特　急

中国人民银行文件

银发〔2016〕170号

中国人民银行关于
进一步加强银行卡风险管理的通知

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；各国有商业银行、股份制商业银行，中国邮政储蓄银行；中国银联股份有限公司，中国支付清算协会：

随着移动通信技术和互联网金融的快速发展，银行卡使用安全面临新的挑战。为进一步加强银行卡信息的安全管理，提升支付风险防控能力，现将有关事项通知如下：

一、强化银行卡信息的安全管理

（一）强化支付敏感信息内控管理。各商业银行、支付机构（从事银行卡收单业务、网络支付业务的非银行支付机构，下同）、银行卡清算机构应严格落实《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》（银发〔2011〕17号），健全支付敏感信息安全内控管理制度，并将有关情况于2016年9月1日前报告人民银行。一是严禁留存非本机构的支付敏感信息（包括银行卡磁道或芯片信息、卡片验证码、卡片有效期、银行卡密码、网络支付交易密码等），确有必要留存的应取得客户本人及账户管理机构的授权。二是明确相关岗位和人员的管理责任，严格分离不相容岗位并控制信息操作权限，制定信息操作流程和规范，强化内部监督、责任追究机制，严禁从业人员非法存储、窃取、泄露、买卖支付敏感信息。三是每年应至少开展两次支付敏感信息安全的内部审计，并形成报告存档备查。发现因系统漏洞造成支付敏感信息泄露或内部人员违规行为的，应立即采取有效措施防止风险扩大，并向人民银行报告；涉嫌违法犯罪的，应及时报告公安机关。

（二）加强支付敏感信息的安全防护。各商业银行、支付机构应在客户端软件与服务器、服务器与服务器之间进行通道加密和双向认证，对重要信息关键字段进行散列或加密存储，保障信息传输、存储、使用安全。开展网络支付业务时，不得委托或授权无支付业务资质的合作机构采集支付敏感信息，应采用具有信

息输入安全防护、即时数据加密功能的安全控件，采取有效措施防止合作机构获取、留存支付敏感信息。

（三）全面应用支付标记化技术。自2016年12月1日起，各商业银行、支付机构应使用支付标记化技术（Tokenization），对银行卡卡号、卡片验证码、支付机构支付账户等信息进行脱敏处理，并通过设置支付标记的交易次数、交易金额、有效期、支付渠道等域控属性，从源头控制信息泄露和欺诈交易风险。

（四）强化交易密码保护机制。各商业银行、支付机构应加强银行卡、网络支付等交易密码的保护管理和客户安全教育，严格限制使用初始交易密码并提示客户及时修改，建立交易密码复杂度系统校验机制，避免交易密码过于简单（如“111111”、“123456”等）或与客户个人信息（如出生日期、证件号码、手机号码等）相似度过高。

（五）严格规范收单外包服务。各商业银行、支付机构应严格落实《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）、《中国人民银行关于加强银行卡收单业务外包管理的通知》（银发〔2015〕199号），承担收单环节支付敏感信息安全管理责任。一是不得将核心业务系统运营、受理终端密钥管理、特约商户资质审核等工作交由外包服务机构办理。二是指定专人管理终端密钥和相关参数，确保不同的受理终端使用不同的终端主密钥并定期更换。三是通过协议禁止实体和网络特约商户、外包服务机构留存支付敏感信息。四是每年对外包服务机构、实体

和网络特约商户至少开展一次有一定独立性的安全评估，并形成报告存档备查，对于未遵守相关协议的，应立即中断合作。

（六）加强支付创新规范管理。对于重要支付技术应用、业务创新，各商业银行、支付机构应至少于项目上线前30日向人民银行备案，提交项目实施方案、外部安全评估报告等书面材料。业务开展过程中，应做好风险的动态监测、评估和防控工作。

