《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	91310000736239890T-2020-0003	
	创新应用名称	基于多方安全计算的图像隐私保护产品	
	创新应用类型	科技产品	
	机构信息 1	统一社会信用代码	91310000736239890T
		全球法人识别编码	300300TAPEDMG3FF9T41
		机构名称	中国银联股份有限公司
		持有金融牌照信息	牌照名称：银行卡清算业务许可证 机构编码：BCCI001 发证机关：中国人民银行、中国银行保险监督管理委员会
	机构信息 2	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 3	统一社会信用代码	91110108MA01EGPQX2
		全球法人识别编码	无
		机构名称	华控清交信息科技（北京）有限公司
		持有金融牌照信息	无
	机构信息 4	统一社会信用代码	913101105680842868
		全球法人识别编码	无
		机构名称	上海聚虹光电科技有限公司
		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.使用图像识别技术，在用户授权的前提下，对手机 POS 采集到的商户责任人或收银员图像进行特征提取，并将提取到的图像特征与交通银行和中国银联两个独立主体存储的图像特征进行比对，实现对商户责任人和收银员身份的一致性核验。 2.采用多方安全计算技术，将采集提取的特征信息进行随机切片、传输并存储至交通银行和中国银联两个独立的主体，避免由于独立主体单独存储用户的图像特征原图带来的数据泄露风险。身份验证时，通过将商户责任人和收银员身份验证时采集提取的图像特征进行随机切片，并与交通银行和中国银联存储的密文切片进行比对，在不泄露各切片的原始信息基础上实现商户责任人和收银员身份准确识别，有效保护了商户责任人和收银员隐私信息安全。	

	功能服务	本项目综合运用多方安全计算、图像识别技术，在手机 POS 上提供商户责任人、收银员身份验证服务，有效核实商户责任人和收银员身份，解决传统收单管理中设备、人工验证带来的管理漏洞，在保护商户责任人和收银员隐私安全的基础上有效提升收单机构反欺诈、反洗钱等风控能力，降低收单机构运营成本。 本项目由中国银联股份有限公司、交通银行股份有限公司联合设计研发及运维，中国银联股份有限公司提供产品支持和多方安全计算平台环境部署，交通银行股份有限公司提供金融应用场景和多方安全计算平台环境部署，上海聚虹光电科技有限公司提供图像识别的算法技术支持，华控清交信息科技（北京）有限公司提供多方安全计算的技术支持，此外无其他第三方机构参与。
	创新性说明	1.图像数据存储方面，将图像特征数据进行随机切片后分别存储在多个独立主体，避免了金融机构单独存储图像隐私信息的风险，同时也保护了用户的隐私数据安全。 2.图像特征计算方面，运用多方安全计算的联合验证技术，保证用户图像特征在密文切片的形态下，仍然能够完成身份信息的验证，从而保障了整体方案的安全、有效。 3.算法更新方面，客户端只需维护一个版本的算法模块，当需要对图像识别算法进行更新时，通过平滑升级机制在新一次的验证过程中同时更新特征并替换算法版本，降低客户端的处理与存储开销。 4.收单业务风控方面，运用图像识别、多方安全计算技术，在核实商户责任人和收银员身份的同时，有效提升收单机构反欺诈、反洗钱等风控能力。
	预期效果	1.不改变现有移动端验证流程和运行体验的前提下，提升客户端图像识别验证的隐私保护能力，降低信息泄露风险。 2.本产品对于图像特征进行随机切片存储，任意一方都无法获得完整特征数据，降低金融机构单独存储图像特征的风险。
	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，未来预期提供每月 10 万次的注册与比对服务调用量。
创新应用服务信息	服务渠道	线上渠道：手机 POS 的 APP
	服务时间	7 × 24 小时
	服务用户	交通银行商户责任人和收银员
	服务协议书	《服务协议书-基于多方安全计算的图像隐私保护产品》（见附件 1-1）
合法合规性评估	评估机构	交通银行股份有限公司
	评估时间	2020 年 12 月 30 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）、《银行卡收单业

		务管理办法》（中国人民银行公告〔2013〕第9号公布）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-基于多方安全计算的图像隐私保护产品》（见附件1-2）		
技术安全性评估	评估机构	中国银联股份有限公司电子支付研究院		
	评估时间	2020年12月10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）、《移动金融客户端应用软件安全管理规范》（JR/T 0092—2019）、《移动终端支付可信环境技术规范》（JR/T 0156—2017）、《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图像隐私保护产品》（见附件1-3）		
风险防控	风控措施	1	风险点	项目应用过程中可能存在用户数据的泄露、篡改和滥用风险。
			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，通过数据泛化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，借助多方安全计算等技术，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。
		2	风险点	目前业务的部署模型为通信密集型，对于网络的要求相对较高，如果产生剧烈网络波动可能产生不可预知的影响。
			防范措施	建立网络维护和预警机制。建立主备网络，网络部署过程中尽量将通信流程设计为局域网访问，并使用网络专线进行外部访问；建立网络日常维护和监控的章程，做到及时告警。
		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（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应急处理预案（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，及相应的违规处理办法，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	交通银行客服热点 95559，选择人工服务联系客服代表。	
		投诉受理与处理机制	交通银行收到投诉后，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。 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）		

