



支付卡行业 (PCI)
数据安全标准
适用于商户的自我评估调查问卷 **B-IP**
和遵从性证明书

使用
**PTS 交互点 (POI) 终端的商户—
无电子持卡人数据存储**
适用于 **PCI DSS 3.2 版**

1.1 版
2017 年 1 月

文档变更记录

日期	PCI DSS 版本	SAQ 修订版	描述
N/A	1.0		未使用。
N/A	2.0		未使用。
2014 年 2 月	3.0		针对仅通过与支付处理商建立 IP 连接的独立 PTS 批准的交互点设备处理持卡人数据的商户适用要求的新 SAQ。 根据新的 PCI DSS 3.0 版要求与测试程序调整内容。
2015 年 4 月	3.1		更新以符合 PCI DSS 3.1 版。有关 PCI DSS 变更的详细信息，请参阅“ <i>PCI DSS – PCI DSS 3.0 版到 3.1 版的变更汇总</i> ”。
2015 年 7 月	3.1	1.1	更新以在 2015 年 6 月 30 日前将参考部分移至“最优方法”。
2016 年 4 月	3.2	1.0	更新以符合 PCI DSS 3.2 版。有关 PCI DSS 变更的详细信息，请参阅“ <i>PCI DSS – PCI DSS 3.1 版到 3.2 版的变更汇总</i> ”。 添加自 PCI DSS 3.2 版附录 A2 的要求。
2017 年 1 月	3.2	1.1	已更新文档变更来阐明 2016 年 4 月更新时添加的要求。 更新“开始之前”部分，以便阐明术语“SCR”以及获允系统的意图。 已添加要求 8.3.1，以便与要求 2.3 保持一致。 已添加要求 11.3.4，以便核实分段控制（若使用了分段）。

确认通知：

在所有使用目的和情况下，PCI SSC 网站上的英文文本应作为此文件的官方版本。当翻译文本和英文文本之间出现任何歧义和不一致之处时，正确的内容应以该位置的英文文本为准。

目录

文档变更记录	i
开始之前 iii	
PCI DSS 自我评估实施步骤	iii
了解自我评估调查问卷	iv
预期测试 iv	
完成自我评估调查问卷	v
某些特定要求的不适用性指南	v
法律规定的例外情况	v
第 1 节： 评估信息	1
第 2 节： 自我评估调查问卷 B-IP	4
构建和维护安全网络	4
要求 1: 安装和维护防火墙配置以保护数据	4
要求 2: 不要使用供应商提供的默认系统密码和其他安全参数	6
保护持卡人数据 8	
要求 3: 保护存储的持卡人数据	8
要求 4: 加密持卡人数据在开放式公共网络中的传输	10
维护漏洞管理计划 11	
要求 6: 开发并维护安全的系统和应用程序	11
实施强效访问控制措施	12
要求 7: 按业务知情需要限制对持卡人数据的访问	12
要求 8: 识别并验证对系统组件的访问	13
要求 9: 限制对持卡人数据的物理访问	14
定期监控并测试网络	17
要求 11: 定期测试安全系统和流程	17
维护信息安全政策 18	
要求 12: 维护针对所有工作人员的信息安全政策	18
附录 A: PCI DSS 附加要求	21
附录 A1: 针对共享托管服务提供商的 PCI DSS 附加要求	21
附录 A2: 针对使用 SSL/早期 TLS 的实体的 PCI DSS 附加要求	21
附录 A3: 指定实体补充认证 (DESV)	22
附录 B: 补偿性控制工作表	23
附录 C: 不适用性说明	24
第 3 节： 认证和证明书详情	25

开始之前

SAQ B-IP 已针对仅通过与支付处理商建立 IP 连接的独立 PTS 批准的交互点 (POI) 设备处理持卡人数据的商户适用要求进行完善。被归为安全读卡器 (SCR) 的 POI 设备有例外情况；使用 SCR 的商户符合使用此 SAQ 的资格。

SAQ B-IP 商户可能为实体 (实卡) 或邮件/电话订购 (无实卡) 的商户，并且不在任何计算机系统中存储持卡人数据。

对于此支付渠道，SAQ B-IP 商户确认：

- 您的企业仅使用与支付处理商建立 IP 连接的独立 PTS 批准的交互点 (POI) 设备 (SCR 除外) 获取客户的支付卡信息；
- 独立 IP 连接 POI 设备经 PCI SSC 网站列出的 PTS POI 计划认证 (SCR 除外)；
- 独立 IP 连接 POI 设备不连接环境中的任何其他系统 (这一点可通过网络分段讲 POI 设备与其他系统隔离来实现)¹；
- 持卡人数据仅可从 PTS 批准的 POI 设备传输至支付处理商；
- POI 设备不依靠任何其他设备 (例如计算机、手机、平板电脑等) 连接至支付处理商；
- 您的企业只会保留持卡人数据的纸质文件 (例如，打印的报告或收据)，且不通过电子方式接收此类文件；**并且**
- 您的企业不以电子格式存储持卡人数据。

此 SAQ 不适用于电子商务渠道。

此简要版 SAQ 包含了适用于特定类型的小商户环境的问题，如以上合格标准中所定义的。如果某些适用于您所在环境的 PCI DSS 要求未包含在本 SAQ 中，可能表示本 SAQ 不适用于您所在环境。此外，您必须遵从所有适用的 PCI DSS 要求以符合 PCI DSS 要求。

PCI DSS 自我评估实施步骤

1. 识别适用于您所在环境的 SAQ – 有关详情，请参见 PCI SSC 网站上的 *自我评估调查问卷说明和指南* 文档。
2. 确认您所在环境的范围适当且满足您所使用的 SAQ 的适用条件 (参见遵从性证明书的第 2g 部分)。
3. 评估您的环境是否达到相应的 PCI DSS 要求。
4. 实施此文档的所有章节：
 - 第 1 节 (AOC 的第 1、2 部分) – 评估信息和实施概要。
 - 第 2 节 – PCI DSS 自我评估调查问卷 (SAQ B-IP)

¹ 该条件不是为了禁止同一网络区域内存在不只一个获允的系统类型 (即 IP 连接 POI 设备)，只要获允的系统独立于其他系统类型即可 (例如通过使用网络分段)。此外，该条件不是为了防止已定义的系统类型能够将交易信息传送到第三方 (如收单机构或支付处理商) 供其通过网络进行处理。