二、加大银行卡互联网交易风险防控力度

（一）强化客户端软件安全管理。一是各商业银行、支付机构应从木马病毒防范、信息加密保护、运行环境可信等方面提升客户端软件安全防控能力。客户端软件应能够监测并向后台系统反馈手机支付环境安全状况，作为限制、拒绝交易等风控策略的依据。二是对客户端软件及官方网站设置可信标识或快捷入口，并通过多种渠道告知客户正确的识别及访问方法。三是每年必须至少开展一次外部安全评估，形成报告存档备查，确保技术标准符合性。

（二）加强业务开通身份认证安全管理。自2016年11月1日起，各商业银行基于银行卡与支付机构、商业机构建立关联业务时，应严格采用多因素身份认证方式，直接鉴别客户身份，并取得客户授权。身份鉴别应采取以下组合方式之一：一是采用符合《金融电子认证规范》（JR/T 0118）的数字证书，并组合交易密码等至少一种认证因素。二是采用符合《动态口令密码应用技术规范》（GM/T 0021）的动态令牌设备，并组合交易密码等至少

一种认证因素。三是至少组合两种动态认证因素（如动态验证码、基于客户行为的动态挑战应答等），并采用语音、短信、数据（如手机银行、即时通讯、邮件）等至少两种不同通信渠道。

（三）提升支付交易安全强度。一是各商业银行应依照《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》（银发〔2015〕392号），建立健全个人银行结算账户分类管理机制，引导客户使用II类、III类银行账户办理小额网络支付业务，有效防控各类银行账户特别是I类账户的信息泄露风险。二是在支付机构等合作方向商业银行发送支付指令、扣划客户银行卡资金时，各商业银行、支付机构应严格落实《非银行支付机构网络支付业务管理办法》（中国人民银行公告〔2015〕第43号公布）第十条规定，采取交易验证强度与交易额度相匹配的技术措施，提高交易的安全性。

（四）加强互联网交易风险监控。各商业银行、支付机构应利用大数据分析、用户行为建模等手段，建立交易风险监控模型和系统，及时预警异常交易，并采取调查核实、风险提示、延迟结算等措施。针对批量或高频登录等异常行为，应利用IP地址、终端设备标识信息、浏览器缓存信息等进行综合识别，及时采取附加验证、拒绝请求等手段。

（五）加大支付风险联动防控力度。各商业银行、支付机构应认真落实《中国人民银行 工业和信息化部 公安部 工商总局关于建立电信网络新型违法犯罪涉案账户紧急止付和快速冻结机制

的通知》（银发〔2016〕86号），按照要求接入电信网络新型违法犯罪交易风险事件管理平台，加强涉案账户的止付、冻结管理。

三、切实防范磁条卡伪卡欺诈交易风险

（一）使用金融IC卡降低磁条交易风险。一是自2016年9月1日起，各商业银行新发行的基于人民币结算账户的银行卡，应为符合《中国金融集成电路（IC）卡规范》（JR/T 0025）的金融IC卡，并采用通过国家认证认可管理部门认可机构安全评估的芯片。二是各商业银行应从交易渠道、刷卡频次、单笔交易金额、日累计交易金额、交易地区等方面，进一步加强磁条交易风险控制。对于可疑交易应通过短信、电话、客户端软件等进行交易确认和风险提示。自2017年5月1日起，全面关闭芯片磁条复合卡的磁条交易。三是各商业银行应采取换卡不换号、实时发卡等措施加快存量磁条卡更换为金融IC卡的进度。

（二）加强受理终端安全管理。各商业银行、支付机构应从受理终端产品选型、验收、现场检查等环节加强安全管理，确保受理终端的技术标准符合性。银行卡清算机构应会同成员机构采取入网终端签名、唯一性标识等技术措施，加强受理终端入网管理，严禁不符合标准、非法改装的受理终端入网使用。对于存量终端应建立定期检查机制，持续开展终端抽检工作，确保布放的终端与合格样品的一致性，严控改装终端的使用。