附件 1-1

基于多方安全计算的图像隐私保护产品
交通银行特约商户支付受理业务协议书

重要提示：

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

甲方：为乙方开通本协议项下支付产品受理业务的交通银行有限公司网点所属的省分行或直属分行

乙方：申请并办理本协议项下支付产品受理业务的商户

为了适应支付业务发展，改善支付环境，繁荣市场，促进消费，共同发展，甲乙双方经平等、友好协商，就有关事项达成如下协议，双方共同遵守，恪守信用。

本协议书分为三部分：第一部分为一般条款，第二部分为银行卡支付受理业务附加条款，第三部分为条码支付受理业务附加条款。

第一部分条款适用于所有的支付受理业务;银行卡支付受理业务除应适用第一部分条款外，还应适用第二部分条款；条码支付受理业务除应适用第一部分条款外，还应适用第三部分条款。

第一部分 一般条款

一、乙方愿意接受银行卡持卡人及条码（含二维码及一维码）支付产品使用人（上述人员在下文中统称为“消费者”）使用甲方发行、代理和认可的，带有“银联”/“VISA”/“MasterCard”/“JCB”/“DINERS”/“Discover”标识的银行卡或甲方发行、代理和认可的加

载支付账户信息的二维码或一维码支付信息(以下简称“条码支付”，包括银联条码支付、微信条码支付、支付宝条码支付）进行交易，按甲方制订的操作规程为合法消费者提供直接购物或支付其它费用的服务，并向甲方支付手续费。除非因不可抗力及/或 IT 系统故障、通讯系统故障、电力系统故障等非甲方所能控制的原因，甲方于每个交易日(即有交易产生的自然日,下同)结束后计算当日发生交易金额，在扣除手续费后，于交易日后的第 1 个工作日（指甲方对公业务营业日，下同）将剩余款项划入乙方指定账户。双方在补充协议中另有约定的除外。

乙方按约定受理下列标题前标示“√”的支付产品，并按对应标准向甲方支付交易手续费。双方另有约定，则以另行约定为准。

<table>
<tr><td colspan="2">☐ 受理境内银行卡</td></tr>
<tr><td>☐ 银联借记卡
手续费标准：</td><td>☐ 银联信用卡
手续费标准：</td></tr>
<tr><td colspan="2">☐ 受理境外银行卡</td></tr>
<tr><td>☐ 银联卡
手续费标准：</td><td>☐ VISA 卡
手续费标准：</td></tr>
<tr><td>☐ MasterCard 卡
手续费标准：</td><td>☐ JCB 卡
手续费标准：</td></tr>
<tr><td>☐ DINERS 卡
手续费标准：</td><td>☐ Discover 卡
手续费标准：</td></tr>
<tr><td colspan="2">☐ 受理条码支付</td></tr>
<tr><td>☐ 银联条码支付</td><td>☐ 微信条码支付</td></tr>
</table>

手续费标准：__	手续费标准：__
□ 支付宝条码支付 手续费标准：	/

二、甲方或由甲方指定的第三方服务机构为乙方提供银行卡或条码支付收单及专业化服务，主要包括商户签约、培训、终端设备（以电子信息的形式上传及接收交易信息的可移动或固定的机具设备，例如 POS 机等。下同）安装、台卡贴码布放、日常维护、资金清算、账务查询及调整等工作。

▲▲三、乙方在办理银行卡或条码支付业务时，应保证遵守下列各项约定：

（一）提供必要的营业设施和安全防范设施，确保终端设备的正常使用，并须妥善管理放置在乙方经营场所的静态及动态二维码（条码），防止二维码（条码）被篡改。承担因本方原因造成的终端设备的损失。

（二）不得以任何形式通过银行卡或条码支付交易支付任何形式的资金（包括现金、支票、银行转款等）给消费者。

（三）除非经过甲方的书面允许，否则乙方不得将受理银行卡或条码支付的业务委托或转让给第三方。

（四）乙方不得将签购单、签购结算单、受理支付产品标识牌、终端设备用于本协议许可范围以外的用途，也不得给本协议许可范围以外的第三方使用。

（五）乙方不得将任何第三方的交易假冒乙方交易进行清算。

（六）不得涂改签购单内容、故意避开授权规则进行分单操作。

（七）对消费者提出符合规定的刷卡、挥卡、扫码消费要求，乙方不得无故拒绝。

（八）不得拒绝受理任何符合甲乙双方约定的受理产品范围内的银行卡或条码支付信息（银行卡或条码支付受理结算系统、终端设备故障除外）。

（九）乙方对消费者使用银行卡或条码支付费用应与支付现金一视同仁，不得有任何歧视行为，不得向消费者收取任何费用，且消费者应享受与现金消费者及其他顾客完全相同的服务。

（十）乙方应将交易签购单（商户联）及相关的原始交易信息和凭证等（如该支付业务有）妥善保存。保存期限自交易日起不少于5年，以便甲方及与本协议项下交易相关的发卡机构或第三方支付公司(支付宝（中国）网络技术有限公司,财付通支付科技有限公司及其他依法取得《支付业务许可证》的非金融机构,下同)（以下简称发卡机构或第三方支付公司）在需要时查对。