- 第 3 节 (AOC 的第 3、4 部分) – 认证和证明书详情以及针对未遵从要求的行动计划 (如果适用)

5. 向收单机构、支付品牌或其他申请机构提交 SAQ、遵从性证明书 (AOC) 以及其他任何要求的文档 (例如 ASV 扫描报告)。

了解自我评估调查问卷

此自我评估调查问卷中“PCI DSS 问题”列所包含的问题基于 PCI DSS 中的要求。

为帮助完成评估流程, 已提供了就 PCI DSS 要求和如何完成自我评估调查问卷予以指导的其他资源。下面概述了其中的一些资源:

文档	内容:
PCI DSS <i>(PCI 数据安全标准要求和安全评估程序)</i>	<ul style="list-style-type: none"> • 有关范围界定的指导 • 有关所有 PCI DSS 要求意图的指导 • 测试程序详情 • 有关补偿性控制的指导
SAQ 说明和指南文档	<ul style="list-style-type: none"> • 所有 SAQ 及其适用标准的相关信息 • 如何确定哪项 SAQ 适用于您所在组织
<i>PCI DSS 和 PA-DSS 术语、缩略词和首字母缩略词词汇表</i>	<ul style="list-style-type: none"> • PCI DSS 和自我评估调查问卷中所使用的术语的说明和定义

上述资源和一些其他资源可在 PCI SSC 网站 (www.pcisecuritystandards.org) 上找到。建议组织在开始评估之前先浏览 PCI DSS 和其他支持文档。

预期测试

“预期测试”列中包含的说明基于 PCI DSS 中的测试程序, 提供了有关认证已满足要求所必须执行的测试活动类型的高级说明。有关针对各项要求的测试程序的完整详情, 请参见 PCI DSS。

完成自我评估调查问卷

对于每个问题，可以选择一个回复选项来表明您所在公司针对该要求的状态。**对于每个问题，只能选择一个回复。**

下表说明了各项回复的含义：

回复	此回复的适用情况：
是	已执行预期测试，且已按照相关说明满足该要求的所有元素。
是，已填写 CCW (补偿性控制工作表)	已执行预期测试，且已采用补偿性控制满足该要求。 如果选择此列中的回复，则必须在 SAQ 附录 B 中填写补偿性控制工作表 (CCW)。 要了解如何使用补偿性控制和填写该工作表，请参见 PCI DSS。
否	该要求的部分或所有元素尚未满足或正处于实施状态，或者需要进一步测试才能确定是否满足。
N/A (不适用)	该要求不适用于相关组织所在环境。(有关示例，参见下面的 <i>某些特定要求的不适用性指南</i> 。) 如果选择此列中的回复，则必须在 SAQ 附录 C 中提供支持说明。

某些特定要求的不适用性指南

由于许多完成 SAQ B-IP 的组织需要认证其对于每项 PCI DSS 要求的遵从性，因此一些具有特定业务模式的组织可能会发现某些要求不适用。举例来说，如果一家公司在任何方面都不使用无线技术，则无需认证对于特定于管理无线技术的 PCI DSS 章节的遵从性（例如，要求 1.2.3、2.1.1 和 4.1.1）。

如果您认为任何要求不适用于您所在环境，请针对该特定要求选择“N/A”选项，然后在附录 C 为所有“N/A”条目填写“不适用性说明”。

法律规定的例外情况

如果您所在组织因受到相关法律限制约束而无法满足 PCI DSS 要求，请针对该要求选择“否”列，然后在第 3 部分填写相关证明书。

第 1 节： 评估信息

提交说明

商户必须填写此文档，以声明其按照支付卡行业数据安全标准要求和安全评估程序 (PCI DSS) 所做的自我评估的结果。填写所有章节：商户应负责确保相关方（如果有）填写所有章节。联系收单机构（商户银行）或支付品牌以确定报告和提交程序。

第 1 部分 商户和合格安全性评估商信息

第 1a 部分 商户组织信息

公司名称：		DBA（经营 别称）：	
联系人姓名：		职务：	
电话：		电子邮件地 址：	
公司地址：		城市：	
州/省：		国家/地 区：	邮编：
网址：			

第 1b 部分 合格安全性评估商公司信息（如果有）

公司名称：			
QSA 主要联系人姓名：		职务：	
电话：		电子邮件地 址：	
公司地址：		城市：	
州/省：		国家/地 区：	邮编：
网址：			

第 2 部分 实施概要

第 2a 部分 商户业务类型（选中所有合适选项）

- 零售商 通信 百货和超市
 石油 电子商务 邮件/电话订购 (MOTO)
 其他（请指明）：

您所在企业提供哪些类型的支付渠道？

- 邮件/电话订购 (MOTO)
 电子商务
 实卡交易（面对面）

此 SAQ 覆盖哪些支付渠道？

- 邮件/电话订购 (MOTO)
 电子商务
 实卡交易（面对面）

注：如果您所在组织的支付渠道或流程未涵盖在此 SAQ 范围内，请咨询您的收单机构或支付品牌了解如何验证其他渠道。

第 2b 部分 支付卡业务说明

您所在企业如何存储、处理和/或传输持卡人数据，以及支持的容量是多少？

第 2c 部分 地点

列出 PCI DSS 审核中包含的场所类型（例如，零售店、公司办公室、数据中心、呼叫中心等等）以及所在地点概要。

场所类型	此类场所数量	场所所在地点（例如，城市、国家/地区）
示例：零售店	3	美国马萨诸塞州波士顿

第 2d 部分 支付应用程序

该组织是否使用一款或多款支付应用程序？ 是 否

提供有关您所在组织使用的支付应用程序的下列信息：

支付应用程序名称	版本号	应用程序供应商	该应用程序是否获得 PA-DSS 认证？	PA-DSS 认证失效日期（如果有）
			<input type="checkbox"/> 是 <input type="checkbox"/> 否	
			<input type="checkbox"/> 是 <input type="checkbox"/> 否	
			<input type="checkbox"/> 是 <input type="checkbox"/> 否	
			<input type="checkbox"/> 是 <input type="checkbox"/> 否	
			<input type="checkbox"/> 是 <input type="checkbox"/> 否	

第 2e 部分 环境说明

提供有关此评估所涵盖的环境的**高级**说明。

例如：

- 对持卡人数据环境 (CDE) 的输入和输出连接。
- 该 CDE 中的关键系统组件（例如 POS 设备、数据库、网络服务器等）以及其他任何必要的支付组件（如果有）。

您所在企业是否使用网络分段来影响 PCI DSS 环境范围？
（有关网络分段的指南，请参见 PCI DSS 的“网络分段”章节）

是 否

第 2f 部分 第三方服务提供商

您的公司是否使用合格集成商和经销商 (QIR)?

