《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	114400004558627585-2021-0001	
	创新应用名称	基于知识图谱的外汇违法违规风险行为识别应用	
	创新应用类型	金融服务	
	机构信息 1	统一社会信用代码	114400004558627585
		全球法人识别编码	无
		机构名称	国家外汇管理局广东省分局
		持有金融牌照信息	无
	机构信息 2	统一社会信用代码	91440000190336428Q
		全球法人识别编码	无
		机构名称	广发银行股份有限公司
		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：B0012H144010001 发证机关：中国银行保险监督管理委员会
	拟正式运营时间	2021 年 06 月 21 日	
	技术应用	1.利用神经网络技术，国家外汇管理局广东省分局将内部数据（企业外汇业务明细数据）和来源合法合规的外部数据（企业人民币历史交易数据、外汇违法违规企业名单、质量失信企业名单、税收违法企业名单及海关行政处罚企业名单）作为样本数据，通过特征分析和样本训练构建外汇违法违规风险行为识别模型，为快速甄别高风险企业提供支持。 2.利用知识图谱技术，国家外汇管理局广东省分局基于企业外汇业务明细数据等信息，分析提取企业间外汇交易资金往来关系及交易时间、交易金额等特征，构建企业关系网络，辅助国家外汇管理局广东省分局识别高风险企业群体，提升外汇检查风险识别能力。 3.基于分布式微服务架构灵活部署特性，构建广东外汇非现场检查系统，将数据处理、特征分析、模型计算、关系网络构建等功能模块独立部署、运行及维护，有效降低系统功能服务间的耦合性，降低成本，提升系统维护效率。	

	功能服务	本项目运用知识图谱、神经网络等技术构建广东外汇非现场检查系统，辅助国家外汇管理局广东省分局在外汇非现场检查阶段识别企业违法违规风险行为，为后续外汇现场检查提供线索，提升外汇监管水平，更好规范外汇市场经济秩序。 本项目由国家外汇管理局广东省分局、广发银行股份有限公司共同研发，广发银行股份有限公司提供技术支持，国家外汇管理局广东省分局负责系统运维并提供应用场景，此外无第三方机构参与。
	创新性说明	1.数据应用方面，国家外汇管理局广东省分局在内部数据基础上，引入企业人民币历史交易数据、质量失信企业名单、税收违法企业名单及海关行政处罚企业名单等外部数据，丰富外汇违法违规风险行为的分析维度，提升外汇违法违规风险行为识别模型的准确性。 2.风险识别效率方面，运用神经网络技术构建外汇违法违规风险行为识别模型，实时分析发现高风险企业，为外汇现场检查提供可疑线索，有效提升外汇监管工作效率。 3.系统维护方面，本项目采用高可用、松耦合的分布式微服务架构，在不影响其它功能运行使用的前提下，可以实现对不同模块功能的快速维护部署，有效降低系统升级维护带来的影响。
	预期效果	增强国家外汇管理局广东省分局外汇违法违规风险行为分析识别能力，提升外汇监管水平，更好规范外汇市场经济秩序。
	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，预计对广东省内有跨境交易的3万多家企业进行非现场检查。
创新应用服务信息	服务渠道	线上渠道
	服务时间	8:30至17:30（工作日）
	服务用户	国家外汇管理局广东省分局及辖内中心支局
	服务协议书	《服务协议书-基于知识图谱的外汇违法违规风险行为识别应用》（见附件1-1）
合法合规性评估	评估机构	国家外汇管理局广东省分局外汇检查处
	评估时间	2021年03月05日

	有效期限	3 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》、《中华人民共和国外汇管理条例》（中华人民共和国国务院令第 532 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）、《中国银监会关于银行业风险防控工作的指导意见》（银监发〔2017〕6 号）、《国家外汇管理局信息系统数据安全管理规定》（汇综发〔2018〕93 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。		
	评估材料	《合法合规性评估报告-基于知识图谱的外汇违法违规风险行为识别应用》（见附件 1-2）		
技术安全性评估	评估机构	国家外汇管理局广东省分局外汇检查处、广发银行股份有限公司研发中心		
	评估时间	2021 年 03 月 29 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）、《金融科技创新安全通用规范》（JR/T 0199—2020）、《金融业数据能力建设指引》（JR/T 0218—2021）、《人工智能算法金融应用评价规范》（JR/T 0221—2021）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。		
	评估材料	《技术安全性评估报告-基于知识图谱的外汇违法违规风险行为识别应用》（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	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，借助标记化等技术，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	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。
			防控措施	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。
		3	风险点	本项目涉及的外汇违法违规风险行为识别模型可能因为历史数据不够准确、样本覆盖度不足、模型算法稳定性等因素导致评估效果产生偏差。
			防范措施	加强数据质量管理，不断验证调整模型算法与技术，迭代优化模型；加强人工监控，建立模型实时监控预警机制，及时发现数据和模型异常指标，并通知工作人员进行人工干预，避免模型准确性问题影响外汇非现场检查效果。
	风险补偿机制	本项目由申请各方共同建立风险补偿方案(见附件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，切实保障本项目所服务用户的合法权益。在本项目所服务用户因使用该服务而出现资金损失时，由金融场景提供方按照风险补偿机制进行赔付，充分保障本项目所服务用户的合法权益。对于非用户自身责任导致的资金损失，提供全额补偿，充分保障本项目所服务用户合法权益。		
	退出机制	本项目由申请各方共同建立退出机制（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。		

