特　急

中国人民银行办公厅文件

银办发〔2016〕192号

中国人民银行办公厅关于开展银行卡信息泄露风险专项排查工作的通知

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：

为防范支付敏感信息和资金的安全风险，切实保障消费者合法权益，人民银行决定开展银行卡信息泄露风险专项排查工作。现就有关事项通知如下：

一、工作目标

全面摸底支付业务系统、风控措施、管理制度等方面存在的

支付敏感信息和资金安全隐患。对发现的风险实施清单管控，及时采取有效措施排除隐患、控制风险传导。建立健全支付风险管理长效机制，持续做好风险监测、预警，切实提升风险防控水平。

二、工作依据

（一）政策文件。

《中国人民银行关于进一步加强银行卡风险管理的通知》（银发〔2016〕170号）、《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）、《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）等。

（二）标准规范。

《中国金融移动支付 客户端技术规范》（JR/T 0092）、《中国金融集成电路（IC）卡规范》（JR/T 0025）、《银行卡销售点（POS）终端技术规范》（JR/T 0001）、《银行卡自动柜员机（ATM）终端技术规范》（JR/T 0002）、《银行卡受理终端安全规范》（JR/T 0120）、《网上银行系统信息安全通用规范》（JR/T 0068）、《非金融机构支付业务设施技术要求》（JR/T 0122）、《金融行业信息系统信息安全等级保护实施指引》（JR/T 0071）等。

三、排查内容和范围

（一）排查内容。

按照《银行卡信息泄露风险专项排查列表》（见附件）开展排查。主要内容包括：一是排查影响支付敏感信息保护、交易安全、业务连续性等系统方面的隐患；二是排查内部审计、外部安

全评估、交易监控、受理终端安全等风控方面存在的问题；三是排查支付敏感信息安全内控、收单外包、特约商户实名制和黑名单等制度方面的不足。

（二）排查范围。

1.机构范围：商业银行、非银行支付机构、银行卡清算机构（以下统称从业机构）。

2.系统范围：涵盖从业机构与个人账户信息、支付业务处理相关的系统。包括商业银行的银行卡、网络支付、网上银行、手机银行等业务系统，非银行支付机构的网络支付、银行卡收单等业务系统，银行卡清算机构的银行卡转接清算系统等。

四、工作安排

（一）从业机构自查整改（2016年9月-11月）。

从业机构严格对照《银行卡信息泄露风险专项排查列表》逐项对本机构银行卡信息泄露风险隐患进行自查，及时采取有效措施，对发现的问题进行整改，并建立问题清单管控和动态跟踪机制。对于短期内无法完成整改的问题，要采取补偿措施，明确整改计划和方案，按期整改。2016年12月2日前，形成自查报告报送人民银行。

（二）人民银行核实（2016年12月-2017年1月）。

人民银行对从业机构自查结果及整改情况采取访谈、查看系统、查阅资料等方式进行全面核实。对于自查质量不高、问题较多或整改率较低的从业机构，将进行现场核实。其中，人民银行

总行负责核实全国性商业银行和银行卡清算机构的自查整改情况，人民银行分支机构负责核实辖区内从业机构的自查整改情况。

（三）总结及后续管理（2017年2月-3月）。

人民银行分支机构要对整体情况及主要问题进行认真全面分析总结，形成书面报告，于2017年2月28日前报送人民银行总行。对于未完成整改的问题，要求从业机构作为2017年内部审计和外部安全评估的重点，持续监督整改。

人民银行总行将根据排查整体情况，总结归纳突出、典型问题，及时发布风险提示，并对风险排查及整改情况进行通报。

五、工作要求

（一）人民银行分支机构要成立由科技、支付结算等部门组成的专项排查小组，制定切实可行的排查方案，认真组织从业机构进行全面自查及整改，做好核实工作。对于排查过程中发现违法违规、情节严重的问题，按照《中国人民银行关于进一步加强银行卡风险管理的通知》要求进行处理。

（二）从业机构要高度重视，根据本通知要求制定行之有效的自查方案，全面展开自查和整改工作，积极配合人民银行分支机构做好核实工作。

（三）对于本通知规定的报告事项，全国性商业银行、银行卡清算机构报送人民银行总行，其他银行业金融机构、非银行支付机构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从事银行卡收单业务、网络支付业务的非银行支付机构，并组织落实。