（十一）对于甲方及发卡机构或第三方支付公司的投诉，应根据甲方要求妥善处理，并予以及时回复。

（十二）乙方发现消费者交易异常的，应及时通知甲方，乙方应根据甲方要求配合调查和提供交易信息和凭证。

▲▲四、乙方应按甲方规定，准确、完整、真实地提供证照、业务资料及相关信息，因本协议约定的乙方通讯资料不准确而造成乙方接收不到甲方发送的相关资料，甲方不承担责任。

乙方同意，甲方有权出于审核本协议项下业务、核实乙方个人身份的目的，在本协议有效期内随时向中国人民银行征信中心个人信用

信息基础数据库查询乙方全部信用信息。无论本协议项下业务是否审核通过，甲方均有权保留依据本条款查得的信用信息。如甲方超越授权范围查询或使用乙方信用信息，甲方应承担相应法律责任。

同时，乙方同意在本协议有效期内，甲方出于业务管理需要，甲方有权向任何有关部门(如乙方营业执照（如有）颁发地当地工商行政管理机构)、单位和个人了解、查询其经营资质、经营情况、其企业法定代表人和其他有关方面的信息，并同意甲方保留和使用上述信息和资料。如甲方超越授权范围查询或使用乙方前述信息，甲方应承担相应法律责任。

乙方提供的乙方及乙方人员相关证照过期时，甲方有权要求乙方提供更新后的证照；如乙方不提供的，甲方有权暂停对乙方的所有服务，在协议有效期内，乙方向甲方提供更新后的证照的，甲方可恢复对乙方提供服务。

五、乙方经营情况发生变更时，须提前 10 个工作日书面通知甲方并按照甲方的要求提供证明材料，经营情况变更包括但不限于以下事项：

（一）变更单位名称、开户名称、开户银行、账号、法定代表人、负责人姓名、地址、电话、注册资本等；

（二）发生停业、经营范围变更、转让、倒闭、被采取财产保全措施等情况；

（三）乙方所有权结构变更；

（四）乙方业务经营或销售方式变动，特别是要新增开展邮购、电话订购、网上订购、批发等业务经营方式时。

六、甲方根据信用卡组织（中国银联/威士卡组织/万事达卡组织/JCB 卡组织/大来卡组织/发现卡组织,下同)、第三方支付公司及具备合法资质的清算机构（ 中国银联/中国网联,以下简称清算机构）有关规则进行业务处理，需事先将相关条款以书面通知方式告知乙方，双方应严格遵守。若前述信用卡组织、第三方支付公司或清算机构有关规则发生变更，甲方知悉后应当及时以书面方式告知乙方。

▲▲七、当甲方或其他交易参与机构提出查询或账务调整要求时，乙方应积极配合，并从收到要求之日起，在两个工作日内将反馈意见及相关证明材料返回甲方进行处理，否则，甲方将以乙方无异议或不能提出相关证明材料为由进行相关业务及账务处理。乙方如有调账要求也必须在信用卡组织、第三方支付公司、清算机构规定时限内提出，否则甲方将不予以受理。

▲▲八、如乙方未按照本协议第三、四、五、七条约定执行的，甲方有权依据本协议第十二条处理。

▲▲九、乙方在受理银行卡时只能将银行卡在甲方提供的终端设备或其他甲方规定可以使用的终端设备上操作，乙方不得使用其他未经过甲方许可的终端设备读取银行卡信息。乙方受理条码支付时需使用甲方提供的终端设备或条码完成交易信息传输，并应要求消费者确认交易金额以及商品及服务已交付。

▲▲十、信息披露与保密：

（一）乙方必须妥善保管甲方及发卡机构或第三方支付公司的所有交易信息资料，未经权利人事先同意，不得将任何的银行卡或条码支付交易信息及资料(包括但不限于消费者姓名、账户号等以及所

有关于使用支付工具交易的有关资料)用作交易对账工作之外的其他用途或向任何第三方透露。

（二）对于在本协议签订和履行过程中获取和知悉的乙方未公开信息和资料，甲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.甲方为行使本协议项下权利及履行本协议项下义务向信用卡组织、清算机构、甲方外部专业顾问或第三方支付公司披露和允许信用卡组织、清算机构、甲方的外部专业顾问或第三方支付公司在保密的基础上使用的；

4.乙方同意或授权甲方进行披露的。

（三）除双方另有约定外，乙方进一步同意交通银行股份有限公司在如下情形可以使用或披露所有有关乙方的信息和资料，包括但不限于乙方的基本信息、交易信息及其他相关信息和资料等，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、信用卡组织、第三方支付公司、清算机构、其他金融机构及甲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，披露和允许其使用该等信息和资料：①为开展特约商户受理银行卡支付、条码支付业务或与特约商户受理银行卡支付、条码支付业务有关；②为甲方向乙

方提供或可能提供新产品或服务或进一步提供服务。

▲▲十一、如因乙方违反第九条、第十条第（一）款约定，造成资料与终端设备保管不当，致使银行卡或条码信息失密或被盗用，前述银行卡或条码信息失密或被盗用引发的纠纷及争议，应由乙方负责解决，甲方有权依照本协议第十二条进行处理。如因甲方违反第十条第（二）、（三）款约定，致使乙方的商业秘密被用作他途或被泄密，造成乙方经济损失的，甲方应依法承担相应的赔偿责任。

▲▲十二、若乙方违反第三、四、五、七、九条，第十条第（一）款，第二十九条中任一约定，或者有下列情形之一，因此产生的甲方损失或/和乙方损失及他方损失均由乙方全部承担，且甲方有权立即解除本协议，并可采取终止乙方的银行卡及条码支付交易、收回业务终端设备、台卡贴码及与交易相关的所有凭证、停止支付所有清算款项、从乙方在甲方开立的任一账户中扣回相关款项，以及其他必要的资产保全措施。甲方将在解除协议的同时，将乙方相关信息报送至清算机构不良信息共享系统，并向执法、监管部门通报：

