的完整性。

第三部分 创新应用场景合规

根据腾讯云与交行提供的资料显示，本项目计划用于理财（首次风险评测服务）、信贷（个人贷款线上签约）和柜面（客服、对公开户申请服务）等远程金融服务三个场景。

根据上述三个应用场景的特性，评估方选择以下两种远程银行通用业务处理流程进行合规性评估。尽调资料显示，本项目如有其他业务场景也将参考两种通用业务办理流程中调用远程银行平台的基础能力，实现新的业务场景线上化办理:

（一）视频客服（适用于理财场景）

7 X 24 小时视频银行是本项目最主要的应用，将取代现有的物理网点和柜员，客户远程即可办理原先只能到营业厅办理的复杂金融业务。视频客服场景主要流程如下:

1）客户以“小程序”为入口，在有业务需求时发起视频呼叫;

2）系统收到客户请求，根据业务场景“客服咨询场景”，进行智能路由分配（随机分配至空闲视频柜员，如当前柜员全忙则进入排队队列）;

3）视频柜员通过 pc 坐席端与客户建立视频会话;

4）会话过程中客户共享手机屏幕给视频柜员，柜员查看客户手机屏幕并语音实时指导客户进行操作，屏幕共享内容支持在双录在双录视频中;

5）柜员在视频上推送链接、文字/表情等;

6）视频柜员解决完成客户问题，介绍新产品的 PPT/PDF 多媒体文件，客户手机上可实时看到视频柜员就详解 PPT 产品;

7）客户听完柜员产品介绍后对产品感兴趣，视频柜员可转接第三方专员办理后续业务;

8）转接成功结束会话，客服场景完成。

上述流程中主要涉及的相关个人信息保护合规问题包括:（1）在个人信息收集阶段，交行拟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。（2）个人信息传输、共享阶段，交行需获得用户授权后，客户共享手机屏幕给视频柜员，柜员才可查看客户手机屏幕并语音实时指导。数据传输时，采用端到端加密的方式，通过音视频加密、密钥自管理等方式确保数据不会被第三方破解。（3）个人信息存储阶段，在音视频阶段收集和传输的数据在外网不落地，双录文件在银行内网安全隔离、分散存储，严控访问权限，降低数据泄露风险。（4）个人信息使用阶段，柜员应明确告知客户数据使用范围，不归集、不共享原始数据前提下，控制在行方业务渠道范围内。包括将法律允许范围内的个人信息提供给第三方专员，以便于为客户办理后续业务。但个人信息仅能基于向客户披露的使用目的使用。

根据本项目的个人信息保护合规情况，我们进一步建议交行和腾讯云按照以下标准，准备或更新所必需的合规文件，包括但不限于如下:

（1）隐私政策

（2）用户协议

（3）产品手册（增加数据安全部分）

（4）数据加密脱敏技术和访问控制方案

（5）系统使用说明书（增加数据安全部分）

（6）客户操作运行环境指引

（7）合同以及治理体系

（8）数据处理指引

（9）特殊数据处理提示

（10）数据处理协议

（11）数据传输协议模板

（12）敏感数据及跨境传输手册（如涉及跨境）

（13）数据主体权利手册

（14）软件许可协议（数据安全条款）

（15）数据事故的指令/指南

（16）员工保密协议修订

（17）数据处理记录模板

（18）供应商/合作伙伴《安全技术标准》

（19）供应商/合作伙伴《安全协议》

（20）个人数据收集同意书

（21）个人数据保护影响评估

综上，在落实上述合规要求和文档等基础上，该应用场景基本符合《个人信息安全规范（GB/T35273-2020）》、《个人金融信息保护技术规范（JR/T 0171-2020）》、《银行业金融机构数据治理指引》等法律规定要求。

（二）贷款视频面签（适用于个人信贷场景）

该场景中，客户可通过交通银行 APP、H5、小程序、合作机构嵌入接口，接入交通银行的个人贷款线上签约服务。通过远程线上视频、电子签名、资料上传等交互方式，使客户享受到线上贷款申请、征信授权、合同签订、线上审批等服务，协助解决客户往返网点办理、办理手续繁琐、耗时较长等问题，提升服务体验。贷款视频面签场景主要流程如下:

1）客户通过手机银行、微信银行、小程序等渠道自助办理银行业务。

2）业务办理过程中需要连接远程的视频柜员座席协助办理业务、授权等操作时，发起

视频呼叫;

3）系统收到该视频呼叫请求后根据排队路由规则，排到合适对于的视频柜员座席（可根据客户情况固定分配至特定客户经理或有此业务办理权限的视频柜员）;

4）客户经理或视频柜员通过企业微信座席端、pc、pad 等方式与客户建立视频会话;