是 否

如果是的话:

QIR 公司名称:

QIR 个人名称:

QIR 所提供服务的说明:

您所在公司是否与任何第三方服务提供商 (例如, 合格集成商和经销商 (QIR)、网关、支付处理商、支付服务提供商 (PSP)、网络托管公司、航班订票代理商、忠诚计划代理商等) 共享持卡人数据?

是 否

如果是的话:

服务提供商名称:

所提供服务的说明:

服务提供商名称:	所提供服务的说明:

注: 要求 12.8 适用于上述列表中的所有条目。

第 2g 部分 完成 SAQ B-IP 的适用性

商户证明符合填写本简要版自我评估调查问卷的适用条件, 因为对于此支付渠道:

<input type="checkbox"/>	商户仅使用与支付处理商建立 IP 连接的独立 PTS 批准的交互点 (POI) 设备 (SCR 除外) 获取客户的支付卡信息;
<input type="checkbox"/>	独立 IP 连接 POI 设备经 PCI SSC 网站列出的 PTS POI 计划认证 (SCR 除外);
<input type="checkbox"/>	独立 IP 连接 POI 设备不连接商户环境中的任何其他系统 (这一点可通过网络分段讲 POI 设备与其他系统隔离来实现);
<input type="checkbox"/>	持卡人数据仅可从 PTS 批准的 POI 设备传输至支付处理商;
<input type="checkbox"/>	POI 设备不依靠任何其他设备 (例如计算机、手机、平板电脑等) 连接至支付处理商;
<input type="checkbox"/>	商户不以电子格式存储持卡人数据; 并且
<input type="checkbox"/>	如果商户存储持卡人数据, 仅可以纸质报告或纸质收据副本的形式存储此类数据, 并不以电子方式接收数据。

第 2 节： 自我评估调查问卷 B-IP

注：以下问题的编号与 PCI DSS 要求和安全评估程序文档中说明的 PCI DSS 要求和测试程序顺序相符。

自我评估实施日期：

构建和维护安全网络

要求 1： 安装和维护防火墙配置以保护数据

PCI DSS 问题	预期测试	回复 (为每个问题选中一个回复)			
		是	是, 已填写 CCW	否	N/A
1.1.2	(a) 是否已存在当前网络图且该图记录了持卡人数据环境与包括任何无线网络在内的其他网络之间的所有连接?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) 是否有相应流程以确保该图及时更新?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.1.4	(a) 各互联网连接以及任何非军事区 (DMZ) 和内部网络区域间是否要求和实施了防火墙?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) 当前网络图是否与防火墙配置标准相符?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.1.6	(a) 防火墙和路由器配置标准是否包含服务、协议和端口的文档记录列表 (包括各自的业务理由和审批)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) 是否已识别出所有不安全的服务、协议和端口且已针对识别出的所有服务记录和实施了安全功能?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.2	防火墙和路由器配置是否按照下述要求限制了不可信网络和持卡人数据环境中任何系统间的连接: 注: “不可信网络”指受审核实体所属网络之外的任何网络, 和/或不受该实体控制或管理的任何网络。				

PCI DSS 问题		预期测试	回复 (为每个问题选中一个回复)			
			是	是, 已填写 CCW	否	N/A
1.2.1	(a) 输入和输出流量是否限制在持卡人数据环境所需的范围?	<ul style="list-style-type: none"> 审核防火墙和路由器配置标准 检查防火墙和路由器配置 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) 是否明确拒绝 (例如, 使用明确的“拒绝所有”或在允许声明后含蓄地表达拒绝之意) 其他所有输入和输出流量?	<ul style="list-style-type: none"> 审核防火墙和路由器配置标准 检查防火墙和路由器配置 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.2.3	是否在所有无线网络和持卡人数据环境间安装了外围防火墙, 并将这些防火墙配置为拒绝流量或 (如果出于业务目的而需要流量) 仅允许无线环境和持卡人数据环境间的授权流量?	<ul style="list-style-type: none"> 审核防火墙和路由器配置标准 检查防火墙和路由器配置 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.3	是否按照下述要求禁止了互联网与持卡人数据环境中任何系统组件之间的直接公共访问:					
1.3.3	是否实施了反欺骗措施以检测并阻止伪造的源 IP 地址进入该网络? (例如, 阻止具有内部地址的互联网流量)	<ul style="list-style-type: none"> 检查防火墙和路由器配置 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.3.4	从持卡人数据环境输出到互联网的流量是否具有明确授权?	<ul style="list-style-type: none"> 检查防火墙和路由器配置 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.3.5	是否仅允许已建立的连接进入该网络?	<ul style="list-style-type: none"> 检查防火墙和路由器配置 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