（一）虚假申请：以虚假资料或盗用其他商户资料向甲方申请为特约商户。

（二）侧录：乙方默许、纵容、与他人共谋或发现后不制止他人在终端设备上装载侧录仪器，盗录消费者磁条信息，出卖给伪卡制作集团或自行制作伪卡。

（三）非法泄露账户及交易信息：乙方违反保密条款，将消费者所使用的账户资料及交易数据信息泄露给不法分子使用。

（四）套现：乙方与消费者或其他第三方勾结，或乙方自身以虚

拟交易套取现金。

（五）洗单：乙方将其他未签约商户的交易在本商户的终端设备上进行刷卡、扫码或在压印机上压卡，假冒本店交易与甲方结算。

（六）恶意倒闭：乙方接受消费者支付的预付款后故意破产，使甲方承担退单损失。

（七）虚假交易：在消费者不知情的情况下利用其账户编造虚假交易或在消费者消费的同时重复交易，并冒用消费者的交易验证信息进行虚假交易。

（八）伪冒交易：一定时期内的非正常交易超过甲方规定的比率。

（九）盗刷：假冒真实消费者身份或变更银联卡、条码支付账户信息后进行欺诈交易。包括变更账户信息后进行交易、手输银行卡号交易或非面对面交易。

（十）名义经营范围与实际情况不符：乙方名义上经营正常，或以正常名义申请成为特约商户后，实际从事禁入商户类型的经营活动。

（十一）违规移机：乙方未经甲方许可，擅自将 POS 机具从登记的经营装机地址转移至另一地址，包括但不限于以下情形：移机后地址与原装机地址的省市、区县、乡镇等行政区域，或与原装机地址的道路名称、门牌号码、楼层、房间号和摊位号不一致；同一商户在多家分店之间自行调换终端设备；使用固定机具上门或流动收款等业务。

（十二）移动终端设备在未经甲方许可的范围外使用。

（十三）因银行卡或条码支付欺诈交易已被司法机关立案或介入调查。

（十四）银行监管机构已书面通知甲方须与乙方解约。

（十五）已被监管机构或其他信用卡组织、第三方支付公司、清算机构认定为“高风险商户”。

（十六）经营不善，停业整顿、申请解散、申请破产以及已停业或破产。

（十七）被工商部门注销登记、吊销营业执照；由于违反国家法令、法规或相关行业管理规定，被有关机关查处。

（十八）利用本协议项下业务从事恐怖融资、洗钱、逃税等犯罪活动的。

（十九）其他违反监管机构、信用卡组织、清算机构 、第三方支付公司或甲方商户风险管理规定的行为。

以上所列风险发生时，乙方同意甲方及信用卡组织、清算机构 、第三方支付公司使用其所涉及的业务风险的所有相关信息。

▲▲十三、乙方同意，甲方有权对其交易进行监控 ，并有权根据监控情况拒绝交易请求、延迟结算。当乙方有下列情形之一时，甲方有权对乙方全部或部分清算款项进行延迟结算处理，及/或从乙方当日或以后交易款，及/或乙方在甲方开立的任一账户中扣回相关款项，并依据实际情况决定何时划回发卡银行及消费者。如经甲方认定，乙方需返还或赔偿的金额小于甲方已从乙方的清算款中或其在甲方的任一账户中暂扣的资金，甲方将在有关业务处理流程完毕后，将差额部分返还乙方银行结算账户或其他指定的同名银行结算账户：

（一）乙方在受理银行卡刷卡交易时在签购单上未留有消费者签名，或消费者签名与银行卡签名栏预留签名明显不符，或银行卡上无预留签名或预留签名字迹模糊不清、有涂改（无卡片出现的支付信息

类交易除外），或发生乙方书面确认的重复扣款交易等。

（二）签购单上交易明细与实际交易情况不符。

（三）自交易日期起，交易流水上送时间超过第三方支付公司、信用卡组织或清算机构相关规定。

（四）乙方未在甲方及信用卡组织或清算机构或第三方支付公司要求的，符合信用卡组织或清算机构或第三方支付公司关于查询类业务反馈时效的规定时限内，对甲方及发卡机构或第三方支付公司所提出的查询信息进行反馈。

（五）乙方未在甲方及信用卡组织或清算机构或第三方支付公司要求的，符合信用卡组织或清算机构或第三方支付公司关于异常交易帐务调整流程所规定的时限内，对甲方及发卡机构或第三方支付公司所发出的异常交易账务调整要求提出异议并提供相应的抗辩证明材料。

（六）交易所涉及的商品销售或服务有违反法律、法规、规章等规范性文件或国家政策要求，并被有权机构/部门以书面方式确认性质或进行处罚的。

十四、对于第十三条约定的有关划款，乙方如有异议，可委托甲方与交易参与机构进行协商处理，也可委托甲方将有关异议转交该支付工具的争议处理机构处理。但甲方只能依据该支付工具的争议处理机构的有关规则进行，若乙方对于争议处理意见有异议，乙方有通过其他救济措施追索的权利。

十五、对于乙方发生第十三条中任意一种情况或故意避开授权规则进行分单操作或采取其他手段获取利益等情况，甲方有权受交易

参与方委托，书面通知乙方有关从乙方当日或以后的交易款及/或乙方在甲方开立的任一账户中扣除有关款项的事宜，因此引发的纠纷及争议，应由乙方负责解决。甲方有权要求乙方赔偿其因此遭受的损失。