联 系 人：汤沁莹 周玥

联系电话：010-66194650 010-66199233

互联网电子邮箱：IC_Office@pbc.gov.cn

附件：银行卡信息泄露风险专项排查列表

中国人民银行办公厅

2016年9月18日

附件

银行卡信息泄露风险专项排查列表

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	排查结果			备注
						通过	不通过	不适用	
一、银行卡信息的安全管理									
1	支付敏感信息内控管理	应禁止在系统中（包括日志文件、数据库等）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）。	系统类	商业银行 非银行支付机构 银行卡清算机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				
2		应对操作系统、数据库、中间件及应用系统进行访问控制，并限制默认用户或高权限用户的使用。包括限制root用户直接登录、限制su命令使用、修改默认用户口令等。	系统类	商业银行 非银行支付机构 银行卡清算机构	1.查阅材料（自查报告、记录文档、系统文档等） 2.查看系统				
3		应在操作系统和数据库中采用最小授权原则，禁止共享账户，并在不同账户之间形成相互制约关系。如设置管理员、安全员、审计员等多个用户角色，且角色权限分离。	系统类	商业银行 非银行支付机构 银行卡清算机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				
4		应加强生产数据的安全管理，包括但不限于: 1.开发环境禁止使用生产数据。 2.测试环境使用的生产数据应进行脱敏处理。	系统类	商业银行 非银行支付机构 银行卡清算机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				
5		系统应具有针对网络、主机和应用软件的审计功能，并对审计日志进行有效保护。	系统类	商业银行 非银行支付机构 银行卡清算机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				

序号	排查项	排查要点	类型	机构类型	排查方法	排查结果			
						通过	不适用	不通过	备注
6	支付敏感信息内控管理	不得留存非本机构的支付敏感信息，确有必要留存的，应建立客户及账户管理机构授权机制，并保存记录。	风控类	商业银行 非银行支付机构 银行卡清算机构	查阅材料（自查报告、记录文档等）				
7		应严格分离不相容岗位并控制信息操作权限，建立关键操作的审批机制，并保存记录。	风控类	商业银行 非银行支付机构 银行卡清算机构	查阅材料（自查报告、记录文档等）				
8		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。	风控类	商业银行 非银行支付机构 银行卡清算机构	查阅材料（内部审计报告等）				
9		应建立支付敏感信息泄露、内部人员违规行为的报告机制（包括向人民银行、公安机关等相关部门报告），并保存记录。	风控类	商业银行 非银行支付机构 银行卡清算机构	查阅材料（自查报告、管理制度、记录文档等）				
10		应具备支付敏感信息安全内控管理制度，明确支付敏感信息保护、相关岗位和人员的管理职责、内部审计、安全事件处置等相关要求。	制度类	商业银行 非银行支付机构 银行卡清算机构	查阅材料（自查报告、管理制度等）				
11	支付敏感信息安全防护	应采取有效措施对生产环境与办公、开发、测试等环境进行隔离。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、管理制度、外部安全评估报告、系统文档等） 2.查看系统				
12		客户端软件与服务器之间、服务器与服务器（通过互联网连接）之间应使用双向认证技术防范中间人攻击，保障通信双方的保密性、真实性。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				
13		用户访问异常中断后，系统应具有防护手段，保证支付敏感信息不丢失。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				

						检查结果			备注
						通过	不通过	不适用	
14	支付敏感信息安全防护	客户端软件应采取有效措施对残余信息进行保护，包括但不限于: 1.支付敏感信息在使用完毕后，立即进行清除。 2.确保无法通过技术手段恢复已清除的支付敏感信息。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				
15		对需要送出维修或销毁的存储支付敏感信息的介质，应采取不可恢复的方式进行信息销毁。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、外部安全评估报告、记录文档、系统文档等） 2.查看系统				
16		系统应对金融IC卡个人化数据进行全过程加密保护，个人化完成后及时删除敏感信息。	系统类	商业银行	1.查阅材料（自查报告、记录文档、系统文档等） 2.查看系统 3.现场访谈				
17		应对重要信息进行保护和备份，包括但不限于以下措施: 1.对重要信息进行严格的访问控制和安全存储。 2.对重要信息及时备份，并定期进行恢复性测试。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、外部安全评估报告、记录文档、系统文档等） 2.查看系统				
18		应对重要信息关键字段进行散列或加密存储。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				