5）客户通过该视频会话，通过语音、视频、文本消息、屏幕共享等方式与远程视频柜员座席沟通业务办理需求，完成咨询、身份核验、授权等操作;

6）过程中视频柜员可根据客户的贷款需求，打开贷款合同、还款计划表并通过投屏展示到客户手机，利用电子白板与画笔功能将协议中重要内容圈点讲解和客户确认;

7）讲解完成，推送给客户进行最终确认，完成电子签约;

8）客户完成业务办理，视频通话结束；整个远程视频办理业务过程中涉及的语音、视频、文本消息、截图、文件、屏幕共享等内容通过融合双录完整的记录并存储，方便后续的业务追踪查证。

个人贷款业务合规

根据《个人贷款管理暂行办法》（银监会令[2010 年]第 2 号）第十三条、第十五条规定，贷款人受理借款人贷款申请后，应履行尽职调查职责，对个人贷款申请内容和相关情况的真实性、准确性、完整性进行调查核实，形成调查评价意见。贷款调查应以实地调查为主、间接调查为辅，采取现场核实、电话查问以及信息咨询等途径和方法。因此，本项目开展过程中应当严格履行尽职调查职责，贷款视频面签的创新应用场景并不能免除银行进行实地调查核实的义务。

此外，根据《个人贷款管理暂行办法》规定，贷款人还应根据审慎性原则，完善授权管理制度，规范审批操作流程，明确贷款审批权限，实行审贷分离和授权审批。贷款人应加强对贷款的发放管理，遵循审贷与放贷分离的原则，设立独立的放款管理部门或岗位，负责落实放款条件、发放满足约定条件的个人贷款。

贷款人还应与借款人当面签订书面借款合同（电子银行渠道办理的贷款除外），需担保的应同时签订担保合同。借款合同采用格式条款的，应当维护借款人的合法权益，并予以公示。

综上所述，交行应当严格履行尽职调查职责，建立、执行贷款面谈、借款合同面签制度，将书面借款合同及相关协议格式条款进行公示，以保障在个人贷款业务的受理与调查、风险评价与审批、协议与发放、支付管理和贷后管理等关键环节全面符合《个人贷款管理暂行办法》的规定。

个人信息保护合规

上述流程中主要涉及的相关合规问题与视频客户场景大致相似，包括：（1）在个人信息收集阶段，交行拟通过隐私政策文件、个人信息授权同意书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。特殊情形下，需要电子签署确认后方可开展业务。（2）个人信息传输、共享阶段，交行需获得用户授权后，才能与客户进行屏幕共享等功能。数据传输时，采用端到端加密的方式，确保数据传输安全。（3）个人信息存储阶段，将双录文件在银行内网安全隔离、分散存储，严控访问权限。（4）个人信息使用阶段，柜员应明确告知客户数据使用范围。特别是提示贷款人因逾期未还款等情形下所导致的违约责任，可能会涉及到个人信息使用时，例如："有权扣划借款人在交通银行股份有限公司所有分支机构开立的任一账户中的资金用于清偿"等类似条款，需要对用户进行明确披露，以符合现行法律要求。

由于该场景下，可能涉及收集用户个人生物识别信息。对此评估方特别提示，根据《个人金融信息保护技术规范（JR/T 0171-2020）》第 4.2 条规定，用于用户鉴别的个人生物识别信息（如在音视频采集阶段的人脸信息、指纹信息、声纹信息）属于 C3 类别信息。该类信息一旦遭到未经授权的查看或未经授权的变更，会对个人金融信息主体的信息安全与财产安全造成严重危害。因此需要特别注意数据存储安全问题。此外，第 6.1.4.3 条规定，项目双方不应公开披露个人生物识别信息。

用户身份验证（KYC）合规

进行应用设计时，各项目方应从金融监管层面注意在视频面签时对用户身份进行验证。根据《中国人民银行关于改进个人银行账户服务加强账户管理的通知》，对个人银行账户采用实名制的要求，银行业金融机构为开户申请人开立个人银行账户时，应核验其身份信息，对开户申请人提供身份证件的有效性、开户申请人与身份证件的一致性和开户申请人开户意愿进行核实，不得为身份不明的开户申请人开立银行账户并提供服务，不得开立匿名或假名银行账户。