要求 2: 不要使用供应商提供的默认系统密码和其他安全参数

PCI DSS 问题	预期测试	回复 (为每个问题选中一个回复)				
		是	是, 已填写 CCW	否	N/A	
2.1	(a) 是否始终在该网络中安装系统之前更改供应商提供的默认值? <i>此要求适用于所有默认密码, 包括但不限于操作系统、提供安全服务的软件、应用程序和系统帐户、销售点 (POS) 终端、支付应用程序、简单网络管理协议 (SNMP) 社区字符串等使用的默认密码。</i>	<ul style="list-style-type: none"> 审核相关政策和程序 检查供应商文档 查看系统配置和帐户设置 与工作人员面谈 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) 是否已于在该网络中安装系统之前删除或禁用不必要的默认帐户?	<ul style="list-style-type: none"> 审核相关政策和程序 审核供应商文档 检查系统配置和帐户设置 与工作人员面谈 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1	对于连接到持卡人数据环境或传输持卡人数据的无线环境, 是否按照下述要求在安装时更改了所有无线供应商提供的默认值:					
	(a) 是否在安装以及知道密钥的任何人离职或更换岗位时更改了默认的加密密钥?	<ul style="list-style-type: none"> 审核相关政策和程序 审核供应商文档 与工作人员面谈 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) 是否在安装时更改了无线设备上的默认 SNMP 社区字符串?	<ul style="list-style-type: none"> 审核相关政策和程序 审核供应商文档 与工作人员面谈 检查系统配置 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) 是否在安装时更改了接入点的默认密码/口令?	<ul style="list-style-type: none"> 审核相关政策和程序 与工作人员面谈 检查系统配置 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS 问题	预期测试	回复 (为每个问题选中一个回复)			
		是	是, 已填写 CCW	否	N/A
(d) 是否已更新无线设备的固件来支持通过无线网络进行的验证和传输的强效加密?	<ul style="list-style-type: none"> ▪ 审核相关政策和程序 ▪ 审核供应商文档 ▪ 检查系统配置 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(e) 是否已更改其他与安全有关的无线供应商默认值 (如果适用)?	<ul style="list-style-type: none"> ▪ 审核相关政策和程序 ▪ 审核供应商文档 ▪ 检查系统配置 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.3 是否按照下述要求对非控制台管理访问 (包括基于 Web 的访问) 进行了加密: 注: 若要使用 SSL/早期 TLS, 须完成附录 A2 中的要求。					
(a) 是否已对所有非控制台管理访问应用强效加密法, 且在要求提供管理员密码前已调用强效加密法?	<ul style="list-style-type: none"> ▪ 检查系统组件 ▪ 检查系统配置 ▪ 查看管理员登录 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) 系统服务和参数文件是否已配置为阻止使用 Telnet 和其他不安全的远程登录命令?	<ul style="list-style-type: none"> ▪ 检查系统组件 ▪ 检查服务和文件 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) 是否已采用强效加密法对管理员进入基于 web 的管理界面的访问权进行加密?	<ul style="list-style-type: none"> ▪ 检查系统组件 ▪ 查看管理员登录 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(d) 是否已按照行业最优方法和/或供应商建议对所使用的技术实施强效加密?	<ul style="list-style-type: none"> ▪ 检查系统组件 ▪ 审核供应商文档 ▪ 与工作人员面谈 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

保护持卡人数据

要求 3: 保护存储的持卡人数据

PCI DSS 问题	预期测试	回复 (为每个问题选中一个回复)				
		是	是, 已填写 CCW	否	N/A	
3.2	(c) 完成授权流程后, 是否删除了敏感验证数据或使其不可恢复?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	<ul style="list-style-type: none"> 审核相关政策 and 程序 检查系统配置 检查删除流程 					
	(d) 是否所有系统均已遵循以下有关授权后不存储敏感验证数据 (即使已经加密) 的要求:					
3.2.1	授权后不存储任意磁道上的完整内容 (位于卡背面的磁条中、芯片上或其他位置)。 此类据也可称为全磁道、磁道、磁道 1、磁道 2 和磁条数据。 注: 在正常业务过程中, 以下磁条数据元素可能需要保留: <ul style="list-style-type: none"> 持卡人姓名, 主帐户 (PAN), 失效日, 以及 业务码 为将风险降至最低, 只存储业务所需的数据元素。	<ul style="list-style-type: none"> 检查数据来源, 其中包括: <ul style="list-style-type: none"> 输入的交易数据 所有日志 存档文件 跟踪文件 数据库架构 数据库内容 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS 问题	预期测试	回复 (为每个问题选中一个回复)			
		是	是, 已填写 CCW	否	N/A
3.2.2 授权后不存储卡验证代码或值 (印在支付卡正面或背面的三位或四位数值) ?	<ul style="list-style-type: none"> ▪ 检查数据来源, 其中包括: <ul style="list-style-type: none"> • 输入的交易数据 • 所有日志 • 存档文件 • 跟踪文件 • 数据库架构 • 数据库内容 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3 授权后不存储个人识别码 (PIN) 或经加密的 PIN 数据块?	<ul style="list-style-type: none"> ▪ 检查数据来源, 其中包括: <ul style="list-style-type: none"> • 输入的交易数据 • 所有日志 • 存档文件 • 跟踪文件 • 数据库架构 • 数据库内容 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.3 PAN 是否在显示时被掩盖 (只有前六位和后四位数字可以显示), 以便仅有正当业务需要者才能看到除前六位/后四位以外的 PAN? 注: 该要求不能取代现行更严格的有关持卡人数据显示的要求, 例如法律或支付卡品牌对销售点 (POS) 收据的要求。	<ul style="list-style-type: none"> ▪ 审核相关政策和程序 ▪ 审核需要能够查看完整 PAN 的角色 ▪ 检查系统配置 ▪ 查看 PAN 的显示 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

要求 4: 加密持卡人数据在开放式公共网络中的传输

PCI DSS 问题	预期测试	回复 (为每个问题选中一个回复)			
		是	是, 已填写 CCW	否	N/A
<p>4.1 (a) 是否使用了强效加密法和安全协议来保护经由公开、公共网络传输的敏感持卡人信息。</p> <p><i>注: 若要使用 SSL/早期 TLS, 须完成附录 A2 中的要求。</i></p> <p><i>在 PCI DSS 的范围内, 公开、公共的网络包括但不限于, 互联网、无线技术 (包括 802.11 和蓝牙)、蜂窝技术 (例如, 全球移动通信系统 (GSM)、码分多址 (CDMA)) 以及通用分组无线业务 (GPRS)。</i></p>	<ul style="list-style-type: none"> 审核书面标准 审核相关政策和程序 审核传输或接收 CHD 的所有地点 检查系统配置 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>(b) 是否只接受可信密钥和/或证书?</p>	<ul style="list-style-type: none"> 查看输入和输出传输 检查密钥和证书 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>(c) 实施的安全协议是否仅使用安全配置且不支持非安全版本或配置?</p>	<ul style="list-style-type: none"> 检查系统配置 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>(d) 是否已根据所使用的加密方法实施了适当的加密强度 (查看供应商建议/最优方法)?</p>	<ul style="list-style-type: none"> 审核供应商文档 检查系统配置 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>(e) 对于 TLS 的实施, 是否在传输或接收持卡人数据时始终启用了 TLS?</p> <p><i>例如, 对于基于浏览器的实施:</i></p> <ul style="list-style-type: none"> “HTTPS”作为浏览器统一记录定位器 (URL) 协议, 且 仅当“HTTPS”作为 URL 的一部分时才需要持卡人数据。 	<ul style="list-style-type: none"> 检查系统配置 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>4.1.1 传输持卡人数据或连接到持卡人数据环境的无线网络是否使用了行业最优方法来对验证和传输实施强效加密?</p>	<ul style="list-style-type: none"> 审核书面标准 审核无线网络 检查系统配置设置 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>4.2 (b) 是否已制定政策来规定不会通过终端用户通讯技术传送不受保护的 PAN?</p>	<ul style="list-style-type: none"> 审核相关政策和程序 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