		在业务方面，按照退出方案终止有关服务，及时告知用户并与用户解除协议。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用户，对用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	本项目由申请各方共同建立应急处置预案（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。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，视需要及时关闭增量业务，妥善处置受影响的存量业务，切实保障用户资金和信息安全。	
投诉响应机制	机构投诉	投诉渠道	国家外汇管理局广东省分局业务联系人办公电话：020-81322576
		投诉受理与处理机制	受理部门：国家外汇管理局广东省分局 受理时间：8:30至17:30（工作日） 处理流程：在接到投诉事件后，受理人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，协调相关人员进行处理解决，并及时将处理进度反馈投诉人员。
	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。 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	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

基于知识图谱的外汇违法违规风险行为识别应用服务协议书

本项目服务协议书包括《广发银行企业手机银行隐私政策》，具体如下:

广发银行企业手机银行隐私政策

更新日期：2021 年 1 月 22 日

生效日期：2020 年 1 月 22 日

一、 前言

1.相关定义及简称

（1）广发银行股份有限公司，在本文中简称“广发银行”或“我行”。

（2）广发企业手机银行用户，系指申请或使用我行企业手机银行业务的自然人用户，在本隐私政策中简称“用户”或“您”。

（3）广发企业手机银行：包括用户端程序、广发企业手机银行安全工具等。

（4）用户端程序：是指用户需要在各类互联网终端（手机、电脑、平板电脑、可穿戴设备、电视盒子等）中安装的程序，用来获取我行信息或服务。

（5）广发企业手机银行**安全工具**：包括但不限于KEY盾、软令牌、短信口令、生物识别等可在广发企业手机银行交易过程中，用于加强用户身份识别的工具。

2.制定本隐私政策的目的

广发银行股份有限公司深知个人信息对您的重要性。您在使用广发企业手机银行产品与服务时，我们将按照法律法规的规定，保护您的用户信息及隐私安全。我们将通过“本隐私政策”向您说明广发企业手机银行如何收集、使用、保存、共享和对外提供这些信息，以及我们为您提供的访问、更新、删除和保护这些信息的方式。请您在使用广发企业手机银行及相关服务前仔细阅读并理解本隐私政策，以便做出适当的选择。**若您为无民事行为能力人，在使用广发企业手机银行产品与服务前，您应事先征得您的监护人的同意。**

3.**本隐私政策的纲要**

本隐私政策包括以下几个部分：

（1）前言。说明相关定义，本隐私政策制定的目的及纲要。

（2）我行对用户信息的收集。描述了我行需要收集何种信息以及相关场景。

（3）我行对用户信息的使用。描述了我行收集信息的用途。

（4）我行对用户信息的存储与保护。描述了我行在信息存储与保护方面采取的措施及方法。

（5）用户信息向第三方的共享、传输与披露。阐释了我行如何获得用户授权，以及如何依据用户授权或依法向第三方进行用户信息的传递与

披露。
（6）用户对个人信息的管理。说明用户如何对个人信息进行访问、变更或删除。
（7）本隐私政策的变更。说明本隐私政策在修订时我行将履行的程序。
（8）如何联系我行。说明您对本隐私政策内容存疑时联系我行的途径。

二、我行对用户信息的收集

为了向您提供优质的对公移动金融服务，保障您的使用安全，在您开通以及使用我行企业手机银行的过程中，我行会**收集您主动提供的或因服务而产生的信息。**

1.当您使用我行的企业手机银行功能或服务时，您可能需要向我行提供或授权我行收集相应服务所需的个人信息。如您拒绝提供，您可能将无法使用相应功能或服务。

（1）登录密码、手势静态信息

①在您使用企业手机银行的过程中，若您选择“记住密码”功能，我行将以加密形式收集及存储您的**登录密码，**用于您登录企业手机银行、现金管理系统移动版、融慧e家时使用。

②当您完成系统校验，我行为您提供了手势登录密码设置、修改及重置功能，开启手势登录功能后，我行将存储并记录您设置的**手势信息**。当您以手势验证方式登录企业手机银行时，需要自行输入手势信息完成身份验证。

（2）指纹、面容生物信息

我行为您提供了指纹登录、面容登录（基于Face ID，仅支持iOS手机部分机型）。

① 您开启指纹登录后，您登录我行企业手机银行、现金管理系统移动版时需要提供您的指纹信息进行验证。我行不会采集您的指纹信息，您的指纹信息仅保存在您授权采集指纹的设备上。