具体身份核实和监管的流程如下：（一）审核身份证件。对身份证件的实性、有效性和合规性进行认真审查，如仍无法核查开户申请人的信息，应当让开户申请人提供其他辅助材料。（二）核验身份信息。银行可利用政府部门数据库、本银行数据库、商业化数据库、其他银行账户信息等，采取多种手段对开户申请人身份信息进行多重交叉验证。有条件的银行业金融机构可将生物特征识别技术和其他安全有效的技术手段作为核验开户申请人身份信息的辅助手段。（三）留存身份信息。成功开立个人银行账户后，银行应登记存款人的基本信息、与存款人身份信息核验有关的身份证明文件信息、完整的身份信息核验记录，留存存款人身份证件、辅助身份证明文件的复印件或者影印件、以电子方式存储的身份信息，有条件的可留存开户过程的音频或视频等。（四）建立健全个人银行账户数据库。银行应建立健全以存款人为中心的个人银行账户管理系统，按照公民身份号码、护照号等实现对个人银行账户的统一查询和管理。对于存款人为非中国居民的，银行应按照存款人国籍（地区）进行标识并实现对非中国居民银行账户的分类查询和管理。（五）停用或注销银行账户。银行发现或者收到被冒用身份的个人声明，并确认该银行账户为假名或虚假代理开户的，应立即停止相关个人银行账户的使用；在征得被冒用人或被代理人同意

后予以销户，账户资金列入久悬未取专户管理。

此外，企业开户与个人开立账户相似，根据《中国人民银行关于优化企业开户指导意见》（银发〔2017〕288号）第（三）条和第（六）条的规定鼓励银行推广电子渠道开户，包括网上银行、手机银行、微信公众号等开户预约，可在线预提交开户资料，同时企业机构信用代码证的提交进行了豁免。对于企业用户的身份验证，鼓励银行充分利用银行数据库、政府数据库、商业数据等合法、有效的信息平台，交叉验证企业身份信息，提高开户审核的效率和准确度。鼓励银行运用人脸识别、光学字符识别（ORC）、二维码等技术其纳入开户流程，作为读取、手机及核验客户身份信息和开户业务处理的辅助手段。

同时，就账户监管持续性和反欺诈措施，根据《中国人民银行关于加强开户管理及可疑交易报告后续控制措施的通知》（银发〔2017〕117号），银行业金融机构和支付机构应遵循“了解你的客户”的原则，认真落实账户管理及客户身份识别相关制度规定，区别客户风险程度，有选择地采取联网核查身份证件、人员问询、客户回访、实地查访、公用事业账单（如电费、水费等缴费凭证）验证、网络信息查验等查验方式，识别、核对客户及其代理人真实身份，杜绝不法分子使用假名或冒用他人身份开立账户。对于不配合客户身份识别、有组织同时或分批开户、开户理由不合理、开立业务与客户身份不相符、有明显理由怀疑客户开立账户存在开卡倒卖或从事违法犯罪活动等情形，各银行业金融机构和支付机构有权拒绝开户。根据客户及其申请业务的风险状况，可采取延长开户审查期限、加大客户尽职调查力度等措施，必要时应当拒绝开户。

远程视频公证合规——赋强KYC效力（如需）

在面签的过程中，本项目可能还会涉及远程公证的问题。根据《中华人民共和国公证法》、《公证规则》的规定，并无排出远程公证问题的可能性。《中共司法部党组关于加强公证行业党的领导优化公证法律服务的意见》更进一步要求“公证机构2020年底前要全部具备应用电子公证书、在线电子证据保全保管、债权文书网上赋予强制执行效力、海外远程视频公证服务等能力”。这给予了远程视频面签一定的合法地位，同时文书电子化。

实践中，公证机构对于远程视频认证通常的流程为：指导申请人通过扫描二维码进入申办页面、进行线上提交证据材料、线上实人核验、查看文书、电子签名、与公证人员视频连线等操作，待公证员核实完毕，出具公证文书。

远程认证过程中运用的技术手段为：（一）人工肉眼识别；（二）谈话识别；（三）系统识别；（三）人证识别等方式，交叉确认当事人身份。与传统线下公证不同，线上远程公证在完成身份确认后，公证人员进行会通过“一对一”远程视频的方式对申请人所处环境、身体情况等可能影响其真实意思表示的因素进行综合评估，并告知其相应的权利义务及法律风险，待确定业务办理确实是其真实意思表示、且内容合法合规后，才会为其办理相关业务，并要求当事人通过电子签名等方式，对相关材料内容逐一确认。整个公证业务

办理过程需要“双录”留证，即同步录音、录像。期间，如果申请人情况稍有异常变动，如人脸离开视频范围、语言表达出现异常等情况，该公证业务需要立即终止。

鉴于各地对于远程视频公证没有统一的国家层面的规范，几个先行试点区，如《深圳市公证协会指导意见》、《江苏省远程视频公证规范》，对于远程视频公证的范围做如下规定：（一）不涉及财产处分的委托；（二）可接受夫妻之间或父母子女之间处分财产的委托申请；（三）不涉及转移、放弃权利的声明；（四）不涉及处分财产、转移或者放弃权利等文书上的签名。