维护漏洞管理计划

要求 6: 开发并维护安全的系统和应用程序

PCI DSS 问题	预期测试	回复 (为每个问题选中一个回复)			
		是	是, 已填写 CCW	否	N/A
<p>6.1 是否制定了包括以下方面的安全漏洞识别流程:</p> <ul style="list-style-type: none"> 使用可信外源获取安全漏洞信息? 为安全漏洞指定风险等级, 包括对所有“高”风险和“重要”漏洞的识别? <p>注: 风险等级应以行业最优方法和潜在影响考虑为依据。例如, 漏洞分级标准可能包括对 CVSS 基础得分的考虑和/或供应商的分类, 及/或相关系统的类型。</p> <p>根据组织的环境和风险评估策略不同, 评估漏洞和指定风险等级的方法也不尽相同。风险等级至少应标识出所有被视为对环境具有“高风险”的漏洞。除风险等级外, 如果安全漏洞即将对环境造成威胁、影响关键系统且/或不解决可能会造成潜在危害, 则可被视为“重要”。关键系统可能包括安全系统、面向公众的设备和系统、数据库以及其他存储、处理或传输持卡人数据的系统。</p>	<ul style="list-style-type: none"> 审核相关政策和程序 与工作人员面谈 查看流程 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>6.2 (a) 是否已安装供应商提供的适用安全补丁, 以确保所有系统组件和软件均杜绝已知漏洞?</p>	<ul style="list-style-type: none"> 审核相关政策和程序 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>(b) 是否在发布后一个月内安装了关键的安全补丁?</p> <p>注: 应按照要求 6.1 中规定的风险分级流程标识关键安全补丁。</p>	<ul style="list-style-type: none"> 审核相关政策和程序 检查系统组件 对比安装的安全补丁列表和最新的供应商补丁列表是否相符 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

实施强效访问控制措施

要求 7: 按业务知情需要限制对持卡人数据的访问

PCI DSS 问题		预期测试	回复 (为每个问题选中一个回复)			
			是	是, 已填写 CCW	否	N/A
7.1	是否如下所述只有具有相应工作需要的个人才能访问系统组件和持卡人数据:					
7.1.2	是否按照下述要求对特权用户 ID 的访问权限进行了限制: <ul style="list-style-type: none"> ▪ 限制为执行工作所需的最小权限? ▪ 只分配给明确需要此类特权访问的角色? 	<ul style="list-style-type: none"> ▪ 检查书面访问控制政策 ▪ 与工作人员面谈 ▪ 与管理人员面谈 ▪ 审核特权用户 ID 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.1.3	是否基于个人的工作分类和职能分配了访问权限?	<ul style="list-style-type: none"> ▪ 检查书面访问控制政策 ▪ 与管理人员面谈 ▪ 审核用户 ID 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

要求 8: 识别并验证对系统组件的访问

PCI DSS 问题	预期测试	回复 (为每个问题选中一个回复)			
		是	是, 已填写 CCW	否	N/A
8.1.5	(a) 是否仅在需要的时间段启用并在不用时禁用第三方用于通过远程访问来访问、支持或维护系统组件的帐户?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) 是否对处于使用中的第三方远程访问帐户进行了监控?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.3	是否使用如下所述的多因素验证保护对 CDE 的所有单独非控制台管理访问和所有远程访问: <i>注: 多因素验证要求在验证过程中至少使用三种验证方法中的其中两种 (有关验证方法的说明, 请参见 PCI DSS 要求 8.2)。使用一个因素两次 (例如, 使用两个不同的密码) 不视为多因素验证。</i>				
8.3.1	是否针对所有非控制台访问在针对具有管理访问权限的工作人员的 CDE 中加入了多因素验证? <i>注: 本要求在 2018 年 1 月 31 日前属于最优方法, 此后将成为一项要求。</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.3.2	是否针对来自该实体网络外部的所有远程网络访问 (针对用户和管理员, 并包括出于支持和维护目的的第三方访问) 加入了多因素验证?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.5	是否按照下述要求禁用了群组、共享或常规帐户、密码或其他验证方法: <ul style="list-style-type: none"> ▪ 禁用或删除了常规用户 ID; ▪ 用于系统管理活动和其他重要功能的共享用户 ID 不存在; 以及 ▪ 不使用共享和常规用户 ID 管理任何系统组件 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

