403--中国银监会办公厅关于加强银行卡信息安全防护工作的通知  
（银监办发〔2014〕248号）

各银监局，各国有商业银行、股份制商业银行，邮政储蓄银行，各省级农村信用联社：

近期，公安机关查获一起银行卡伪卡犯罪案件，犯罪嫌疑人系银行ATM设备维护服务商的工作人员，其利用工作之便，在所维护的银行ATM设备上大肆复制交易数据，并批量制作伪卡，导致多家银行的客户资金被盗，涉案金额数量较大。这起案件反映出部分商业银行未认真贯彻落实银监会发布的信息科技外包风险监管指引，以及加强客户数据保护，禁止明文存储客户密码、银行卡磁道数据等监管要求，还存在对信息安全工作不够重视，对外包人员缺乏基本监控，对信息安全的事中、事后监督检查不够等问题。为有效防范风险现就进一步加强银行卡安全保护工作有关事项通知如下：

一、严格落实信息安全管理的领导责任。银行业金融机构要提高法律意识，切实承担保护消费者合法权益的责任。要加强信息安全工作的组织领导，落实信息安全责任制度、考核制度和问责制度。要明确并落实董事会和高管层的安全管理责任，明确具体主管领导和责任部门。要强化“一把手”问责，对于有关安全事件，要追究相关领导责任。

二、通过审计、风险、合规等条线加强监督检查。银行业金融机构银行卡相关业务主管部门要负起管理责任，切实落实安全管理要求。风险管理的二、三道防线要明确职责边界，建立对数据安全保护常态化监督和检查机制，督导业务和技术各相关部门做好风险评估、问题排查。要充分发挥审计部门独立监督作用，针对上述案暴露的问题，银行业金融机构审计部门要立即牵头在全行范围内开展一次银行卡系统及机具的安全和外包管理检查，防范案件风险。检查要不留死角、排查到位，对检查发现的问题要制定时间表、抓紧整改。通过检查，要确保本行信息系统和机具内没有客户密码、银行卡磁道信息等敏感数据明文存放现象，审计部门要在检查报告对上述内容予以确认，检查情况要报董事会审批。

三、强化自助设备外包管理。银行业金融机构要严格落实信息科技外包风险监管要求，评估并完善外包服务机构安全管理标准，着力加强自助设备外包服务的过程监督和信息安全管控，强化ATM设备维护人员管理，加强监督核查，对于达不到安全管理要求的外包服务机构，要建立退出机制。银监会将把自助设备运维外包纳入非驻场集中式外包风险监管框架，将其作为监管评级的重要因素；对风险高、问题突出的外包服务机构，将建立“黑名单”，向银行业进行通报。

四、加快信息系统升级改造。银行业金融机构要对本行的信息系统和机具进行重检，及时对老旧设备和系统进行升级。ATM设备要做到对客户密码的硬加密，并在加密通道内进行安全传输，严禁以明文形式在ATM设备、交换网络、收单前置等系统中“落地”，禁止在日志和归档文件内保存；禁止制卡文件明文保存。要加强持卡人数据的访问控制管理，根据业务“必须知道”和“最小授权”原则，严格对敏感数据的访问实行授权管理。

请各银行业金融机构11月10日前向银监会或其派出机构报送检查报告；银监局汇总报告后于11月15日前报送银监会。银监会将对各银行业金融机构自查情况进行检查，对自查不认真、走过场、问题突出的银行业金融机构将进行通报，并采取监管措施。

联系人：戴越，郑妍

联系电话：010-66278562，010-66278565

邮　箱：daiyue@cbrc.gov.cn

中国银行业监督管理委员会办公厅

2014年10月8日