个人电子签名合规

在进行电子签约时，还需要注意电子签名有效性的问题。以防止因电子签名瑕疵导致的数据授权瑕疵或合同无效等问题。《中华人民共和国电子签名法》第十三条规定，电子签名同时符合下列条件的，视为可靠的电子签名：（一）电子签名制作数据用于电子签名时，属于电子签名人专有；（二）签署时电子签名制作数据仅由电子签名人控制；（三）签署后对电子签名的任何改动能够被发现；（四）签署后对数据电文内容和形式的任何改动能够被发现。 当事人也可以选择使用符合其约定的可靠条件的电子签名。

银行应当与有资质的 CA 合作，开展电子签名业务，同时结合可信时间戳、哈希值校验、区块链等证据收集、固定和防篡改的技术手段或者通过电子取证存证平台认证，证明签约过程的真实性和合法性。

第三方合规审计

在用户通过第三方合作方接口接入时，还应当注意对第三方的数据安全状况进行评估，确保收集、传输个人信息时，已获得用户合法授权。确有必要的情形下，还应当与相关第三方签署《安全协议》，保障用户使用时的数据安全性，并方便金融机构对第三方进行定期安全审计。

基于上述分析，我们进一步建议交行和腾讯云按照以下标准，准备或更新所必需的合规文件，以符合用户身份验证等合规要求，包括但不限于如下:

（1）《客户个人信息保护现状调研报告》；
（2）《客户个人数据分级分类》；
（3）《客户个人信息保护差距评估分析报告》；
（4）《客户个人信息安全合规评估报告》；
（5）客户个人信息数据安全审计模板;
（6）《客户个人信息保护方案》；
（7）《客户个人信息防泄露工具选型报告》；
（8）《客户个人信息使用手册》；
（9）《客户个人信息保护应急响应机制》；

（10）公司内部有关客户个人信息保护的制度模板;

（11）公司与各类合作机构合作中客户个人信息的保护要求以及与合作协议有关的条款模板;

（12）公司与客户签订的贷款协议、客户知情确认书等涉及客户个人信息收集、使用的条款或专门的协议模板;

（13）网站和 App 的用户协议、隐私政策模板;

（14）与客户相关的司法查询制度。

综上，在落实上述合规要求和文档等基础上，贷款视频面签业务场景基本符合《个人信息安全规范（GB/T35273-2020）》、《个人金融信息保护技术规范（JR/T 0171-2020）》、《个人贷款管理暂行办法》等法律规定要求。对于薄弱环节，可以根据本评估报告有针对性地进行改善，以符合现行法律规定。在金融监管和司法公证程序方面，符合审慎监管以及公证文书的合法性的要求。

（三）柜面场景（适用于对公开户）

该场景主要流程如下:（1）办事员在线上提交企业开户信息，中间环节法人呼叫视频坐席；（2）视频柜员核实企业法人身份及真实意愿，法人签署电子协议；（3）审核完成，结束视频。

根据《中国人民银行关于取消企业银行账户许可的通知》、《人民币银行结算账户管理办法》、《中国人民银行关于印发<人民币银行结算账户管理办法实施细则>的通知》规定，境内依法设立的企业法人、非法人企业、个体工商户（以下统称企业）在银行办理基本存款账户、临时存款账户业务（含企业在取消账户许可前已开立基本存款账户、临时存款账户的变更和撤销业务），由核准制改为备案制，人民银行不再核发开户许可证。

银行应当按规定履行客户身份识别义务，落实账户实名制，不得为企业开立匿名账户或者假名账户，不得为身份不明的企业提供服务或者与其进行交易。《中国人民银行关于取消企业银行账户许可的通知》第七条规定，“企业申请开立银行结算账户，应当按规定提交开户申请书，并出具下列开户证明文件:

（一）营业执照。

（二）法定代表人或单位负责人有效身份证件。

（三）法定代表人或单位负责人授权他人办理的，还应出具法定代表人或单位负责人的授权书以及被授权人的有效身份证件。

（四）《人民币银行结算账户管理办法》等规定的其他开户证明文件。…..”

此外，本场景下还涉及用户身份验证（KYC）合规、远程视频公证合规、法人电子签名合规问题，可以参照前述“贷款视频面签（适用于个人信贷场景）”场景执行。法人电子签名还可参照法人一证通的电子签核实。

综上所述，交行银行应负责对企业提交的全部开户申请资料的真实性、完整性和合规性进行审查。同时，严格参照上述法律规定和指引进行人民币银行结算账户开立、使用、变更、撤销与管理。

