中国人民银行文件

银发〔2019〕237号

中国人民银行关于发布金融行业标准加强移动金融客户端应用软件安全管理的通知

中国人民银行上海总部，各分行、营业管理部，各省会（首府）城市中心支行，各副省级城市中心支行；国家开发银行，各政策性银行、国有商业银行、股份制商业银行，中国邮政储蓄银行；各证券公司、基金公司、期货公司、私募投资基金管理机构；各保险集团（控股）公司、保险公司、保险资产管理公司；中国银联股份有限公司、中国互联网金融协会、网联清算有限公司；各非银行支付机构：

为贯彻落实《中华人民共和国网络安全法》，加强移动金融客

户端应用软件（以下简称客户端软件）安全管理，现将《移动金融客户端应用软件安全管理规范》（JR/T 0092-2019，见附件，以下简称《规范》）印发给你们，并提出如下实施工作要求：

一、提升安全防护能力

各金融机构应严格按照《规范》要求，加强客户端软件设计、开发、发布、维护等环节的安全管理，构建覆盖全生命周期的管理机制，切实保障客户端软件安全。落实网络安全主体责任，采取有效措施防范应对网络攻击，保障相关系统平稳安全运行。对于资金交易类客户端软件，应从资金安全、信息保护等方面开展外部评估。对于信息采集类客户端软件，应重点从信息保护方面开展外部评估。外部评估应每年至少开展一次，形成报告存档备查。

二、加强个人金融信息保护

各金融机构应严格按照《规范》要求，采取有效措施加强客户端软件个人金融信息保护。一是收集、使用个人金融信息时应遵循合法、正当、必要的原则，明示收集使用信息的目的、方式和范围，并经用户同意。不得以默认、捆绑、停止安装使用等手段变相强迫用户授权，不得收集与其提供金融服务无关的个人金融信息。二是应采取数据加密、访问控制、安全传输、签名认证等措施，防止个人金融信息在传输、存储、使用等过程被非法窃取、泄露或篡改。三是信息使用结束后应立即删除敏感信息，在客户端软件卸载后不得留存个人金融信息。四是不得违反法律法

规与用户约定，不得泄露、非法出售或非法向他人提供个人金融信息。

三、提高风险监测能力

各金融机构要建立健全客户端软件风险监测管理机制，充分利用客户端软件风险监测平台，识别和处置客户端软件潜在的安全漏洞、权限滥用、信息泄露等风险隐患，对发现的漏洞和潜在的风险及时采取补救措施。中国互联网金融协会等应会同金融机构建立健全风险信息共享机制，加大联防联控力度，共同提高客户端软件安全水平。

四、健全投诉处理机制

各金融机构、中国互联网金融协会等要按照金融消费者权益保护相关规定，完善客户端软件投诉处理机制，按照“有人理诉，有序办诉，高效处诉”的工作原则，规范受理渠道和办理流程，及时处理投诉建议。中国互联网金融协会等应完善投诉调查取证和转移处理机制，通过机构核实、现场检查、技术检测、专家评议等方式进行查证，对查证属实的要督促金融机构做好整改。

五、强化行业自律管理

中国互联网金融协会等要加强客户端软件行业自律管理，制定行业公约，建立健全黑名单管理、自律检查、违规约束、信息共享等机制，做好客户端软件实名备案、风险监测等工作，督促金融机构严格落实本通知各项规定。同时，定期向人民银行报送相关情况。

请人民银行副省级城市中心支行以上分支机构将本通知转发至辖区内分支机构和金融机构，组织做好客户端软件安全管理等工作。

联 系 人：科技司刘雨露、关晓辉

联系电话：010-66199548、010-66195269

附件：移动金融客户端应用软件安全管理规范

中国人民银行

2019年9月27日

附件

ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0092—2019
代替 JR/T 0092—2012

移动金融客户端应用软件安全管理规范

Financial mobile application software security management specification

2019－09－27 发布　　2019－09－27 实施

中国人民银行　　发布