十六、乙方应严格按照甲方提供的各类支付工具受理规则的要求正确操作终端设备及受理支付业务，并有义务参加甲方组织的免费培训活动。所有收银员均须参加培训后方可受理支付业务，凡未按规定办理或未接受培训而受理各类支付业务所造成的经济损失由乙方承担。

十七、乙方如发现甲方计算的交易金额与实际发生金额不符时，或发生调、换、退货等业务，或因通讯故障或操作失误等原因需对受理的支付交易作调账处理时，乙方应及时向甲方发出书面调账通知。

十八、乙方如有培训、维修终端设备等要求，可通过书面的方式提出，或通过甲方或由甲方指定的第三方服务机构设置的 24 小时咨询服务热线口头提出，甲方或由甲方指定的第三方服务机构应为乙方提供准确及时的服务。如终端设备出现故障，甲方或由甲方指定的第三方服务机构应在收到乙方口头或书面终端设备维护通知后及时提供检查维修等服务。如甲方或由甲方指定的第三方服务机构维修人员无法在收到乙方通知的 24 小时内检查维修完毕的，甲方或由甲方指定的第三方服务机构应向乙方提供备用终端设备。由于甲方或由甲方指定的第三方服务机构原因，导致终端设备维护未在收到乙方通知的 24 小时内检查维修完毕，且未向乙方提供备用终端设备，而影响乙方正常业务开展的，由甲方或甲方指定的第三方服务机构承担相应的损失赔偿责任。

十九、乙方如有账务查询要求，可通过甲方设置的服务电话进行查询。

二十、甲方或由甲方指定的第三方服务机构将为乙方提供回访服务，对终端设备的使用等相关情况进行调查。在进行银行卡业务服务时，乙方应积极配合甲方或由甲方指定的第三方服务机构相关人员的工作，如甲方或由甲方指定的第三方服务机构提出对回访结果进行确认等要求，乙方应完成相关的签字、盖章工作。

二十一、乙方在使用及保管终端设备时，应遵守以下要求：

（一）甲方具有终端设备及配件的所有权，乙方只具有终端设备的使用权，乙方不得买卖、转让、拆卸和毁坏甲方提供的所有终端设备及配件。

（二）甲方可依照本协议约定，向乙方收取终端设备押金。当乙方使用和保管的终端设备损毁或丢失时，甲方有权根据实际损毁或丢失终端设备数量，没收相应金额的押金。

（三）甲方或乙方按本协议约定解除本协议的，乙方应向甲方归还所有终端设备，甲方应依据终端设备归还情况退回押金。如乙方未归还的，将视为终端设备已经丢失，甲方有权没收相应金额的押金。

（四）协议期内，如甲方提供的终端设备发生故障，并经甲方证实属正常使用，甲方负责给予免费修理。对于经甲方认定系出现下列情况而更换机具的，乙方须缴付相应工本费用：

1. 由于非正常使用所造成之故障或损坏；

2. 由于曾被非甲方或甲方指定的第三方服务机构维修人员维修、拆卸、改装所造成之故障或损坏；

3.由于运输意外、跌落、震荡所造成之故障或损坏；

4.由于自然灾害、不适当电压等所造成之故障或损坏；

5.由于储存疏忽或不当（即把产品放在高温、高湿、高压或临近有害毒品、化学药品等地方）及保养不当等所造成之故障或损坏。

▲▲二十二、除本协议另有约定外，如本协议任何一方要求提前解除本协议，须提前 30 天（自然日）书面通知对方，本协议自通知上载明的终止之日起终止。协议终止前，双方应继续履行本协议。本协议终止时，乙方应退还甲方所提供的全部终端设备和有关业务物品。

二十三、协议终止后 36 个月内，如有因以往交易引起的查询，乙方仍有义务配合甲方工作；如因乙方违反本协议或违反支付工具的受理规则，造成退单或拒付的，甲方有权向乙方追索业已支付的款项。自本协议终止后 36 个月内，因本协议而引起的各方的职责，包括因以往交易引起的查询、由乙方所产生的未结账务或因发卡机构或第三方支付公司提出的有关异常交易账务，双方必须继续履行本协议的相关条款并进行与之有关的账务处理，守约方对违约方不履行职责所产生的损失具有追索权（超过单据保管有效期的不在此列）。

二十四、本协议终止后，乙方仍有退货调账要求的，其中因不可抗力及/或 IT 系统故障、通讯系统故障、电力系统故障等非甲方所能控制的原因造成的退货调账，均由乙方自行处理，甲方提供必要的协助，由此产生的费用由乙方负担。

▲▲二十五、通知：

（一）乙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、微信号等）均真实有效。任一联系方式发生变更，乙

方应立即以书面方式将变更信息寄/送至甲方在本协议填写的通讯地址。该等信息变更在甲方收到更改通知后生效。

（二）除本协议另有明确约定外，甲方对乙方的任何通知，甲方有权通过以下任一方式进行。甲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、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。甲方同时选择多种通知方式的，以其中较快到达乙方者为准：

1.公告，以甲方在其网站、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，以乙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）送达于甲方最近所知的乙方通讯地址，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甲方最近所知的乙方传真号码、乙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。