（三）加大特约商户实名制管理力度。银行卡清算机构应会同成员机构建立健全实体和网络特约商户信息电子化管理体系，

严格落实特约商户实名制相关规定，完整、准确记录特约商户及其法定代表人或主要负责人的身份信息，并对同一特约商户在不同商业银行和支付机构注册的信息进行关联管理。充分利用影像采集、区域定位等技术，采取多渠道交叉验证等有效手段，健全特约商户资质审核和信息更新机制，持续加强特约商户信息真实性管理。

（四）加强违规特约商户黑名单管理。一是各商业银行、支付机构应建立健全违规实体和网络特约商户黑名单管理制度，明确黑名单纳入与移出条件、惩罚措施等。加强对特约商户的监测、巡检，对于存在支付敏感信息泄露、非法改装终端、参与伪卡欺诈等违规行为的，应纳入黑名单管理，视严重程度从严采取延迟结算、暂停交易、终止合作等惩戒措施，并及时通知中国支付清算协会、银行卡清算机构。二是中国支付清算协会、银行卡清算机构应会同商业银行、支付机构建立健全黑名单信息共享和查询机制，加大联合惩戒力度，禁止拓展已纳入黑名单的特约商户。

（五）落实伪卡欺诈风险责任转移规则。银行卡清算机构应会同成员机构进一步落实银行卡受理过程中的伪卡欺诈风险责任，保护芯片化迁移方的权益。建立完善的投诉处理机制，妥善处理欺诈风险事件，切实保障客户的合法权益。

四、严格落实各项规定，加大督查处罚力度

（一）严格落实国家网络安全和标准符合相关规定。各商业银行、支付机构、银行卡清算机构要严格落实国家网络安全和信

息技术安全有关规定，使用经国家密码管理机构认可的商用密码产品。一是涉及的客户端软件、受理终端、银行卡、数字证书、动态令牌设备等应符合国家和金融行业相关标准，并通过国家认证认可管理部门认可机构的安全评估。二是业务系统建设和运营应符合国家信息安全等级保护的相关要求。三是业务系统及备份系统应按照国家网络安全相关要求部署在我国境内。

（二）建立健全监督检查机制。人民银行分支机构要高度重视、长抓不懈，成立银行卡风险管理领导小组，建立日常监督检查机制，将支付业务系统安全生产、受理终端（含网络支付接口）安全、支付敏感信息保护等纳入执法检查，统筹做好指导协调、政策宣传、执法检查、情况通报等工作。

（三）加大违规行为处罚力度。人民银行分支机构要严查因银行卡受理终端改装、支付交易验证强度低、系统存在安全漏洞及受到网络攻击等造成的支付服务中断、支付敏感信息泄露、资金损失事件，并依照《银行卡收单业务管理办法》、《非银行支付机构网络支付业务管理办法》等有关规定从严处罚。对于情节严重的，依照《中华人民共和国中国人民银行法》第四十六条规定，对相关机构及负有直接责任的董事、高级管理人员和其他直接责任人员进行处罚；涉嫌犯罪的，及时报告公安机关。对于情节严重的支付机构，还应按照《非金融机构支付服务管理办法》（中国人民银行令〔2010〕第2号发布）、《非银行支付机构分类评级管理办法》（银发〔2016〕106号文印发）规定调低分类评级直至注

销《支付业务许可证》。

（四）加强行业自律规范。中国支付清算协会要按照本通知要求和相关规定，制定银行卡风险管理行业自律规范，建立自律检查、违规约束机制，并于2016年9月30日前向人民银行报备后组织实施，督促会员单位加强自律，严格落实各项规定。

对于本通知规定的报告、报备事项，全国性商业银行、中国支付清算协会、银行卡清算机构应报送人民银行总行，其他银行业金融机构、支付机构应报送法人所在地人民银行副省级城市中心支行以上分支机构。

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地方性银行业金融机构和支付机构，加强组织落实。

联 系 人：汤沁莹 王禄禄

联系方式：010-66194650　010-66199520

互联网电子邮箱：IC_Office@pbc.gov.cn

中国人民银行

2016年6月13日

内部发送：办公厅，科技司，条法司，支付司，消保局。

中国人民银行办公厅　　2016年6月15日印发