（四）现行法规、标准支持

在个人信息收集、传输、存储、使用、共享、删除、销毁等数据流各阶段，本应用需严格遵循《个人金融信息保护技术规范（JR/T 0171-2020）》6.1.1-6.1.6 条等相关法律规定，如金融机构应采取技术措施（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。在获得其明示同意后，开展有关个人金融信息的收集活动。对于 C3 类别信息（如：用于用户鉴别的个人生物识别信息），通过受理终端、客户端应用软件、浏览器等方式收集时，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。在数据传输时，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。在数据存储时，应将去标识化、匿名化后的数据与可用于恢复识别个人的信息采取逻辑隔离的方式进行存储，确保去标识化、匿名化后的信息与个人金融信息不被混用。双录数据应存储在行内，切实保障个人信息安全。最后，金融机构内部还应建立个人金融信息销毁策略和管理制度，明确销毁对象、流程、方式和要求。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。

在此基础上，根据《中华人民共和国反洗钱法》、《中华人民共和国商业银行法》、《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、中国银行业监督管理委员会、公安部、国家工商总局关于加强银行卡安全管理预防和打击银行卡犯罪的通知》、《中国人民银行关于改进个人银行账户服务 加强账户管理的通知》、《中国人民银行关于优化企业开户指导意见》、《中国人民银行关于加强开户管理及可疑交易报告后续控制措施的通知》等金融反欺诈、反洗钱的合法合规性要求，切实履行客户身份识别义务，确保申请人开户资料真实、完整、合规。要充分利用联网核查公民身份信息系统，验证客户身份信息。

《中华人民共和国公证法》、《公证规则》及《中共司法部党组关于加强公证行业党的领导优化公证法律服务的意见》的规定给予远程视频公证合法性，通过公证的方式固定开户的过程，增强身份认证过程的公信力。

根据《中国人民银行金融消费者权益保护实施办法》第三十二条规定，“金融机构应当建立个人金融信息使用管理制度。因监管、审计、数据分析等原因需要使用个人金融信息数据的，应当严格内部授权审批程序，采取有效技术措施，确保信息在内部使用及对外提供等流转环节的安全，防范信息泄露风险。”

《个人贷款管理暂行办法》规定，贷款人受理借款人贷款申请后，应履行尽职调查职责，对个人贷款申请内容和相关情况的真实性、准确性、完整性进行调查核实，形成调查评价意见。贷款调查应以实地调查为主、间接调查为辅。贷款人应根据审慎性原则，完善授权管理制度，规范审批操作流程，明确贷款审批权限，实行审贷分离和授权审批，确保贷款审批人员按照授权独立审批贷款。遵循审贷与放贷分离的原则，设立独立的放款管理部门或岗位。按规定建立、执行贷款面谈、借款合同面签制度，借款合同采用格式条款应予以公示。

在对公开户场景中，交行还应当严格落实《中国人民银行关于取消企业银行账户许可的通知》、《人民币银行结算账户管理办法》、《中国人民银行关于印发<人民币银行结算账户管理办法实施细则>的通知》规定。

综上所述，交通银行与腾讯云在进行平台搭建和应用设计阶段，应当充分考虑对数据主体的明示告知义务，包括但不限于向个人用户披露收集的数据类型、数据处理方式和目的、存储期限、与第三方机构合作的合法合规性、数据泄露安全保障措施和相应的应急处理机制，并获得用户的书面授权（包括电子授权）。确保个人金融信息收集、数据传输、处理及融合阶段、组织架构、内部数据安全制度体系符合《信息安全技术 个人信息安全规范》（GB/T 35273-2020）、《个人金融信息保护技术规范（JR/T 0171-2020）》等上述法律法规的合法合规性要求。同时，交行方面还应严格落实《个人贷款管理暂行办法》等法律法规关于个人贷款业务的要求，以及《中国人民银行关于取消企业银行账户许可的通知》、《人民币银行结算账户管理办法》、《中国人民银行关于印发<人民币银行结算账户管理办法实施细则>的通知》对于对公开户业务的合规要求。

第四部分 服务方式合规

（一）面向交行客户

本应用的主要服务流程为用户在 App 端发起呼叫 —— 视频接通 —— 柜员 PPT 展示产品信息 —— 柜员操作交易，投屏给客户 —— 柜员推送客户确认交易要素 —— 客户进行交易验证 —— 交易回单和评价。对于该服务流程的评估情况如下:

本应用通过线上接口服务（包括交通银行 APP、H5、小程序、合作机构嵌入接口）为交通银行企业用户提供全天候的应用服务，同时采取多种措施保护交行客户信息的隐私性和安全性。本应用严格遵循央行“用户授权、最小够用、全程防护“的数据治理原则:

（1）在数据采集时，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，获取用户授权后再进行采集;

（2）在数据使用时，借助标记化、加密等技术，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。但在特殊场景下，例如贷款人因逾期未还款等情形下依法申请强制执行时，可能会向第三方披露相关可识别的个人信息，对此应当提前对客户予以披露，并应获得用户明示授权;