② 当您开启面容登录功能后，您登录我行企业手机银行、现金管理系统移动版时需要提供您的面容信息进行验证。我行不会采集您的面容图像原图，您的图像原图仅保存在您授权采集脸部图像的设备上。

（3）位置信息

当您使用我行企业手机银行网点预约服务时，我行将会通过您的移动设备GPS定位或Wi-Fi网络收集您的位置信息，以使得向您推荐的信息更具针对性。如您拒绝提供位置信息，我行或将无法为您提供精准的服务结果，但这并不影响您使用我行企业手机银行的其他功能。

（4）收款人信息

当您使用转账汇款功能时，您需要提供**收款人的姓名、银行账号、开户行、手机号码、附言**信息，以便我行根据您的交易指令将您要求的款项

顺利汇出。如您拒绝提供上述信息，您的转账汇款指令将无法正常执行，但这并不影响您使用我行企业手机银行的其他功能。
当您使用我行企业手机银行完成转账汇款后，我行系统将记录该笔转账信息便于您进行交易明细查询。为方便您后续操作，我行系统为您记录了**收款人名册**，您也可以自行登录我行企业手机银行、企业网银进行收款人名册的删除、修改与添加。
（5）其他重要的身份验证信息
当我行需要持续识别您的身份进而向您提供基于真实身份的各类企业手机银行服务与功能时，您需要提供**手机号码、私密问题及答案、短信验证码、KEY盾密码、数字证书及PIN码、面容图像**进行身份验证。上述基于真实身份的企业手机银行服务与功能包括转账与支付、安全设置、企业手机银行登录密码修改或重置及我行根据业务发展、风险控制、金融监管需要开发出的其他类似业务。
2.**设备型号、IP地址、Mac地址**等技术信息。当您使用企业手机银行服务时，为了维护系统的正常运行，保障您的使用安全（转账及支付安全、登录安全、信息查询安全、网络环境安全），我行会收集以下基础信息：包括**设备型号、操作系统版本、IMEI号、Mac地址、IP地址、端口信息、网络接入方式、登录渠道、APP版本、登录时间、硬件编号、系统参数、服务日志**信息。这些信息是为您提供服务或保证您的使用安全所必须收集的信息。
3.统计分析信息。为了持续提升服务体验，改进服务质量，我行会收集您使用企业手机银行功能或服务的类别、登录及操作轨迹、交易记录、使用偏好，我行会对这些信息进行统计、分析，且信息仅**用于我行改进APP功能，为您持续提供更好的使用体验。**
4.**您对于手机设备功能的控制**。当您在使用我行企业手机银行时，可自行通过更改手机设备的设置，来选择是否授权我行收集您的信息。（例如，您可以在手机设备的“设置-应用-权限”菜单中关闭对企业手机银行APP相关功能的授权）在您关闭手机相关基础功能后，对应的手机银行功能服务可能无法正常使用。具体涉及的功能有如下几项：
（1）**手机摄像头**。用于完成企业手机银行、现金管理系统移动版“扫一扫”、“面容识别”、“业务资料上传”、“交易追踪”、“面容登录”功能或服务。
（2）**手机相册**。用于企业手机银行、现金管理系统移动版、融慧e家的“头像上传”、“二维码识别”、“业务资料上传”需要调用手机相册的功能或服务。
（3）**蓝牙通讯模块。**用于企业手机银行、现金管理系统移动版蓝牙KEY盾验密功能。
（4）**定位功能。**用于企业手机银行“网点预约”服务，以及ANDROID系