（三）乙方同意，除非甲方收到乙方关于变更通讯地址的书面通知，乙方在本协议填写的通讯地址是法院向乙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。如乙方应诉并直接向法院提交送达地址确认书，该确认地址与甲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。

本协议争议解决过程中，法院可通过以下任一方式将判决书、裁定书、调解书送达于乙方：

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

2.专人送达，以乙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，如乙方未在送达回证上签收或乙方所填写的通讯地址不准确或通讯地址实际发生变更但甲方未收到乙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，如乙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，法院对乙方的任何通知，法院有权通过本条第（二）款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，以其中较快到达乙方者为准。

（四）本条约定属于合同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。

二十六、适用法律及争议处理：

（一）本协议适用中华人民共和国的法律（为本协议目的不包括香港、澳门和台湾地区的法律）。因本协议引起的或与本协议有关的任何争议，由甲乙双方协商解决；协商不成的，双方一致同意将争议

提交甲方所在地法院通过诉讼解决，双方另有约定的除外。

（二）本协议部分条款无法执行时，不影响其他条款的有效性、合法性，也不影响其他条款的继续执行。

二十七、乙方在《交通银行特约商户支付受理业务协议书》签署界面点击“同意协议并下一步”按键，即表明乙方已知悉并同意本协议的全部内容，愿意按照本协议的约定享有权利并承担义务。本协议自乙方点击“同意协议并下一步”按键发起协议签署申请，交通银行系统接受乙方的协议签署申请后生效。

除按本协议另有约定外，本协议有效期为永久持续。

二十八、其他：

（一）乙方需如实提供申请信息，并承诺所提供信息的真实可靠。

▲▲（二）协议履行期间，甲方下调收费标准，将于执行前 10 个工作日在交通银行门户网站、相关电子渠道或甲方营业网点公告；甲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，有权提前在交通银行门户网站、相关电子渠道或甲方营业网点公告。乙方不同意公告内容的，有权在公告执行前依本协议的约定终止本协议。乙方在公告执行后继续办理相关业务的，视同接受公告内容。

▲▲（三）甲方有权根据法律法规、监管规定、国家相关政策变化，第三方支付公司、信用卡组织、清算机构的运营状况变化，第三方支付公司、信用卡组织、清算机构的相关规定和规则变动，及甲方收单业务发展的实际需求，而相应调整甲方关于特约商户受理支付工具的业务规则。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，甲方有权在调整生效日 30 个工作日前在交通银行门户网站或甲方营业网点等适当渠道公告或通过电话、短信或其他适当方式通知乙方。乙方不同意该等调整的，有权在调整生效日前解除本协议，否则即视为乙方接受甲方对该等内容的调整。

前述特约商户受理支付工具业务规则包括但不限于《交通银行特约商户银行卡受理规则》及甲方其他相关规定。

（四）前述特约商户受理支付工具业务规则是本协议的组成部份，与本协议具有同等法律效力。

（五）本协议未尽事宜，由双方协商解决。

▲▲（六）本协议签署后，如适用的法律法规、监管规定发生变化，本协议有内容违反新修订的法律法规、监管规定的，甲方有权对本协议相关内容进行修改或增补。

甲方根据前款约定对本协议进行修改或增补的，甲方应于修改生效日 30 个工作日前以书面形式通知乙方，自修改生效日起，甲乙双方按照修改后的协议处理相关业务。

（七）甲方将根据法律法规及相关规定提供合法合规的增值税发票，具体时间及方式双方另行协商确定。

第二部分、银行卡支付受理支付业务附加条款

二十九、本条规定仅适用于受理银行卡支付业务情形。

乙方在受理银行卡交易时除应按照本协议第一部分一般条款约定进行操作外，还应按照甲方提供的《交通银行特约商户银行卡受理规则》的规定进行操作。如乙方违反下述操作规定所造成的交易损失，由乙方承担，并且甲方有权依据本协议第十二条进行处理：

（一）必须确认消费者为卡片合法持有人本人，若非本人应拒绝其持卡消费。否则，乙方将承担违反上述操作规定所造成的交易损失。

（二）认清银行卡上的有关标志、中文提示及有效期等信息，仔细查看激光防伪标志，确认卡片无损毁或有无涂改痕迹，确认卡片上无“样卡”、“VOID”（无效卡）等字样，照片卡须核对消费者与照片是否相符，对不符合受理要求的，乙方应拒绝受理；对于使用测试卡及其他明显非正常银行卡（如没有任何银行和品牌标识、设计图案的白卡等）的，或乙方经办人员发现有人使用他人丢失、被盗或伪造的银行卡的，乙方应拒绝受理。

（三）遵守甲方有关检查消费者身份证件的规定。

（四）应严格按照甲方提供的操作流程，正确进行 IC 卡受理，特别是 IC 卡读卡失败时的降级交易处理。

（五）在受理过程中出现未打印签购单的情况时，应按规定先进行重打交易操作，如仍然未能打印出签购单，才能重新进行刷卡交易（银行卡或条码支付受理结算系统、终端设备故障除外）。

（六）每日营业结束后，应按规定进行“结算”或“签退”操作，上送外卡交易流水和脱机交易流水。乙方未按上述操作程序办理而造成发卡行或银行卡持有人拒付时，造成损失由乙方承担。甲方应积极协助乙方处理，以尽可能减少或挽回损失。如因甲方的银行卡或条码支付受理系统或机具问题导致重复扣款而引起的纠纷由甲方负责协调解决。