序号	排查项	排查要点	类型	适用范围	排查方法				
19	支付敏感信息安全防护	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等技术，防范合作机构获取、留存支付敏感信息。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				
20		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。	系统类	商业银行 非银行支付机构 银行卡清算机构	1.查阅材料（自查报告、系统文档等） 2.查看系统				
21		系统应遵循最小化安装原则，包括但不限于： 1.最小化安装系统组件和应用程序。 2.仅开启必要的服务及端口，禁用或删除无用的服务，如Telnet、SendMail等。	系统类	商业银行 非银行支付机构 银行卡清算机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				
22		应增强系统账户口令复杂度（包括生产、测试环境等），包括但不限于： 1.口令长度不少于8位。 2.包含数字、字母、特殊字符中至少两种。 3.定期修改口令。	系统类	商业银行 非银行支付机构 银行卡清算机构	1.查阅材料（自查报告、外部安全评估报告等） 2.查看系统				
23		系统应采取有效的技术措施对单个账户的多重并发会话进行限制。	系统类	商业银行 非银行支付机构 银行卡清算机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				
24		系统应定期进行漏洞扫描，对扫描发现的漏洞及时进行修补确认。	系统类	商业银行 非银行支付机构 银行卡清算机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				

						检查结果			备注
						通过	不通过	不适用	
25	支付敏感信息安全防护	应对使用的第三方软件进行安全管理，包括但不限于: 1.使用第三方软件前进行测试确认。 2.及时对第三方软件进行更新。	系统类	商业银行 非银行支付机构 银行卡清算机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				
26		系统应对统一资源定位符（URL）地址使用进行安全控制，包括但不限于: 1.禁止在URL地址中直接引用内部文件名或数据库关键字。 2.设置服务器上目录和文件夹的访问权限。 3.验证并拒绝包含“./”或“../”的URL地址请求。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				
27		系统应对输入信息进行有效过滤，防范结构化查询语言（SQL）注入攻击。包括过滤或替换输入信息中的危险SQL字符、使用SQL防注入系统或应用层防火墙等。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				
28		系统应采取有效措施防范跨站脚本攻击，如对客户端通过Get、Post等方式提交的字符串进行过滤。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				
29		系统应限制上传文件的类型和大小，防范恶意文件上传。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				
30		系统应采取有效技术措施保护本地缓存，防范用户非法获取支付敏感信息或破坏WEB缓存文件。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、系统文档等） 2.查看系统				

序号	排查项	排查要点	类型	适用主体	排查方法				
31	支付敏感信息安全防护	系统应具备防钓鱼措施，包括要求用户设置预留信息、防范用户请求被恶意重定向等。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				
32		应禁止通过互联网直接访问生产环境数据库服务器、日志服务器等。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				
33		应与合作机构签订协议，明确网络支付业务敏感信息保护的相关条款。	风控类	商业银行 非银行支付机构	查阅材料（自查报告、合同协议等）				
34		应具备密钥管理制度，明确密钥安全保护措施，控制密钥的使用权限。	制度类	商业银行 非银行支付机构	查阅材料（自查报告、管理制度等）				
35		应具备相关管理制度，明确网络支付业务敏感信息保护相关要求，包括但不限于: 1.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。 2.禁止合作机构获取、留存支付敏感信息。	制度类	商业银行 非银行支付机构	查阅材料（自查报告、管理制度等）				
36	支付标记化技术应用	系统应能够通过支付标记化技术，防范跨渠道交易安全风险。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、系统文档等） 2.查看系统				
37		对互联网渠道业务，系统应能够使用支付标记化技术对银行卡卡号、卡片验证码、非银行支付机构支付账户等信息进行脱敏处理，防范信息泄露风险。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、系统文档等） 2.查看系统				
38		对互联网渠道业务，系统应能够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，进行交易风险控制。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、系统文档等） 2.查看系统				