统的蓝牙KEY盾验密功能。

（5）消息推送权限。用于企业手机银行的“消息推送”功能。

（6）网络、WIFI状态/访问网络连接。用于企业手机银行“安全监测”功能。

（7）发送短信/允许编写短信权限。用于企业手机银行、现金管理系统移动版、融慧e家的“短信分享”功能。

（8）通讯录读取权限。用于企业手机银行的“一站式转账 - 手机号码转账”，向您指定的通讯联系人进行转账。

（9）查看是否支持指纹。用于企业手机银行、现金管理系统移动版的“指纹登录”、“指纹设置”功能。

若我行企业手机银行APP进行版本升级，用户覆盖安装后，对于已经授权的相关系统权限设置将不会发生改变。

5.不属于个人信息的范畴

我行尊重并采取适当的措施充分保障您的个人信息安全，但您应充分知悉并了解，根据现行法律法规，以下信息不属于个人信息的范畴：

（1）经脱敏处理后的信息，即采用技术手段对个人信息进行处理后，使得个人信息主体无法被识别，且处理后不能被复原的信息。

（2）无法识别特定自然人身份或反映特定自然人活动情况的信息。

对上述信息的保存、分析和处理，我行无需另行向您通知并征得您的同意。

6.征得同意的例外

根据相关法律法规及监管要求，以下情形中，我行可能会收集、使用您的相关个人信息无需另行征求您的授权同意：

（1）与国家安全、公共安全、重大公共利益直接相关的。

（2）按照法律规定或有权机关规定，向金融监管机关、公安机关、人民法院等（司法）行政机关披露个人信息的。

（3）与案件立案、侦查、起诉、审判、执行等刑事司法事项相关的。

（4）出于维护您或其他主体的生命、财产等重大合法权益但又很难得到本人同意的。

（5）所收集的个人信息是您自行向社会公众公开的。

（6）从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道。

（7）根据您要求签订和履行合同所必需的。

（8）用于维护所提供的产品或服务的安全稳定运行所必需的，例如发现、处置产品或服务的故障，控制业务风险。

（9）法律法规及监管要求规定的其他情形。

三、我行对用户信息的使用

我行将严格遵守法律法规的规定以及与您的约定，将收集的信息用于以下用途或者场景：
1.用于向您提供我行的金融产品或服务或对这些功能或服务进行持续的优化、改进、升级。
2.提高服务的精确度，满足您的个性化需要。
3.用于投诉处理、工单排查、故障分析与解决，优化我行企业手机银行。
4.用于安全保障，如身份认证、反欺诈分析与监测、安全服务。
5.您授权同意的以及法律允许的其它用途。
在我行向您提供金融服务期间，您授权我行持续收集和使用您的信息，我们**不会**将我们存储在分析软件中的信息与您在应用程序中提供的任何个人身份信息相结合，以用于分析或投放广告/市场营销和其他商业目的。在您注销服务时，我行将停止收集您相关的个人信息，但我行会在业务资料归档、审计、监管协查等领域继续使用此前收集的您的相关个人信息。

四、我行对用户信息的存储与保护
1.我行会按照法律法规及监管要求，将在中华人民共和国境内收集和产生的**用户信息存储于中国境内**。
2.在为实现本隐私政策所述目的必要时限和法律法规、监管规定的时限内，我行将保留您的个人信息。超出必要期限后，我们将对您的个人信息进行删除或匿名化处理，但法律法规另有规定的除外。
3.我行将遵守相关法律规定，**采取必要措施保障用户信息的安全**，以防止用户信息在意外的、未经授权的情况下被非法访问、复制、修改、传送、遗失、破坏、处理或使用。
4.我行已建立配套的管理制度、内控机制和流程以保障您的信息安全。例如，设定**严格数据访问权限，落实数据请求的最小必要原则，使用专线加密传输数据，对电子银行相关系统的源代码进行统一管控**。加强员工对于个人信息保护领域的宣导与教育；在信息技术部门设立专门的安全管理团队；建立需要由信息安全主管部门参加的重大项目评审制度；通过营业网点及电子渠道对客户开展关于信息安全的提示与教育。

5.若发生用户信息泄露等安全事件，我行将采取应急业务管控措施和技术手段，阻止安全事件扩大。

五、用户信息向第三方的共享、传输与披露
除国家有关机关依法查询或使用您的用户信息外，我行不会主动向任何第三方共享、传输、披露您的用户信息，除非符合以下情形：
1.向您告知个人信息使用目的、涉及的个人信息范围、应用场景并征得

您的同意或授权。涉及的第三方SDK及应用场景如下：
（1）蓝牙SDK。用于电子签名认证交易，需获取蓝牙权限、地理位置信息。
（2）同盾设备指纹SDK。用于判断设备唯一性以及风险控件，保障您的账户安全，使用APP期间会获取以下信息：设备唯一标示符、本机手机号码、当前运行程序列表、位置、无线mac地址、蓝牙mac地址、ip地址。
（3）灵图地图SDK。用于用户进行网点预约，需获取地理位置信息。
（4）音频SDK。用于电子签名认证交易，需获取音量控制和音频录制权限。
（5）腾讯云清场 SDK。用于扫描APP运行环境以及病毒木马,需获取软件列表，WiFi信息，MAC地址信息。
（6）TalkingDataSDK。用于后台数据统计分析记录用户使用行为，以便优化操作体验和完善服务，需获取手机型号、地理位置信息。

（7）微信分享 SDK。用于用户进行分享到微信朋友圈、微信好友，需获取设备标示符。

（8）百度识别 SDK。用于用户活体检测和是否本人验证，以提升用户账户安全和交易安全，需获取摄像头权限。

（9）身份证 OCR SDK。用于身份识别，并自动填充证件号、证件有效期，需获取摄像头权限。

（10）菊风远程双录 SDK。用于法人开户意愿视频核实，需获取调用麦克风、摄像头。

以上SDK权限的索取，我们都会通过弹窗提示取得您的同意及授权。
2.根据您自主下达的交易指令，您使用的电子银行服务属于经由通过我行严格筛选的合作方或供应商方可实现或完成的。
3.另外，根据相关法律法规及监管要求，以下情形中，我行可能会共享、传输、公开披露您的个人信息而无需事先征得您授权同意，但我行会尽可能提供适当的保护措施进行保护：
（1）与国家安全、公共安全、重大公共利益直接相关的。
（2）按照法律规定或有权机关规定，向金融监管机关、公安机关、人民法院等（司法）行政机关披露个人信息的。
（3）与刑事案件立案、侦查、起诉、审判、执行等刑事司法事项相关的。
（4）出于维护您或其他主体的生命、财产等重大合法权益但又很难得到本人同意的。
（5）所收集的个人信息是您自行向社会公众公开的。

