国家金融监督管理总局办公厅关于加强银行业保险业移动互联网应用程序管理的通知

金办发〔2024〕99号

各金融监管局，各政策性银行、大型银行、股份制银行、外资银行、直销银行、金融资产管理公司、金融资产投资公司、理财公司，各保险集团（控股）公司、保险公司、保险资产管理公司、养老金管理公司，各金融控股公司：

为指导银行业金融机构、保险业金融机构和金融控股公司（以下统称金融机构）进一步提升服务质量，规范移动互联网应用程序（运行在移动智能终端上向内、外部用户提供服务的应用软件，包括但不限于移动应用APP、小程序、公众号等，以下简称移动应用）管理，经金融监管总局同意，现就有关工作通知如下：

一、金融机构应当重视移动应用管理工作，将移动应用建设纳入数字化转型整体规划，明确牵头管理部门，强化统筹管理，加强业务与科技协同，压实各方管理职责，规划建设功能全面、安全合规的移动应用。

二、金融机构应当加强移动应用统筹管理，建立移动应用台账，完善准入退出机制，统筹各部门及各分支机构的移动应用建设规划，合理控制移动应用数量。对用户活跃度低、体验差、功能冗

余、安全合规风险隐患大的移动应用及时进行优化整合或终止运营。

三、金融机构应当明确各移动应用的管理部门及责任人，完善内部管理机制，将合规要求落实到业务需求、产品研发、推广和运营的各个环节。

四、与政府部门、企业等第三方合作建设移动应用的，金融机构应当通过合同或者协议明确移动应用管理责任主体、约定双方责任义务，切实履行网络安全、数据安全责任。严禁第三方通过移动应用违规开展金融业务。

五、金融机构应当建立移动应用业务合规审核机制（含第三方合作业务），严格按照许可证载明的业务范围和地域范围开展业务，按监管要求开展销售过程可回溯、信息披露等工作，定期进行业务合规检查和审计。

六、金融机构开展移动应用需求管理，应当进行同类同质业务需求整合，使移动应用具备相对独立且完整的业务场景及功能，具有较高的使用便捷度，满足适老化、未成年人保护等要求，不得有歧视性限制，加强移动应用及第三方软件开发工具包安全需求分析。

七、金融机构应当做好移动应用方案设计、方案评审、软件开发、代码管理和变更控制等工作，对移动应用集成的源代码或组件（含第三方组件）开展安全风险管理，加强对客户认证和系统应用

逻辑控制的安全性测试，禁止在移动应用中嵌入无关链接、失效链接、恶意程序等存在风险的代码，并及时做好排查清理工作。

八、金融机构应当为移动应用（含第三方软件开发工具包）建立测试验证和上架发布制度，交付前完成缺陷和漏洞修复，与移动应用分发平台（通过互联网提供应用程序发布、下载、动态加载等服务活动的平台，包括应用商店、快应用中心、互联网小程序平台、浏览器插件平台等类型）协同配合，完成资质核验、上架审核、问题整改等工作，满足网络安全、数据安全、隐私保护、合规展业等要求后方可上架发布。金融机构应当自行管控移动应用的上架发布账号。

九、金融机构应当对移动应用（含第三方软件开发工具包）的运行状态进行实时监控，加强账号权限管理，做好老旧版本的更新、维护和下线。金融机构终止移动应用运营的，应当协同移动应用分发平台做好风险评估、数据迁移、隐私保护、用户告知等下架管理工作。金融机构应当加强对仿冒移动应用的监测排查，发现仿冒移动应用，应当尽快采取公开澄清等处置措施，并及时向金融监管总局或其派出机构报告。

十、金融机构应当加强移动应用与运行环境的兼容性、适配性管理，密切跟踪智能终端主要操作系统版本升级信息，关注移动应用分发平台的软件版本升级公告，提前开展移动应用（含第三方软件开发工具包）兼容性测试。开展移动应用适配性改造，应当制定改造方案和应急预案，强化安全管理。

十一、金融机构应当按照网信、工信部门要求，开展互联网信息服务和移动互联网应用程序备案工作。确定为重要信息系统（支撑重要业务，其信息安全和服务质量关系公民、法人和其他组织的权益，或关系社会秩序、公共利益乃至国家安全的信息系统，包括面向客户、涉及账务处理且实时性要求较高的业务处理类、渠道类和涉及客户风险管理等业务的管理类信息系统）的移动应用，应当按照重要信息系统投产变更相关要求，向金融监管总局或其派出机构报告。

十二、金融机构应当加强移动应用网络安全管理，严格落实国家网络安全等级保护制度，定期对移动应用进行安全加固，采取加密方式进行数据传输，监测识别异常流量、恶意程序、攻击入侵、安全漏洞、非法逆向分析破解、代码篡改及重打包等风险，发现问题及时处置。金融机构应当对移动应用注册用户进行有效身份核验。

十三、金融机构应当按照“谁管业务、谁管业务数据、谁管数据安全”的原则，明确移动应用数据安全管理责任。结合移动应用特点强化数据安全措施，有效防范数据泄露、篡改和勒索攻击等风险。

十四、金融机构委托外包服务提供商建设维护移动应用的，应当严格落实信息科技外包风险监管要求，开展移动应用外包准入、监控评价和风险管理，按照“必需知道”和“最小授权”原则严格控制外包服务提供商数据访问权限，督促其加强数据安全管理，防范数据泄露。

十五、金融机构应当加强移动应用业务连续性管理和突发事件应急管理，结合移动应用特点开展业务影响分析，建立应急处置机制，制定应急预案，定期开展演练，及时向金融监管总局或其派出机构报告重大突发事件。

十六、金融机构应当严格落实国家法律法规和监管要求，建立移动应用个人信息保护制度，规范个人信息管理，遵循“合法、正当、必要”原则收集个人信息，向用户告知收集个人信息的目的、使用和保护个人信息的方式，公布投诉渠道信息，及时处理信息泄露和隐私合规相关问题，保障消费者权益。

十七、金融机构应当将移动应用风险纳入全面风险管理，识别违规展业、侵害消费者权益等业务风险及网络安全漏洞等科技风险，健全风险防控措施，每年至少开展一次移动应用风险评估，每三年至少开展一次审计，发生重大移动应用风险事件时，应立即开展专项审计。

十八、各级派出机构应当压实辖内金融机构移动应用管理主体责任，督促辖内金融机构落实信息科技监管制度要求，加强移动应用监测预警，定期开展渗透测试。在非现场监管和现场检查中对移动应用相关风险加强关注，加大风险漏洞通报力度，及时督促整改。加强对金融机构移动应用违法违规问题处罚问责力度，对于因管理不当导致重大风险事件、存在严重风险隐患、风险排查流于形式、问题整改不力等情形严肃问责。

国家金融监督管理总局办公厅

2024年9月12日

标　题：	国家金融监督管理总局办公厅关于加强银行业保险业移动互联网应用程序管理的通知	发文机关：	金融监管总局办公厅
发文字号：	金办发〔2024〕99号	来　源：	金融监管总局网站
主题分类：	财政、金融、审计\其他	公文种类：	通知
成文日期：	2024年09月12日		