						检查结果			备注
						通过	不通过	不适用	
39	支付标记化技术应用	应制定支付标记化技术应用的工作方案，明确工作计划和具体措施，确保支付标记化技术应用有序推进。	风控类	商业银行 非银行支付机构	查阅材料（自查报告）				
40	交易密码保护	在客户首次交易时，系统应限制使用初始交易密码并提示客户及时修改。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、系统文档等） 2.查看系统				
41		在客户设置或修改交易密码时，系统应采取风险提示、密码复杂度校验等措施，防范因密码过于简单或与客户个人信息相似度过高带来的风险。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、系统文档等） 2.查看系统				
42		应对客户开展安全教育工作，及时提示加强密码保护。如提醒客户设置独立的支付密码等。	风控类	商业银行 非银行支付机构	查阅材料（自查报告）				
43	收单外包服务	应与实体和网络特约商户、外包服务机构签订协议，明确禁止其留存支付敏感信息的相关条款。	风控类	商业银行 非银行支付机构	查阅材料（自查报告、合同协议等）				
44		应按照《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）要求，每年对所有外包服务机构至少开展一次有一定独立性的安全评估，形成报告存档备查。	风控类	商业银行 非银行支付机构	查阅材料（自查报告、记录文档等）				
45		应制定具有一定独立性的安全评估方案，每年对实体和网络特约商户至少开展一次抽查，并保证在三年内每个商户被抽查一次，形成报告存档备查。	风控类	商业银行 非银行支付机构	查阅材料（自查报告、外部安全评估报告、记录文档等）				

序号	排查项	排查要点	类型	检查对象	排查方法				
46	收单外包服务	应具备收单外包服务管理制度，明确相关管理要求，包括但不限于： 1.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。 2.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。 3.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。	制度类	商业银行 非银行支付机构	查阅材料（自查报告、管理制度等）				
47	支付创新规范管理	重要支付技术应用、业务创新开展过程中，应建立风险动态监测、评估和防控工作机制，保存记录。	风控类	商业银行 非银行支付机构	查阅材料（自查报告、记录文档等）				
48		应具备支付创新规范管理制度，明确对于创新技术首次在支付领域使用、跨境合作、社会关注度较高等重要支付创新项目的相关要求，包括但不限于： 1.至少于项目上线前30日向人民银行备案。 2.备案材料包括项目实施方案、外部安全评估报告等书面材料。	制度类	商业银行 非银行支付机构	1.查阅材料（自查报告、外部安全评估报告、管理制度等） 2.现场访谈				
二、银行卡互联网交易风险防控									
49	客户端软件安全管理	客户端软件应具有木马病毒防范、信息加密保护、完整性检查等功能，能够防篡改、防破解。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				
50		系统应能够对手机支付环境安全风险进行监控，包括但不限于： 1.客户端软件能够监测并向后台系统反馈手机支付环境安全状况，如手机是否被root等。 2.后台系统能够根据手机支付环境监测数据采取限制、拒绝交易等风控措施。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				

						排查结果			备注
						通过	不通过	不适用	
51	客户端软件安全管理	客户端软件应对应用程序接口进行保护，防止应用程序接口被非授权调用。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				
52		客户端软件应设计合理的账户登录超时控制策略，当用户闲置在线状态超出时限时，客户端自动退出登录状态。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				
53		客户端软件应设计合理的交易时限控制策略，当用户单笔交易超出规定时限时，交易自动终止。	系统类	商业银行 非银行支付机构	查阅材料（自查报告、外部安全评估报告、系统文档等）				
54		客户端软件登录时，若身份验证连续失败超过一定次数，应及时锁定用户登录权限或支付账户使用权限，并立即通过可靠渠道（如短信、电话、即时通讯等）通知客户。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				
55		客户端软件应采取有效措施防范登录操作的重放攻击，如在登录交互过程提交的认证数据中增加服务器生成的随机信息。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				
56		应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。	风控类	商业银行 非银行支付机构	1.查阅材料（自查报告） 2.现场访谈				
57		应每年至少开展一次客户端软件外部安全评估，并形成报告存档备查。	风控类	商业银行 非银行支付机构	查阅材料（自查报告、外部安全评估报告等）				