（6）从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道。
（7）根据您要求签订和履行合同所必需的。
（8）用于维护所提供的产品或服务的安全稳定运行所必需的，例如发现、处置产品或服务的故障，控制业务风险。
（9）法律法规及监管要求规定的其他情形。

六、用户对个人信息的管理

1.在您使用企业手机银行期间，您有权访问或自主**更新**您的个人信息。在您修改个人信息之前，我行会验证您的身份。
例如，您可以登录企业手机银行，前往“我的”页面修改头像；前往“密码设置”功能修改登录密码，或对指纹/面容、手势功能进行设置。
2.您通过智能移动设备使用企业手机银行时，可以通过硬件服务商或通讯提供商提供的功能**关闭相关软硬件服务来停止向我行提供信息，**如关闭GPS、关闭蓝牙、关闭麦克风、关闭数据存储访问权限、关闭Wi-Fi功能或移动数据连接功能，但**上述方式可能导致您无法使用我行的企业手机银行的部分或全部功能**。（具体关闭方式及相关功能说明详见“二、**我行对用户信息的收集**-4.您对于手机设备的控制”）
3.若您发现我行收集、存储的您的个人信息存在错误，您可以要求我行予以更正。若您发现我行违反法律、行政法规、监管部门规定或双方约定收集、使用您的个人信息，您可通过合法方式通知我行要求删除。
4.您作为我行企业手机银行用户，可以自行通过我行柜面或企业网银停用您的企业手机银行。**通过企业网银停用用户的具体路径为“登录企业网银-进入手机银行页签-进入用户启停页面—选择用户停用”。**如您非我行企业手机银行用户，您可以自主选择卸载或停止使用我行企业手机银行，以彻底阻止向我行提供您的个人信息。
一旦您停用，我行将不再通过企业手机银行收集您的个人信息，并将**删除**有关您企业手机银行用户的相关信息，例如您的**登录名、登录密码、定制头像**，但法律法规或监管机关对个人信息存储另有规定的除外。

七、本隐私政策的变更

1.因业务发展需要或法律法规及监管政策要求，我行可能会适时对本隐私政策进行修订。
2.本隐私政策发生变更时，我行会在变更内容生效前通过企业手机银行进行公告，在公告期间，您可对变更后的协议进行详细阅读并通过正式途径向我行提出意见或建议。
3.若您不同意对本隐私政策的变更，应立即停止使用我行企业手机银行服务，并按照本隐私政策第六条第4点约定的方式操作注销相关用户，

我行将停止收集您的相关个人信息。

八、如何联系我行

如对本隐私政策有任何意见、建议或疑问，您可以通过以下渠道与我行联系：

1.致电我行客户服务热线4008308003-3，将您的意见、建议或诉求向我行客服人员反映。

2.将您的身份证明文件、拟投诉反映的问题及电话联系方式（如手机号码、固话号码等）以书面材料形式寄送到：**中国广东省广州市越秀区东风东路713号25层广发银行总行消费者权益保护与服务监督部，邮编：510080。**我行会及时处理您提出的与本隐私政策相关的意见、建议或问题。

附件 1-2

基于知识图谱的外汇违法违规风险行为识别应用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》、《中华人民共和国外汇管理条例》（中华人民共和国国务院令第 532 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）、《中国银监会关于银行业风险防控工作的指导意见》（银监发〔2017〕6 号）、《国家外汇管理局信息系统数据安全管理规定》（汇综发〔2018〕93 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，本项目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。

国家外汇管理局广东省分局外汇检查处

2021 年 03 月 05 日

附件 1-3

基于知识图谱的外汇违法违规风险行为识别应用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）、《金融科技创新安全通用规范》（JR/T 0199—2020）、《金融业数据能力建设指引》（JR/T 0218—2021）、《人工智能算法金融应用评价规范》（JR/T 0221—2021）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。

国家外汇管理局广东省分局外汇检查处

广发银行股份有限公司研发中心

2021 年 03 月 29 日

附件 1-4

基于知识图谱的外汇违法违规风险行为识别应用风险补偿机制

本项目由申请各方联合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，切实保障本项目所服务用户的合法权益。在本项目所服务用户因使用该服务而出现资金损失时，由国家外汇管理局广东省分局按照风险补偿机制进行赔付，充分保障本项目所服务用户的合法权益。对于非用户自身责任导致的资金损失，提供全额补偿，充分保障本项目所服务用户合法权益。