（七）若乙方受理境内银联卡支付，且同意接受消费者使用银联小额免签、免密支付，则需遵守小额免签、免密支付业务规则开展业

务。

第三部分、条码支付受理业务附加条款

三十、本条规定仅适用于信用卡组织或清算机构系统产生或转接的条码，进行支付受理业务的情形。

如乙方开通受理条码支付业务，则以下（一）至（八）项适用：

▲▲（一）甲方有权根据信用卡组织或清算机构的要求对交易结算周期进行调整，并以书面方式通知乙方。

▲▲（二）乙方连续90个自然日未受理条码支付交易的，甲方有权终止提供本协议项下条码支付受理服务而无需书面通知乙方，并无需承担任何法律责任。前述约定不免除因甲方过错依法应由其承担的责任。

（三）乙方在办理条码支付收单业务时，应保证将实物与虚拟产品业务分开使用，不得混用，并对虚拟产品业务进行明确标注。不得将条码支付运营商的服务电话或电子邮箱作为自身的服务电话或电子邮箱向外公布。

（四）如甲方发现乙方在使用条码支付收单业务中存在异常交易或异常行为的，甲方有权要求乙方提供合理、合法、有效的证据，包括但不限于货物采购合同、出库清单、订单等信息。

（五）因甲乙双方系统升级或维护，导致短暂停止服务时，应提前发布相关公告，由此产生的服务中断或不稳定状态，不视为违约。

（六）甲、乙双方对于“中国国内电子商务环境尚未成熟，电子商务立法以及信用体制还不完善”的现状以及开展电子商务业务存在的风险性均完全知悉，双方均承诺采取合理的风险防范措施，以尽量

避免或减小风险。

（七）如乙方违反国家法律、法规、政策或法令、违反对消费者的承诺或乙方违反与甲方的约定等情形而造成甲方或消费者损失的，乙方应自行解决上述情况而导致的索赔等纠纷；乙方出现前述情形的，甲方有权立即暂停、中止或终止向乙方提供本协议项下的服务，同时有权要求乙方赔偿其因此遭受的损失。

（八）在单个自然日内，若消费者因通过乙方进行的本合同项下条码支付而主张非授权交易等情形的交易金额累计达到人民币 3000 元，乙方需根据甲方要求采取对应的配合工作联合防御相关交易风险；如乙方在收到甲方通知后的 5 日内未采取措施控制的，甲方有权终止向乙方提供的条码支付收单业务，但应在终止前通知乙方；若上述非授权交易的交易金额连续两个月累计超过 10000 元，甲方有权终止向乙方提供的条码支付收单业务，但应在终止前通知乙方。

乙方已通读协议全部条款，甲方已应乙方的要求作了详细说明，乙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。

附件 1-2

基于多方安全计算的图像隐私保护产品
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）、《银行卡收单业务管理办法》（中国人民银行公告〔2013〕第 9 号公布）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。

交通银行股份有限公司

2020 年 12 月 30 日

附件 1-3

基于多方安全计算的图像隐私保护产品
技术安全性评估报告

本项目符合《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）、《移动终端支付可信环境技术规范》（JR/T 0156—2017）、《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。

本产品实现了基于多方安全计算的图像隐私保护产品，应用于手机 POS 商户责任人、收银员身份验证场景。项目基于 PrivPy 技术框架进行应用层开发，实现图像数据（图像特征信息）隐私保护。

在商户责任人或收银员图像信息录入阶段，通过 PrivPy MPC 输入组件将提取后的图像特征信息进行随机切片、传输并存储至交通银行和中国银联两个独立的主体。由于密文切片的随机性，任何一方都无法恢复出图像的完整特征，有效避免由于独立主体单独存储用户的图像特征原图带来的数据泄露风险，提升隐私信息保护的安全性。

在身份识别阶段，利用 PrivPy 秘密分享技术，将商户责任人或收银员身份验证时的图像特征进行随机切片后，与多主体存储的注册时

密文切片进行比对，在不泄露各切片的原始信息基础上实现商户责任人或收银员身份准确识别，有效保护了商户责任人或收银员隐私信息安全。

PrivPy 的安全性分析如下：

1、协议安全性

PrivPy 协议基于秘密分享机制，成果已经形成论文，并发表于 2019 年知识发现与知识挖掘国际顶级会议（Knowledge Discovery and Data Mining，KDD 2019）。

PrivPy 协议基于半诚实模型而设计，在论文中已提供了 PrivPy 协议的形式化证明，形式化证明过程如下图所示。由于 PrivPy 协议中所定义的加法计算过程只需在本地完成，因此论文中采用举例方式对乘法计算过程进行了形式化证明。

Theorem 1. *Protocol 1 securely realizes $\mathcal{F}_{mult}$ presence of semi-honest adversaries.*