序号	排查项	排查表单	类型	适用机构	检查方法				
58	业务开通身份认证安全管理	开通支付业务时，系统应采取以下身份鉴别组合之一： 1.采用数字证书+交易密码（或动态验证码）方式，且数字证书符合《金融电子认证规范》（JR/T 0118）。 2.采用动态口令+交易密码（或动态验证码）方式，且动态口令符合《动态口令密码应用技术规范》（GM/T 0021）。 3.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。 4.经外部安全评估，安全强度不低于以上三种方式的多因素身份鉴别组合。	系统类	商业银行	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统 3.现场访谈				
59		商业银行基于银行卡与非银行支付机构、商业机构建立关联业务时，应采用多因素身份认证方式，直接鉴别客户身份，取得客户授权，并保存记录。	风控类	商业银行	1.查阅材料（自查报告、记录文档等） 2.现场访谈				
60	支付交易安全强度	系统应依照《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）要求，实现对Ⅰ类、Ⅱ类和Ⅲ类个人银行账户的有效区分、识别，并引导客户使用Ⅱ类、Ⅲ类账户办理小额网络支付业务。	系统类	商业银行	1.查阅材料（内部审计报告、管理制度、系统文档等） 2.查看系统				
61		系统应按照《非银行支付机构网络支付管理办法》（中国人民银行公告〔2015〕第43号公布）要求，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。	系统类	非银行支付机构	1.查阅材料（自查报告、管理制度、系统文档等） 2.查看系统				
62		系统应采用哈希校验或数字签名等技术保证交易报文的完整性。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				

						检查结果			备注
						通过	不通过	不适用	
63	支付交易安全强度	系统应采用数字签名等技术确保交易报文的真实性、不可抵赖性。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				
64	互联网交易风险监控	系统应能够利用大数据分析、用户行为建模等技术，建立交易风险监控模型和机制。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、系统文档等） 2.查看系统				
65		系统应能够对交易过程进行监控，包括但不限于: 1.禁止在交易过程中拆分交易金额，变造商户名称、商户类别码、交易类型等要素。 2.通过限额、限次等风控规则，及时预警异常交易。 3.对异常交易采取风险提示、延迟结算等措施。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				
66		系统应对交易订单的唯一性进行检查，防止重复支付。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				
67		系统应采取防暴力破解、防撞库等登录控制措施，包括但不限于: 1.利用IP地址、终端设备标识、浏览器缓存等信息综合识别异常登录行为，如批量或高频登录。 2.使用图形验证码。 3.登录失败自动锁定。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				

序号	排查项	排查要点	类型	适用机构	检查方法				
68	互联网交易风险监控	系统应防范服务器端的拒绝服务或分布式拒绝服务（DoS/DDoS）攻击，包括但不限于以下措施： 1.进行流量监控和日志分析。 2.使用具有DoS/DDoS防护功能的网络设备。 3.防火墙只开启业务必需的端口，并开启DoS/DDoS防护功能。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				
三、伪卡欺诈风险管理									
69	金融IC卡降低磁条交易风险防控	新发行的金融IC卡应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。	系统类	商业银行	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				
70		系统应从交易渠道、刷卡频次、单笔交易金额、日累计交易金额、交易地区等方面，加强磁条交易风险控制。	系统类	商业银行	1.查阅材料（自查报告、系统文档等） 2.查看系统				
71		应制定切实的实施方案和保障措施，确保系统于2017年5月1日起关闭ATM终端、POS终端、自助终端等境内线下渠道复合卡的磁条交易。	系统类	商业银行	1.查阅材料（自查报告、系统文档等） 2.查看系统				
72		应通过短信、电话、客户端软件等方式对可疑交易进行确认和风险提示。	风控类	商业银行	查阅材料（自查报告）				
73		新发行的基于人民币结算账户的银行卡应符合《中国金融集成电路（IC）卡规范》（JR/T 0025）标准。	风控类	商业银行	查阅材料（自查报告、外部安全评估报告等）				
74	受理终端安全管理	ATM等自助终端应具备异常状态监测报警功能，当监测到终端设备存在异常时，及时报警并停止服务。	系统类	商业银行	1.查阅材料（自查报告、系统文档等） 2.查看系统				