附件 1-5

基于知识图谱的外汇违法违规风险行为识别应用退出机制

本项目由申报各方共同建立退出机制，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，及时告知用户并与用户解除协议。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用户，对用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:

一是用户退出，包括关闭系统相关用户权限，清理用户数据，并删除用户、删除角色等。二是服务退出，包括停止数据源清洗加工流程、指标加工流程，取消建模任务、运算任务及定时调度任务配置，关停包括 Nginx 服务、微服务统一注册中心、微服务统一配置中心，微服务网关等各类服务。三是数据退出，包括清理特征数据、加工过程中产生的中间数据、运行批次信息和模型结果等数据。四是系统及硬件资源退出，包括网络隔离、应用服务器回收、数据库备份及销毁等流程。

附件 1-6

基于知识图谱的外汇违法违规风险行为识别应用应急预案

本项目由申请各方共同建立应急处置预案，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。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，视需要及时关闭增量业务，妥善处置受影响的存量业务，切实保障用户资金和信息安全。

具体应急预案如下:

1 编制总则

1.1 编制目的

为有效预防、及时控制和消除突发事件对广东外汇非现场检查系统及其支撑的业务应用造成的影响，指导和规范各类突发事件处理工作，最大程度减少突然事件对业务造成的影响，特编制

本预案。本预案由国家外汇管理局广东省分局外汇检查处主导，广发银行提供技术支持的方式进行。

1.2 编制依据

依《项目全流程管理体系过程文件》、《项目问题升级机制及要求》、《实施项目全流程操作指南》、《变更管理办法》、《应急管理预案》编制本预案。

1.3 适用范围

凡发生数据安全、资源高级、任务失败等事件影响广东外汇非现场检查系统正常运行或使用效果的，适用于本预案。

1.4 工作原则

坚持团队协作、资源共享、快速反应的工作原则，突然事件发生后，立即按照职责分工和相关预案开展应急处置工作。

2 应急保障

2.1 组织形式

应急团队由项目申报各方的运维、架构、安全、业务和其他相关团队组合建立，目标是推进稳定性建设、保障线上系统稳定运行，及时组织排除故障，跟进通报处理进展，回顾追踪遗留问题。

应急团队：所有人员。

应急基建团队：来自运维、架构、安全的参与者。

应急业务团队：来自业务团队的参与者。

应急值班小组：负责本周的线上保障工作，人员从应急团队中抽调，一般每周轮换一次，在周会上交接，受应急常务委员会领导。

基建小组：运维、架构、安全组成的值班小组。

业务小组：各业务线组成的值班小组

应急组长：一般由运维、架构或其他业务线同事担任，负责本周整个应急值班小组的协调工作。在故障发生时做决策、组织协调排查问题的第一责任人。组长也是对外发布信息的第二责任人（当副组长没有及时发布信息的情况下）。组长同时负责该组团队成员的工作分配和协调，并考核成员的表现。

应急副组长：负责故障处理时对外发布信息，同时兼任组长的备份。当故障发生时，包括但不限于以下情况：组长不能及时作出响应、组长授权、常务委员会授权或更高领导层授权等，应立即承担起组长的职责。

应急组员：非组长和副组长的当周值班成员都是组员，平时组员受组长和副组长协调和安排任务。在组长和副组长无响应的情况下，每一个组员都有义务承担起组长和副组长的职责。

组员和分工

运维：负责基础设施监控和处理、工单处理、变更实施。

架构：负责中间件的监控，错误码问题定位；在故障时采取何种止损方法应起到牵头作用。

安全：负责安全应急响应。

2.2　工作范围

包括系统线上故障的接单、组织处理、跟踪和回顾。原则上线上故障的发生都应在第一时间通知应急团队，应急团队组织协调力量处理并跟踪故障解决过程，同时负责及时对外发布线上故障的处理情况，包括不限于故障的接单、开始处理、持续更新的处理过程、系统恢复和后续跟踪。

应急值班小组当周的其他工作任务，包括不限于：跟踪事件工单上遗留项、梳理监控项、执行工单、变更、模拟演练、培训考试和其他委员会分配的任务。

2.3　工作时间

应急团队的工作时间是 7×24 小时，值班小组人员每周一轮换，周会上交接。周会结束前的故障由前一团队负责，周会结束后的故障由后一团队负责。

工作日 9:00-20:00 是应急团队的标准服务时间。值班时间内应急值班小组建议在监控中心驻场办公，不能现场办公的，应尽力在公司内办公，方便协作。小组对各系统实施持续监控，故障实施现场组织处理。

每日的 0:00-7:00 为应急团队的降级服务时间，此期间内各类响应时间不作考核，但成员电话需保证可达。应急小组成员应根据故障级别初判尽力提供服务，在高级别故障发生时，应急委员会成员和应急小组当班组长有权力组织成员立即提供标准级别服务。