要求 9: 限制对持卡人数据的物理访问

PCI DSS 问题	预期测试	回复 (为每个问题选中一个回复)			
		是	是, 已填写 CCW	否	N/A
<p>9.1.2 是否已实施物理和/或逻辑控制, 以限制对公共网络插座交换机的访问?</p> <p><i>例如, 位于公共区域和访客可进入区域的网络插座交换机可能被禁用, 并且仅在明确授权进行网络访问时才能启用。或者, 也可以实施相应流程, 以确保访客处在网络插座交换机正在运行的区域时始终有人陪同。</i></p>	<ul style="list-style-type: none"> 审核相关政策和程序 与工作人员面谈 查看位置 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>9.5 是否已采取措施来保护所有媒介实体安全 (包括但不限于计算机、可移动电子媒介、纸质收据、纸质报告和传真)?</p> <p><i>在要求 9 中, “媒介”指所有包含持卡人数据的纸质和电子媒介。</i></p>	<ul style="list-style-type: none"> 审核用于保护媒介实体安全的政策和程序 与工作人员面谈 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>9.6 (a) 是否严格控制任何媒介的内部或外部分发?</p>	<ul style="list-style-type: none"> 审核针对媒介分发的政策和程序 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>(b) 相关控制是否包含以下方面:</p>					
<p>9.6.1 是否已对媒介进行分类以便确定数据的敏感性?</p>	<ul style="list-style-type: none"> 审核针对媒介分类的政策和程序 与安全人员面谈 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>9.6.2 媒介是否通过可靠的快递公司或可准确跟踪的其他投递方法发出?</p>	<ul style="list-style-type: none"> 与工作人员面谈 检查媒介分发跟踪日志和文档 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>9.6.3 转移媒介时 (尤其是将媒介分发给个人时) 是否经过管理层的批准?</p>	<ul style="list-style-type: none"> 与工作人员面谈 检查媒介分发跟踪日志和文档 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>9.7 是否严格控制对媒介的存储和获取?</p>	<ul style="list-style-type: none"> 审核相关政策和程序 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS 问题		预期测试	回复 (为每个问题选中一个回复)			
			是	是, 已填写 CCW	否	N/A
9.8	(a) 是否销毁了因业务或法律原因而不再需要的所有媒介?	<ul style="list-style-type: none"> 审核媒介定期销毁政策和程序 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) 是否按照下述要求销毁媒介:					
9.8.1	(a) 硬拷贝材料是否已被粉碎、焚烧或打浆以确保无法重建持卡人数据?	<ul style="list-style-type: none"> 审核媒介定期销毁政策和程序 与工作人员面谈 查看流程 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) 是否已确保待销毁材料所用存储容器的安全性以免他人访问相关内容?	<ul style="list-style-type: none"> 检查存储容器的安全性 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.9	是否已按照下述要求保护通过直接接触卡本身便可捕获支付卡数据的设备以免其被篡改和替换? <i>注: 此要求适用于销售点实卡交易 (即刷卡) 中使用的读卡设备。本要求不适用于手动密钥输入组件, 如计算机键盘和 POS 机键盘。</i>					
	(a) 相关政策和程序是否要求维护此类设备列表?	<ul style="list-style-type: none"> 审核相关政策和程序 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) 相关政策和程序是否要求定期检查设备以查找篡改或替换迹象?	<ul style="list-style-type: none"> 审核相关政策和程序 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) 相关政策和程序是否要求培训工作人员, 以确保其了解可疑行为和举报篡改或替换设备行为?	<ul style="list-style-type: none"> 审核相关政策和程序 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.9.1	(a) 设备列表是否包含以下方面? <ul style="list-style-type: none"> 设备的外形、型号 设备位置 (例如安放设备的现场或设施的地址) 设备的序列号或其他独特验证方法 	<ul style="list-style-type: none"> 检查设备列表 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) 该列表是否准确且已及时更新?	<ul style="list-style-type: none"> 查看设备及设备位置, 并与该列表进行对比 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS 问题		预期测试	回复 (为每个问题选中一个回复)			
			是	是, 已填写 CCW	否	N/A
	(c) 设备列表是否随着设备的新增、更换位置、停用等进行更新?	<ul style="list-style-type: none"> 与工作人员面谈 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.9.2	(a) 是否按照下述要求定期检查设备表面, 以查找篡改 (例如为设备增加读卡器) 或替换 (例如通过检查序列号或其他设备特征确认其未被欺诈性设备调换) 迹象? <i>注: 设备可能被篡改或替换的迹象包括: 不明附件或有缆连接到设备, 安全标签丢失或改变, 外壳破损或颜色不同, 序列号或其他外部标记改变。</i>	<ul style="list-style-type: none"> 与工作人员面谈 查看检查流程并与规定的流程进行对比 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) 工作人员是否了解设备的检查程序?	<ul style="list-style-type: none"> 与工作人员面谈 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.9.3	是否已按照下述要求培训工作人员, 使其了解尝试篡改或替换设备的行为?					
	(a) 针对销售点所在地工作人员的培训材料是否包含以下方面? <ul style="list-style-type: none"> 在允许对设备进行调整或修理之前, 验证任何自称修理或维护人员的第三方人员的身份。 在未经验证的情况下, 不要安装、替换或退还设备。 注意设备周围的可疑行为 (例如, 陌生人尝试拔掉设备插头或打开设备)。 向相关人员 (例如, 经理或安全人员) 报告篡改或替换设备的可疑行为和迹象。 	<ul style="list-style-type: none"> 审核培训材料 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) 是否已培训销售点所在地的工作人员, 使其了解用于检测和报告尝试篡改或替换设备行为的程序?	<ul style="list-style-type: none"> 与 POS 所在地的工作人员面谈 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

定期监控并测试网络

要求 11: 定期测试安全系统和流程

PCI DSS 问题	预期测试	回复 (为每个问题选中一个回复)			
		是	是, 已填写 CCW	否	N/A
11.2.2 (a) 是否每个季度运行了一次外部漏洞扫描? <i>注: 季度外部漏洞扫描必须由支付卡行业安全标准委员会 (PCI SSC) 认证的授权扫描服务商 (ASV) 执行。如需了解扫描客户的责任、扫描准备等, 请参阅 PCI SSC 网站上发布的《ASV 计划指南》。</i>	<ul style="list-style-type: none"> 审核最近四个季度的外部漏洞扫描结果 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) 每个季度的外部扫描和重复扫描结果是否符合 ASV 计划指南对扫描通过的要求 (例如不存在 CVSS 评级为 4.0 或以上的漏洞或无自动故障)?	<ul style="list-style-type: none"> 审核每个季度的外部扫描和重复扫描结果 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) 季度外部漏洞扫描是否由 PCI SSC 认证的授权扫描服务商 (ASV) 执行?	<ul style="list-style-type: none"> 审核每个季度的外部扫描和重复扫描结果 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.3.4 如果利用网络分段将 CDE 与其他网络隔离:					
(a) 是否已规定用于测试所有分段方法的穿透测试程序以确认其行之有效, 并将所有范围外系统与 CDE 内的系统隔离?	<ul style="list-style-type: none"> 检查分段控制 审核穿透测试法 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) 用于验证分段控制的穿透测试是否满足下述要求? <ul style="list-style-type: none"> 至少每年执行一次, 且在分段控制/方法发生任何变更后也执行 覆盖使用中的所有分段控制/方法 确认分段方法行之有效并隔离所有范围外系统与 CDE 内的系统。 	<ul style="list-style-type: none"> 检查最近一次穿透测试的结果 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) 测试是否由合格的内部人员或合格的外部第三方执行, 且 (如果适用) 确保测试者的组织独立性 (不要求是 QSA 或 ASV)?	<ul style="list-style-type: none"> 与负责人面谈 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