Proof. Our proof is similar to the proof in [3]. Specifically, we first construct an efficient simulator for $\mathbf{S_1}$, which are referred to as Sim_1 and receives the input $X_1 = (x_1, x'_1)$ and $Y_1 = (y_1, y'_1)$, as well as the seed for generating pseudo-random numbers. Sim_1 generates r^*_{12} and r'^*_{12} using the seed, then calculates $t^*_1 = x_1 y'_1 - r^*_{12}$ and $t'^*_1 = x'_1 y_1 - r'^*_{12}$. Sim_1 samples random numbers $t'^*_a \in \mathbb{Z}_\phi$ and $t^*_b \in \mathbb{Z}_\phi$, and sets $z^*_1 = (t^*_b + t^*_1)/2^d$ and $z'^*_1 = (t'^*_a + t'^*_1)/2^d$, then sends z^*_1 and z'^*_1 to $\mathcal{F}_{mult}$. Sim_1 adds r^*_{12} and r'^*_{12}, t'^*_a and t^*_b to the view of $\mathbf{S_1}$. In a real execution, r_{12} and r'_{12} are pseudo-random numbers that are generated using the same seed from $\mathbf{S_1}$, thus are equal to r^*_{12} and r'^*_{12}. On the other hand, t'_a and t_b are masked by pseudo-random numbers generated by S_a and S_b. As the pseudo-random numbers are generated using seeds unknown by $\mathbf{S_1}$, t'_a and t_b are indistinguishable with truely-random numbers (t'^*_a and t^*_b) for $\mathbf{S_1}$. We can then conclude that $View_1$ and Sim_1 are indistinguishable. The simulators for the other servers can be constructed in the same way. □

图 1 论文中形式化证明过程截图

2、PrivPy 技术框架安全性说明

基于 PrivPy 协议可实现 PrivPy 多方安全安全计算技术框架。该技术框架满足《多方安全计算金融应用技术规范》(JR/T 0196-2020)，从安全性上看主要包括以下几个方面：

1) 数据使用授权。保证数据提供方对自身数据使用的用途、用量可控。

2) 身份认证。使用数字证书机制保证多方交互时身份可鉴别。

3) 安全通信。使用密码技术保护通信过程的安全性，包括数据的完整性和机密性。

4) 密钥管理。采用随机数发生器产生随机数，并保证使用过程的安全性，包括安全存储、分发、使用、销毁等环节。

5) 日志审计。对关键操作进行存证，保证信息可审计。

中国银联股份有限公司电子支付研究院

附件 1-4

基于多方安全计算的图像隐私保护产品
风险补偿机制

本项目按照由中国银联股份有限公司、交通银行股份有限公司、华控清交信息科技（北京）有限公司及上海聚虹光电科技有限公司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、 风险防控原则

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，通过数据泛化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，借助多方安全计算等技术，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。

二、 风险补偿机制

在消费者知情授权、数据隐私等方面的风险事件，中国银联根据《中国银联数据共享项目业务合作框架协议》等协议所认定的风险责任划分进行风险承担，建立完善的事前风险防范、事中监控、事后追溯机制，明确权责认定，全方位保障用户的合法权益。

本项目首先对部分商户和用户进行试点，优化完善流程之后再做全面推广。主要包括下面两方面：

1、控制业务范围：采用试点用户的方式，限制该业务目前的影响范围。

2、模拟风险场景：对现有的业务进行截包分析，以及假设业务方串通恶意攻击的场景，从而完善具体的风险处理手段，保证目标流程的安全性和稳定性。

三、 申诉处理渠道

交通银行建立客户投诉快速响应机制，可通过交通银行客服热线95559为相关终端用户提供申诉渠道，交通银行收到投诉后，将指派专职人员核实情况，并及时告知客户投诉处理进展。关于用户隐私数据的违规使用、泄露等问题，支持用户通过《网络安全法》等法律法规维护自身合法权益。

附件 1-5

基于多方安全计算的图像隐私保护产品
退出机制

本项目按照国家及金融行业的相关规范要求，坚持最大限度的保证用户信息安全的原则，中国银联股份有限公司、交通银行股份有限公司、华控清交信息科技（北京）有限公司及上海聚虹光电科技有限公司联合建立退出机制，将采取以下措施做好数据清理和隐私保护工作，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、 退出条件

本项目依据政策及监管要求执行下线。

二、 退出方案

1） 技术退出

相关数据：按照《网络安全法》等要求，在退出时对用户的相关

数据进行备份、归档和清理。保证该服务下线后用户的其他业务不受影响。

资源回收：停止本项目的相关系统资源、计算资源等，包括服务器，以及相关合作机构之间的网络接口，确保网络的安全。

2） 业务退出

根据协议中，本项目约定的时限，提前通知合作方，并通知用户。使其实现有序退出。同时若合作四方均满意业务相关运行状况，协商后可以续签合作协议，持续化运营。

3） 用户退出

根据相关要求，通过相关渠道通知用户服务即将终止。在用户取消该服务时确认该业务已经停止，删除相关隐私数据。

附件 1-6

基于多方安全计算的图像隐私保护产品
应急预案

本项目按照以下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。本预案由中国银联股份有限公司、交通银行股份有限公司、华控清交信息科技（北京）有限公司及上海聚虹光电科技有限公司四方联合成立的系统保障小组制定，包括监控和评估机制，对系统的运行情况和潜在的风险进行定期和不定期的验收和检查，如发现系统问题出现故障，通信异常，部分数据丢失等问题进行快速介入。

具体应急预案如下：

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，以及相应的违规处理办法，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。

另外，在上线前，系统会进行综合测试，并编写系统相关的应急操作手册；在系统上线后会定期开展生产运维评估。如服务意外中断无响应，使用该服务模块的替代模块对中断时间内的服务进行检查验证，确保风险可控。

在项目投产前，对各方分别存储的数据做好备份统筹，完成相应的压力测试，保证业务的连续稳定。

通过本项目，基于多方安全计算的图像隐私保护产品，可以对移动端图像信息验证过程中的隐私图像数据进行严格保护，推动数据利用合理化，增加客户的信任。