其他时间段为非现场服务时间，应急小组成员在远程接单和处理故障。

2.4　工作地点

应急小组常用的会议和讨论室是应急指挥中心。

2.5　轮值人员纪律

组员在轮值期间始终在线。

非值班时间，前往无信号的地区应提前向组长报备，经批准后前往。避免长时间开车、出城旅行、户外、越野。随身应携带电脑并确保网络、电量。确保手机没有欠费。

夜间手机铃声应调大，避免静音。有必要的情况可以留一个备用电话给组长。

值班期间，所有当班人员应 5 分钟内响应（任何通讯方式）。非值班期间 15 分钟（企业微信或电话），夜间 20 分钟（电话）。从第一次尝试联系开始计算。

所有当班成员应避免休假、出差。无法避免的提前自己主管和应急组长提出，可以调配一名替换成员，但需明确职责和替换时间起终点。

组长发现应急成员工作量过大时，应及时向委员会提出资源请求。

组长在故障时拥有组织权和决定权，以止损为目的的操作可以先执行后汇报；组长对故障处理过程和结果负责。

3 应急事件

3.1 数据安全

出现不正常访问，包括：越权访问、违规下载数据、高频请求数据。

3.2 资源告急

当出现数据量急剧膨胀导致计算或存储资源不足时，可水平扩展达到快速扩容。

3.3 系统异常

由于系统异常如某个任务运行失败，使得模型任务失败导致关系网络不可用或运行结果不正确，影响业务应用。

4 应急响应

系统预警监控模块以邮件和短信的形式发布告警信息，应急响应小组当日相关负责人员快速介入定为问题，判断问题影响范围，无法判断的通知所有值班技术人员介入排查，3 分钟内无响应则升级到主管人员，一直升级到一级负责人为止。通过发布回滚，限流和机房切换等应急方案及时止损。实际操作过程中，根据部署环境是否双机房决定是否执行机房切换。

4.1　沟通机制

收到问题反馈–> 第一时间电话联系相关技术负责人 –> 3 分钟没有响应直接电话其主管 –> 超 5 分钟没有响应记录为一次应急响应纪律事件 –> 继续往上级升级到一级负责人。

4.2　问题闭环机制

每一个事件要求由当周值班业务线值班人员和组长、副组长负责到底，组长分配给业务线应急值班人员的事件由其负责跟进协调相关人员处理直到拿到结果，记录到事件单;

所有事件的第一负责人永远是当周应急值班人员，由其负责跟进协调相关人员处理直到拿到结果，记录到事件单;

因未全力跟进导致故障或者导致故障级别升级由其作为故障间接责任人。

4.3　响应流程

事件来源：应急响应团队的事件来源包括不限于：主动发现的异常、运营团队的反馈、应急响应群的消息、监控系统的告警、日志错误码或异常和其他任何方式反映线上系统可能或已经发生的故障。

接单：任何 1）形式的故障消息出现，应急团队应在 5 分钟内（非值班时间 15 分钟）作出响应，即接单。此时，副组长应该发布信息：“xx 问题收到，已经开始处理”。同时，需要把

问题录入到工单中，并给出链接，并将处理过程关键信息在上面进行更新。小组组长应该组织内部及外部力量开始处理问题。

判断：接单成员初判一下问题的影响大小，初定这个事件的级别，以下是大致的分类，实际情况级别可能随着问题的清晰而调整。

c0 ~ 已经有大面积故障反馈、核心主干断网、大面积机器或者网络故障。

c1 ~ 通过运营反馈的故障。

c2 ~ 技术上监控到异常但是并没有收到影响报告。

在值班时间内，初判 c1 以上的故障立即组织小型团队进行故障定位，包括对应该业务的相关人员、运营人员、架构组相关人员。

此时，副组长应该发布信息：“xx 问题初判级别 c1，正在联系 xx 处理”。这条消息应该在发布接单消息的 2 分钟内（非值班时间 5 分钟）。

升级和降级：当故障的影响更加清晰后，副组长可以调整问题的级别，对外发布。

处理：故障发生时，应急团队的主要职责是判断故障影响大小、迅速调用力量开始止损，这种力量可以是应急团队内的，但是大多数情况是团队外和发生故障的业务最紧密的成员。应先集中力量恢复系统，即止损。事故原因可以放在恢复以后再查。短时间无法恢复的，考虑切换机房解决。

故障处理信息发布：

如果故障持续在处理中，首小时内，c1 故障副组长应该每 5 分钟（非值班时间 20 分钟）对外发布简要处理情况；首小时后每 10 分钟通告一次。

c0 故障应该每 5 分钟对外发布情况。

故障处理日志记录: 应急小组接单时可以由组长或者副组长分配一名成员对这个故障进行记录，成为接单记录人，组员也可以自行记录时间点。在当周文档库中编辑故障处理文档，应一事一文档。记录内容应包括整个处理过程的日志、后续问题的跟进。