维护信息安全政策

要求 12: 维护针对所有工作人员的信息安全政策

注: 在要求 12 中, “工作人员”指“常驻”实体经营场所或能够以其他方式访问该公司的持卡人数据环境现场的全职和兼职员工、临时工和工作人员、承包商和顾问。

PCI DSS 问题	预期测试	回复 (为每个问题选中一个回复)			
		是	是, 已填写 CCW	否	N/A
12.1	是否已建立、公布、维护并向所有相关人员宣传安全政策?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.1.1	是否至少每年审核一次安全政策, 并在环境发生变更时进行更新?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3	是否已制定关键技术的使用政策, 以规定这些技术的正确用法并包含以下方面: 注: 关键技术包括但不限于, 远程访问和无线技术、笔记本电脑、平板电脑、可移动电子媒介以及电子邮件和互联网的使用。				
12.3.1	被授权方明确允许使用这些技术?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.3	一份列出所有此类设备和具有访问权的工作人员的列表?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.5	可接受的技术使用方式?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.9	仅在供应商和业务合作伙伴需要时为其激活远程访问技术, 并在使用后应立即停用?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS 问题		预期测试	回复 (为每个问题选中一个回复)			
			是	是, 已填写 CCW	否	N/A
12.4	安全政策和程序是否明确规定所有工作人员的信息安全责任?	<ul style="list-style-type: none"> 审核信息安全政策和程序 抽样选取部分负责人员进行面谈 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.5	(b) 是否已将下列信息安全管理职责正式分配给个人或团队:					
12.5.3	建立、记录并分发安全事故响应和逐级上报程序, 以确保及时有效地处理所有情况?	<ul style="list-style-type: none"> 审核信息安全政策和程序 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.6	(a) 是否已实施正式的安全意识计划, 以使所有工作人员了解持卡人数据安全政策和程序?	<ul style="list-style-type: none"> 审核安全意识计划 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8	是否已按照下述要求实施并维护政策和程序以管理共享持卡人数据或可能影响持卡人数据安全的服务提供商:					
12.8.1	已维护服务提供商列表 (包括所提供服务的说明)?	<ul style="list-style-type: none"> 审核相关政策和程序 查看流程 审核服务提供商名单 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.2	是否维护书面协议, 其中确认服务提供商负责其处理或者代表客户以其他方式存储、处理或传输的持卡人数据的安全性以及他们可能会影响客户持卡人数据环境的安全性? <i>注: “确认”的确切措辞取决于双方协议、所提供服务的详情以及分配给每一方的责任。“确认”不一定要包含与本要求完全相同的措辞。</i>	<ul style="list-style-type: none"> 查看书面协议 审核相关政策和程序 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.3	是否已建立雇用服务提供商的流程 (包括雇用前的相应尽职调查)?	<ul style="list-style-type: none"> 查看流程 审核政策、程序和支持文档 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.4	是否已维护相应计划来至少每年监控一次服务提供商的 PCI DSS 遵从性状态?	<ul style="list-style-type: none"> 查看流程 审核政策、程序和支持文档 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.5	是否已维护有关分别由各服务提供商和实体管理的 PCI DSS 要求的信息?	<ul style="list-style-type: none"> 查看流程 审核政策、程序和支持文档 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS 问题		预期测试	回复 (为每个问题选中一个回复)			
			是	是, 已填写 CCW	否	N/A
12.10.1	(a) 是否已建立在出现系统漏洞时实施的事故响应计划?	<ul style="list-style-type: none"> ▪ 审核事故响应计划 ▪ 审核事故响应计划程序 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

附录 A: PCI DSS 附加要求

附录 A1: 针对共享托管服务提供商的 PCI DSS 附加要求

此附录不用于商户评估。

附录 A2: 针对使用 SSL/早期 TLS 的实体的 PCI DSS 附加要求

PCI DSS 问题	预期测试	回复 (为每个问题选中一个回复)			
		是	是, 已填写 CCW	否	N/A
<p>A2.1 针对使用 SSL 和/或早期 TLS 的 POS POI 终端 (及其连接到的 SSL/TLS 终端点):</p> <ul style="list-style-type: none"> 是否已证实这些设备不易受到任何已知 SSL/早期 TLS 漏洞的影响 或者: 是否根据要求 A2.2 制定了适当的正式风险降低和迁移计划? 	<ul style="list-style-type: none"> 查看证明 POS PIO 设备不受任何已知 SSL/早期 TLS 使用影响的文档 (例如供应商文档、系统/网络设置详情等) 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>A2.2 是否针对使用 SSL 和/或早期 TLS 的所有实施 (A2.1 中允许的除外) 制定了适当的正式风险降低和迁移计划, 包括:</p> <ul style="list-style-type: none"> 使用说明, 包括传输的数据、使用和/或支持 SSL/早期 TLS 的系统的类型和数量、环境类型; 风险评估结果和适当的风险降低控制; 对用于监控 SSL/早期 TLS 相关漏洞的流程的说明; 对实施以确保 SSL/早期 TLS 未实施到新环境的变更控制流程的说明; 迁移项目计划概述, 包括目标迁移完成时间不迟于 2018 年 6 月 30 日? 	<ul style="list-style-type: none"> 查看记录的风险降低和迁移计划 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

附录 A3: 指定实体补充认证 (DESV)

此附录仅适用于支付品牌或收单机构要求对现有 PCI DSS 要求进行补充认证时指定的实体。要求验证此附录的实体应使用 DESV 补充报告模板和报告遵从性补充证明书，并咨询适当的支付品牌和/或收单机构了解提交程序事宜。