（3）在数据存储时，通过不可逆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。

（4）在数据传输时，需要对数据进行加密和脱敏。原则上，在中华人民共和国境内提供金融产品或服务过程中收集和产生的个人金融信息，应在境内存储、处理和分析。另外，由于本应用可能会出现用户在境外使用涉及跨境传输的问题，应根据《个人金融信息保护技术规范（JR/T 0171-2020）》第 7.1.3 条规定进行处理: “因业务需要，确需向境外机构（含总公司、母公司或分公司、子公司及其他 为完成该业务所必需的关联机构）提供个人金融信息的，具体要求如下:

- 应符合国家法律法规及行业主管部门有关规定;
- 应获得个人金融信息主体明示同意;
- 应依据国家、行业有关部门制定的办法与标准开展个人金融信息出境安全评估，确保境外机构数据安全保护能力达到国家、行业有关部门与金融业机构的安全要求;
- 应与境外机构通过签订协议、现场核查等方式，明确并监督境外机构有效履行个人金融信息保密、数据删除、案件协查等职责义务。”

（5）同时，本应用建立了风险补偿机制和退出机制，为可能存在的风险隐患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。当满足退出条件时，本应用会按照退出方案中止有关服务并及时告知客户，对客户造成的损失予以赔偿。

（二）技术架构

根据尽调材料显示，本应用将支持混合部署，其中音视频通信过程中，腾讯云作为技术服务商对数据不留存。所有业务应用服务及其数据，支持私有化部署在银行数据中心，由银行控制全部用户个人数据。

根据《个人金融信息保护技术规范（JR/T 0171-2020）》第 6.1.2-6.1.3 条显示，通过公共网络传输时，C2、C3 类别信息应使用加密通道或数据加密的方式进行传输，保障个人金融信息传输过程的安全；对于 C3 类别中的支付敏感信息，其安全传输技术控制措施应符合有关行业技术标准与行业主管部门有关规定要求。在进行存储时，C3 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。

对于音视频通信数据，评估方建议在传输时应当严格履行前述义务，做到数据不留存，合法合规地开展业务。对于所有业务应用服务及其数据，建议部署在银行数据中心，处于交行可控网络内，并进行有效的访问控制。

（三）第三方软件开发工具包 SDK 安全

根据项目资料显示，本项目中远程音视频能力平台提供的 SDK 需包含标准 SIP 接口，灵活地与其他外围系统进行对接，并具备与当前主流厂商的 AI 原子能力进行对接的能力。

考虑到系统交互可能会产生数据安全风险，对于 SDK 的技术安全标准可以参考《网络安全标准实践指南—移动互联网应用程序（App）中的第三方软件开发工具包（SDK）安全指引（征求意见稿）》所列的相关标准。

同时，由于《移动互联网应用程序（APP）SDK 安全指南》（以下简称“《指南》”）编制工作研讨会已经召开，该《指南》由全国信息安全标准化技术委员会公示立项，将根据《中华人民共和国网络安全法》等相关法律，从 SDK 安全开发、SDK 个人信息安全、App 集成安全等方面，提出 SDK 控制者在开发、运营、个人信息处理、数据安全管理、跨境管理等环节应遵循的原则和安全措施。建议本项目进展过程中，技术支持方腾讯云能够参照现行有效的法律法规和国家标准对相关的 SDK 技术安全问题进行审查和改善。

（四）现行法规、标准支持

根据《中国人民银行金融消费者权益保护实施办法》第三十条规定，“金融机构通过格式条款取得个人金融信息书面使用授权或者同意的，应当在条款中明确该授权或者同意所适用的向他人提供个人金融信息的范围和具体情形，应当在协议的醒目位置使用通俗易懂的语言明确向金融消费者提示该授权或者同意的可能后果。”

《中国银监会办公厅关于加强银行业金融机构内控管理有效防范柜面业务操作风险的通知》规定“十、 加强客户信息安全管理。银行业金融机构应加强对接触客户信息岗位的权限管理和行为管理，特别关注互联网环境下新兴业务应用、交易系统存在的客户信息泄露隐患，确保对可能产生信息泄露的环节有足够的监测和管控能力；对信用卡持卡人信息、网上银行业务客户信息等，应提高风险防范级别，加强风险管控措施。

根据《中国人民银行关于金融机构进一步做好个人金融信息保护工作的通知》第一条规定，“依法合规收集、保存、使用和对外提供个人金融信息，不得向任何单位和个人出售客户个人金融信息，不得违规对外提供客户个人金融信息。”《个人金融信息保护技术规范（JR/T 0171-2020）》第 6.1.4、7.2.2 条也有类似规定。

根据《信息安全技术 个人信息安全规范》（GB/T 35273-2020）第四条规定，“个人信息控制者开展个人信息处理活动应遵循合法、正当、必要的原则，具体包括：a) 权责一致——采取技术和其他必要的措施保障个人信息的安全，对其个人信息处理活动对个人信息