每天现场值班结束前，若当天发生过应急事件，应急组长或者指定组员负责与运营部门沟通当天故障处理情况回顾，并记录日志。

早会：前一天晚上（20 点～9 点）有重大故障发生的情况，组长应在工作日组织早会，时间一般是 10 点～11 点。组织该故障相关的所有成员参加，并作记录。有必要时，委员会成员参与会议。

5 应急培训与演练

5.1 培训知识点

目前运维后台的监测机制以及监控方法;

如何使用监控系统

如何快速使用日志系统

各个应用的的含义、作用

如何查看专线信息以及分配的宽带资源

不常见的错误码的详情解释及处理机制

不常见的错误码的详情解释及处理机制

是否有异常调用的统计信息，如何查询

关于流量下跌异常报警的处理方式

5.2 演练

故障演练每月一次，一般为当月第三周的周四

故障演练一般会提前同步到各业务线，演练过程中需确保业务不会阻碍演练过程。

演练人员安排:

总指挥-组长	负责现场统筹安排整个切换演练过程和现场决策
副组长	负责整个切换过程中的信息同步通报和信息记录，出记录文档
机房切换操作	负责整个切换流程的实际操作
机房切换指导	负责机房切换相关的指导
故障植入	负责在机房限制实施故障植入
质量保障	负责机房切换和故障植入期间所有缺陷和故障的记录，跟进相关改进措施制定和落实，包括在质量团队的闭环。

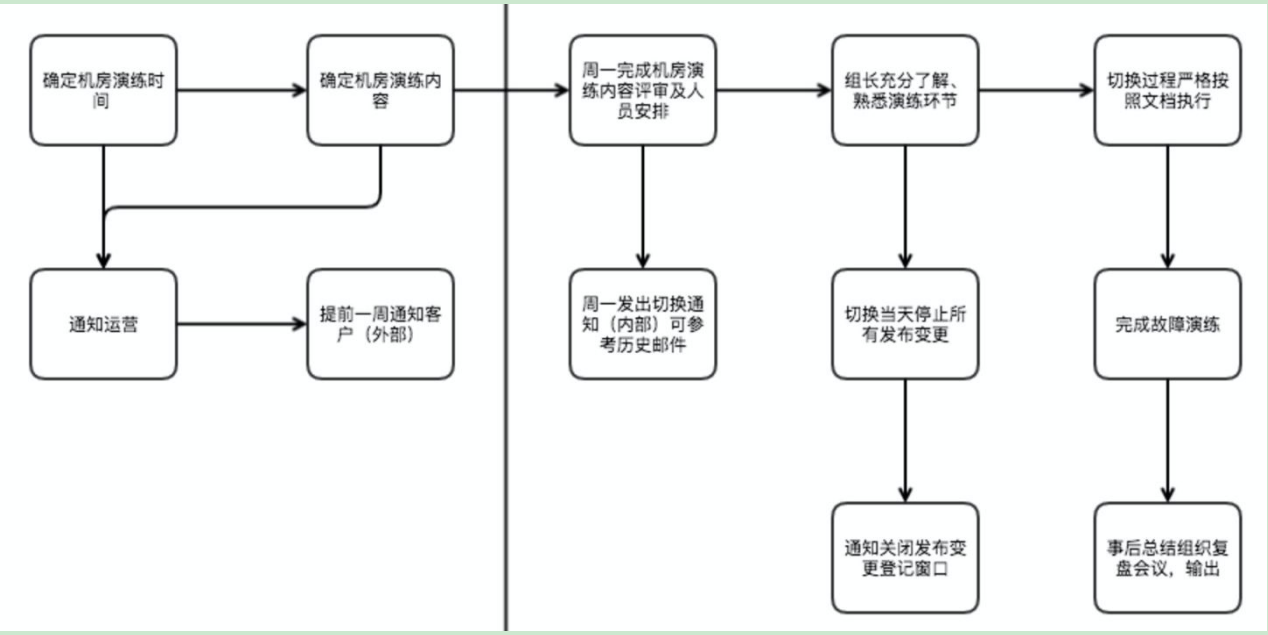

图 2　演练组织流程

注：上述流程中，根据环境是否双机房决定是否执行机房切换演练。

一、前期准备过程

1、发出演练通知，通知演练相关人员，各应用负责人包括运营负责人，提前一周发布通知。

2、机房自检，确保当前无上下联线路异常，处于单机或者单链路状态，检查当前机房是否正常。

3、演练当天禁止所有线上网络变更与应用发布，演练结束后恢复。

二、执行演练过程中涉及的变更

根据实际需要演练的内容填写，并详细填写每一步骤的时间。

三、失败的回滚处理

如果出现异常情况，按照事先预定的方案进行失败的回滚操作。

四、演练结束，确保所有演练的设备恢复正常后

恢复演练是所有涉及的操作、设备和应用配置等。

五、对演练过程出现的问题总结整改

总指挥负责发起故障回顾会议，并就本次应急演练相关事宜做总结。