						检查结果			备注
						通过	不通过	不适用	
75	受理终端安全管理	ATM等自助终端与服务器间应使用加密算法和安全协议，保护敏感数据的传输安全，防范中间人攻击。	系统类	商业银行	1.查阅材料（自查报告、系统文档等） 2.查看系统				
76		应对ATM等自助终端进行安全维护，包括但不限于: 1.及时升级版本和安装补丁，并采用数字签名等技术手段确保程序的完整性、可靠性。 2.遵循最小化安装原则，关闭不安全、不必要的服务和端口。 3.切换至维护模式时采取多因素身份验证机制。	系统类	商业银行	1.查阅材料（自查报告、管理制度、系统文档等） 2.查看系统				
77		ATM等自助终端应具有防病毒、防木马等安全防护机制，防范被植入恶意程序或恶意修改配置参数等风险，包括安装杀毒软件、设置程序白名单等。	系统类	商业银行	1.查阅材料（自查报告、管理制度、系统文档等） 2.查看系统				
78		终端入网管理系统应采取签名、唯一性标识等技术措施，对入网终端进行统一管理。	系统类	银行卡清算机构	1.查阅材料（自查报告、系统文档等） 2.查看系统				
79		POS终端应具备防拆开关、斑马条等软硬件电路防护机制，防止被非法改装。	系统类	商业银行 非银行支付机构	1.查阅材料（自查报告、外部安全评估报告、系统文档等） 2.查看系统				
80		布放的受理终端应具备技术标准符合性证明材料。	风控类	商业银行 非银行支付机构	查阅材料（自查报告、外部安全评估报告等）				

序号	排查项	排查要点	类型	被检机构	检查方法	检查结果			备注
81	受理终端安全管理	应定期对ATM等自助终端进行安全检查，保存记录，并及时修复检查发现的问题。检查内容包括但不限于： 1.按键区域、读卡器等组件是否被恶意改造。 2.是否采用物理保护手段，防止网线或网络接口裸露在外。 3.是否对通用串行总线（USB）接口、网络接口等采取限制使用措施。	风控类	商业银行	查阅材料（自查报告、记录文档等）				
82		应定期开展存量终端抽检，确保布放的终端与合格样品的一致性，并保存记录。	风控类	商业银行 非银行支付机构	查阅材料（自查报告、记录文档等）				
83		应具备受理终端安全管理制度，内容包括但不限于： 1.明确受理终端产品选型、验收、现场检查等环节的具体要求。 2.明确存量终端定期检查要求，严控非法改装终端的使用。	制度类	商业银行 非银行支付机构	查阅材料（自查报告、管理制度等）				
84		应具备受理终端入网管理制度，明确受理终端入网管理要求，严控不符合标准、非法改装的受理终端入网使用。	制度类	银行卡清算机构	查阅材料（自查报告、管理制度、记录文档等）				
85	特约商户实名制管理	应加强特约商户信息电子化管理，落实特约商户实名制相关规定，包括但不限于： 1.商业银行、非银行支付机构的系统应完整、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。 2.银行卡清算机构的系统应能够对同一特约商户在不同商业银行和非银行支付机构注册的信息进行关联管理。	系统类	商业银行 非银行支付机构 银行卡清算机构	1.查阅材料（自查报告、系统文档等） 2.查看系统				
86		应按照《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），落实特约商户实名制规定，对特约商户法人身份信息及商户营业执照进行核实，并保存记录。	风控类	商业银行 非银行支付机构	查阅材料（自查报告、管理制度、记录文档等）				

						排查结果			备注
						通过	不通过	不适用	
87	特约商户实名制管理	应充分利用影像采集、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，并保存记录。	风控类	商业银行 非银行支付机构	1.查阅材料（自查报告、记录文档等） 2.现场访谈				
88		应具备特约商户管理制度，明确特约商户实名制、资质审核和信息更新等相关要求。	制度类	商业银行 非银行支付机构 银行卡清算机构	查阅材料（自查报告、管理制度等）				
89	违规特约商户黑名单管理	应建立特约商户黑名单信息共享和查询机制，加强对已纳入黑名单的特约商户管理。	风控类	银行卡清算机构	查阅材料（自查报告）				
90		应具备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。	制度类	商业银行 非银行支付机构 银行卡清算机构	查阅材料（自查报告、管理制度等）				

四、排查确认单

机构类别	机构名称	机构法人所在地
被查机构人员签名：		日期：
排查组人员签名：		日期：

注：
1.“排查方法”列用于人民银行分支机构现场核实环节参考。
2.从业机构自查环节可在“备注”列填写自查记录，人民银行分支机构现场核实环节可在“备注”列填写核实记录。
3.“四、排查确认单”部分为人民银行分支机构现场核实环节填写的内容。
4.“排查要点”列中的“客户端软件”包括网上银行客户端软件、手机银行客户端软件、移动支付客户端软件、浏览器端安全控件等。

内部发送：科技司，条法司，支付司。

中国人民银行办公厅　　2016 年 9 月 19 日印发