主体合法权益造成的损害承担责任；b)目的明确——具有明确、清晰、具体的个人信息处理目的；c) 选择同意——向个人信息主体明示个人信息处理目的、方式、范围等规则，征求其授权同意；d) 最小必要——只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量。目的达成后，应及时删除个人信息；e) 公开透明——以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则等，并接受外部监督；f) 确保安全——具备与所面临的安全风险相匹配的安全能力，并采取足够的管理措施和技术手段，保护个人信息的保密性、完整性、可用性；g) 主体参与——向个人信息主体提供能够查询、更正、删除其个人信息，以及撤回授权同意、注销账户、投诉等方法。”

根据《信息安全技术 个人信息安全规范》（GB/T 35273-2020）第六条第一款的规定，“对个人信息控制者的要求包括： a) 个人信息存储期限应为实现个人信息主体授权使用的目的所必需的最短时间，法律法规另有规定或者个人信息主体另行授权同意的除外；b) 超出上述个人信息存储期限后，应对个人信息进行删除或匿名化处理。”；同时该规范第六条第二款规定，“收集个人信息后，个人信息控制者宜立即进行去标识化处理，并采取技术和管理方面的措施， 将可用于恢复识别个人的信息与去标识化后的信息分开存储并加强访问和使用的权限管理。”本项目中，交行作为个人信息控制者和金融机构还应遵守该规范第十、十一条规定，建立个人信息安全事件应急处置和报告体系，完善个人信息保护组织架构和内部制度体系。

根据《中华人民共和国个人信息保护法》（征求意见稿）对处理个人信息的企业提出了“风险评估—记录—保存”的要求（第 38 条、第 54 条）。企业对个人有重大影响的信息处理活动，在事前要开展风险评估和记录，评估事项包含：处理敏感个人信息；利用个人信息进行自动化决策；委托处理个人信息、向第三方提供、公开个人信息；向境外提供个人信息等。风险评估的内容包括：个人信息的处理目的、处理方式是否合法、正当、必要；对个人的影响及风险程度；所采取的安全保护措施是否合法、有效并与风险程度相适应。

综合上述事实和法律规定，交行和腾讯云应在确保系统业务连续性、数据和资金安全的前提下，秉持安全优先、对用户负责的原则，充分采取法律和技术数据安全措施，避免可能存在的风险隐患。在服务提供和事故处理阶段应当充分遵循“最小必要性”原则，收集和使用用户数据时应事先告知其使用目的，征得数据主体的书面同意。同时应对所获取的个人数据进行脱敏和加密处理，分开存储可用于恢复识别个人的信息和去标识化后的信息。

此外，交行和腾讯云应制定完善的内部数据安全制度（包括访问权限设置、员工保密义务、操作指引、系统安全运行环境指引、数据安全保护标准等）、安全事件应急预案和风险补偿机制，保障数据主体的数据安全，在事故发生后及时对其损失进行赔偿。双方应确保个人数据从收集到使用到删除均符合《中国人民银行金融消费者权益保护实施办

法》、《信息安全技术 个人信息安全规范》（GB/T 35273-2020）、《个人金融信息保护技术规范》（JR/T 0171-2020）、《中华人民共和国个人信息保护法》（征求意见稿）等法律法规的合规要求。

在本应用中，腾讯云还应当坚守技术服务方的角色，坚持不控制、不处理相关的个人数据的，仅提供相应的技术支持服务的原则，以避免因收集、处理个人数据等问题产生附加的数据安全保护义务。同时，在数据处理协议或技术服务协议中，明确自身的数据处理权限和安全义务，以厘清合同各方的法律义务和责任。

在此基础上，保障业务流程符合《中国银监会办公厅关于加强银行业金融机构内控管理有效防范柜面业务操作风险的通知》等法律规定。

第五部分 结论意见

在项目具体进展过程中，评估方仍需深入开展调查、考察交通银行股份有限公司、腾讯云计算（北京）有限责任公司合作项目，特别是针对个人客户前端数据授权、用户身份验证（KYC）、远程视频公证、电子签名等情景以及实时音视频、智能选路、生物识别、安全加密、双录存储等技术环节的合法合规性问题，并协助各方建立健全相关的数据安全和隐私合规体系。

在前述基础上，我们认为，交行和腾讯云合作开展的远程视频银行服务是合法合规的，可以依法开展进一步的研发和实施。

——本评估报告正文结束——

第六部分 签署页

（本页无正文，为《北京德和衡（上海）律师事务所关于远程视频银行服务的合法合规性评估报告》签署页）

本评估报告仅作为交通银行股份有限公司、腾讯云计算（北京）有限责任公司合作的“远程视频银行服务”央行课题项目联合申报之目的使用，非经本所事先书面同意，本评估报告不得用作其他目的。