附录 B： 补偿性控制工作表

使用本工作表为任何选中“是，已填写 CCW”的要求定义补偿性控制。

注：只有已采取风险分析并具有合理的技术限制或书面业务限制的公司才能考虑使用补偿性控制来实现遵从性。

有关补偿性控制和如何填写本工作表的信息，请参见 PCI DSS 的附录 B、C 和 D。

要求编号和定义：

	所需信息	解释
1. 限制	列出导致无法遵守最初要求的限制。	
2. 目的	定义最初控制的目的；确定通过补偿性控制实现的目的。	
3. 已确定的风险	确定由于缺少最初控制而导致的任何其他风险。	
4. 补偿性控制的定义	定义补偿性控制并解释其如何实现最初控制的目的并解决增加的风险（若有）。	
5. 补偿性控制的验证	定义如何验证并测试补偿性控制。	
6. 维护	规定流程和控制措施以维护补偿性控制。	

第 3 节： 认证和证明书详情

第 3 部分 PCI DSS 认证

此 AOC 基于 (SAQ 填写日期) 填写的 SAQ B-IP (第 2 节) 中的结果。

基于上述 SAQ B-IP 中记录的结果, 第 3b-3d 部分中指定的签署者 (如果适用) 针对本文档第 2 部分中指定的实体声明以下遵从性状态 (选中一个选项):

<input type="checkbox"/>	<p>遵从: 已填写 PCI DSS SAQ 的所有章节且已针对所有问题提供积极回复, 从而获得了总体遵从评分; 因此 (商户公司名称) 已证明其完全遵从 PCI DSS。</p>						
<input type="checkbox"/>	<p>未遵从: 未填写 PCI DSS SAQ 的部分章节或未针对所有问题提供积极回复, 从而获得了总体未遵从评分, 因此 (商户公司名称) 未证明其完全遵从 PCI DSS。</p> <p>遵从目标日期:</p> <p>如果某实体提交的本表单具有未遵从状态, 则可能需要填写本文档第 4 部分中的行动计划。在填写第 4 部分之前, 请先咨询您的收单机构或支付品牌。</p>						
<input type="checkbox"/>	<p>遵从但包含法律规定的例外情况: 由于受到阻止满足相关要求的法律限制, 因此一项或多项要求选为了“否”。此选项要求收单机构或支付品牌进行附加审核。</p> <p>如果选中此选项, 请填写以下内容:</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">相关要求</th> <th>有关法律限制如何阻止满足相关要求的详情</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	相关要求	有关法律限制如何阻止满足相关要求的详情				
相关要求	有关法律限制如何阻止满足相关要求的详情						

第 3a 部分 确认状态

签署者确认:

(选中所有合适选项)

<input type="checkbox"/>	已根据本文中的说明填写第 (SAQ 版本) 版 PCI DSS 自我评估调查问卷 B-IP。
<input type="checkbox"/>	上述引用的 SAQ 和本证明书中的所有信息在一切重要方面均完全代表本次评估的结果。
<input type="checkbox"/>	已向相应的支付应用程序供应商确认自己的支付系统未在验证后存储敏感验证数据。
<input type="checkbox"/>	已阅读 PCI DSS 且了解必须始终遵从适用于所在环境的 PCI DSS。
<input type="checkbox"/>	了解如果所在环境发生变化则必须重新评估所在环境, 并实施任何适用的 PCI DSS 附加要求。

第 3a 部分 确认状态 (续)

<input type="checkbox"/>	未在本次评估所审核的 ANY 系统中发现交易授权后仍存储完整磁道数据 ² 、CAV2、CVC2、CID、CVV2 数据 ³ 或 PIN 数据 ⁴ 的迹象。
<input type="checkbox"/>	ASV 扫描正由 PCI SSC 认证的授权扫描服务商 (ASV 名称) 完成

第 3b 部分 商户证明书

商户执行官签名 [↑]	日期:
商户执行官姓名:	职务:

第 3c 部分 合格安全性评估商 (QSA) 确认 (如适用)

如果 QSA 参与了或帮助完成本次评估, 请说明其执行的角色:

QSA 公司正式授权管理人员签名 [↑]	日期:
正式授权管理人员姓名:	QSA 公司:

第 3d 部分 内部安全性评估商 (ISA) 参与 (如适用)

如果 ISA 参与了或帮助完成本次评估, 请确认该 ISA 工作人员, 并说明其执行的角色:

² 实卡交易中用于授权的磁条编译数据或芯片上的类似数据。实体不得在交易授权后保留完整磁道数据。唯一可保留的磁道数据部分为主帐户 (PAN)、失效日期和持卡人姓名。

³ 用于验证非实卡交易而印于支付卡签名条或正面的三位或四位数值。

⁴ 持卡人在实卡交易中输入的个人识别码, 和/或交易消息中包含的加密 PIN 数据块。

第 4 部分 针对未遵从要求的行动计划

针对每项要求的“PCI DSS 要求遵从性”选择合适的回复。如果您针对任一要求回复了“否”，则需要提供您所在公司预计遵从该要求的日期，并简要说明为满足该要求所采取的行动。

在填写第 4 部分之前，请先咨询您的收单机构或支付品牌。

PCI DSS 要求*	要求说明	遵从 PCI DSS 要求 (选择一个选项)		补救日期和行动 (如果针对任一要求选择了“否”)
		是	否	
1	安装并维护防火墙配置以保护持卡人数据	<input type="checkbox"/>	<input type="checkbox"/>	
2	不要使用供应商提供的默认系统密码和其他安全参数	<input type="checkbox"/>	<input type="checkbox"/>	
3	保护存储的持卡人数据	<input type="checkbox"/>	<input type="checkbox"/>	
4	加密持卡人数据在开放式公共网络中的传输	<input type="checkbox"/>	<input type="checkbox"/>	
6	开发并维护安全的系统和应用程序	<input type="checkbox"/>	<input type="checkbox"/>	
7	按业务知情需要限制对持卡人数据的访问	<input type="checkbox"/>	<input type="checkbox"/>	
8	识别并验证对系统组件的访问	<input type="checkbox"/>	<input type="checkbox"/>	
9	限制对持卡人数据的物理访问	<input type="checkbox"/>	<input type="checkbox"/>	
11	定期测试安全系统和流程	<input type="checkbox"/>	<input type="checkbox"/>	
12	维护针对所有工作人员的信息安全政策	<input type="checkbox"/>	<input type="checkbox"/>	
附录 A2	针对使用 SSL/早期 TLS 的实体的 PCI DSS 附加要求	<input type="checkbox"/>	<input type="checkbox"/>	

* 此处提及的 PCI DSS 要求是指本 SAQ 第 2 节中的问题。