本评估报告正本贰份，无副本。

本评估报告的出具日为二零二零年十二月二十八日。本报告有效期自出具之日起一年。

北京德和衡（上海）律师事务所

经办律师： 陈国彧律师

娄 鹤律师

附录 主要参考法律法规及标准

序号	法律法规和政策名称	主要章节及条款
1	中华人民共和国网络安全法	第四章
2	中华人民共和国个人信息保护法（征求意见稿）	第 38 条、第 54 条
3	中华人民共和国消费者权益保护法	第二十九条
4	中华人民共和国反洗钱法	第五条、第十九条
5	中华人民共和国电子签名法	第十三条
6	中华人民共和国公证法	第四章、第五章
7	全国人民代表大会常务委员会关于加强网络信息保护的决定	第一至十条
8	国务院办公厅关于加强金融消费者保护工作的指导意见	第三条第（十）项
9	中国人民银行、信息产业部关于商业银行与电信企业共享企业和个人信用信息有关问题的指导意见	第三条、第四条
10	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	第三条、第二十八条
11	中国人民银行关于改进个人银行账户服务加强账户管理的通知	第一条
12	中国人民银行关于优化企业开户指导意见	第（三）条、第（六）条
13	中国人民银行关于加强开户管理及可疑交易报告后续控制措施的通知	第一条、第二条
14	中国人民银行金融消费者权益保护实施办法	第三章
15	中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知	第二至九条
16	中国人民银行关于金融机构进一步做好个人金融信息保护工作的通知	第一条
17	《中国人民银行关于取消企业银行账户许可的通知》	第一章、第二章
18	《人民币银行结算账户管理办法》	第一章、第二章
19	《中国人民银行关于印发<人民币银行结算账户管理办法实施细则>的通知》	第一章、第二章
20	金融数据安全 数据安全分级指南（JR/T 0197—2020）	第 5 条
21	中国银监会办公厅关于加强银行业金融机构内控管理有效防	第三、十、十一条

	范柜面业务操作风险的通知	
22	个人贷款管理暂行办法	第十三条、第十五条、第二十条、第二十三条、第二十七条
23	商业银行互联网贷款管理暂行办法	第十、十七、十八、二十一、二十三条
24	个人信用信息基础数据库管理暂行办法	第十二条
25	银行业金融机构数据治理指引	第五章
26	银行业消费者权益保护工作指引	第十二条
27	电信和互联网用户个人信息保护规定	第一章、第二章、第三章
28	个人金融信息保护技术规范（JR/T 0171-2020）	第 6. 1. 1 条至 6.1.6 条、第 7.1.3 条、7.2.2.条
29	个人信息安全规范（GB/T35273-2020）	第 4、7.3、7.6 条

附件 1-3

远程视频银行服务
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）、《网上银行系统信息安全通用规范》（JR/T 0068—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，并从技术架构、应用场景、安全机制、运维容灾、权限控制和隐私保护等方面进行全面安全评估，采取了有效的技术和管理手段进行针对性安全增强，方案合理有效。经评估，本项目符合现有相关行业标准要求。

腾讯云计算(北京)有限责任公司

2020 年 11 月 25 日

附件 1-4

远程视频银行服务
风险补偿机制

本项目针对可能存在风险隐患，按照由申请各方联合建立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，根据责任认定结果，由相关责任方提供全额补偿，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综合评估，并合法合规予以项目运行。

二、保护客户授权的各类信息安全，确保相关数据信息仅用于项目项下的对应业务需求。

三、如相关业务出现违约风险，将通过法律诉讼等途径合理、有效解决。

四、基于项目项下由参与各方共同提供的金融服务，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。

五、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

远程视频银行服务
退出机制

本项目按照由申请各方联合建立的退出机制，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、如项目未达到监管部门或项目两方目标要求，或运营过程中存在重大问题且无法解决的，或在运营过程中经评估发现存在重大风险隐患不适合项目继续运行的，及时终止项目和数据的使用，对涉及的相关数据按照国家及金融行业相关规范要求做好数据清理工作。

二、如项目顺利运行至项目结束期后，且两方对平台整体运行满意且符合合规性要求，经两方共同协商后，可续签相关协议并对平台进行持续化运营，并根据实际业务情况扩大数据使用范围。

三、如项目顺利运行至项目结束期后，但两方共同协商后不继续运营平台，则合作协议不再续签。项目合作到期后，合作各方各自清理音视频加密节点、交互网关、数据库基础组件及相关数据。

附件 1-6

远程视频银行服务
应急预案

本项目按照由申请各方联合建立的应急处置预案，针对不同的问题提供相应的解决方案，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。具体应急预案包括但不限于以下内容：

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，而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。