Payment Card Industry (PCI)
数据安全标准》

现场评估遵从性证明书 – 商户

3.2.1 版

2018 年 6 月

第 1 节： 评估信息

提交说明

商户必须填写此遵从性证明书，以声明其按照*支付卡行业数据安全标准 (PCI DSS) 要求和安全评估程序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）或支付品牌以了解报告和提交程序。

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）	此评估覆盖哪些支付渠道？ ☐ 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评估范围内，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（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）
			☐ 是 ☐ 否	
			☐ 是 ☐ 否	
			☐ 是 ☐ 否	
			☐ 是 ☐ 否	
			☐ 是 ☐ 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)？ 如果是的话： QIR 公司名称： QIR 个人名称： QIR 所提供服务的说明：	☐ 是 ☐ 否
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：**

注：*要求 12.8 适用于上述列表中的所有条目。*

第 2 节：　遵从性报告

本遵从性证明书反映了现场评估的结果，该结果已文档记录在随附的遵从性报告 (ROC) 中。

文档记录在本证明书以及本 ROC 中的评估完成于：	
补偿性控制是否被用于满足本 ROC 中的任何要求？	☐ 是　☐ 否
本 ROC 中的任何要求是否被识别为不适用 (N/A)？	☐ 是　☐ 否
有任何要求未经测试吗？	☐ 是　☐ 否
本 ROC 中有任何要求由于法律限制而无法得到满足吗？	☐ 是　☐ 否

第 3 节： 认证和证明书详情

第 3 部分 PCI DSS 认证

此 AOC 基于*（ROC 填写日期）填写的 ROC 中的结果。*

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

☐	**遵从：**已填写 PCI DSS ROC 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。
☐	**未遵从：**未填写 PCI DSS ROC 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。 **遵从目标日期：** 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。*
☐	**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标为了“不到位”。此选项要求收单机构或支付品牌进行附加审核。 *如果选中此选项，请填写以下内容：*

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）

☐	本 ROC 是根据 *PCI DSS 要求和安全评估程序*版本*（版本号）*，并按照其中的说明完成。
☐	上述引用的 ROC 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。
☐	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。
☐	已阅读 PCI DSS 且了解必须始终遵从适用于所在环境的 PCI DSS。
☐	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）	
☐	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[1]、CAV2、CVC2、CID、CVV2 数据[2]或 PIN 数据[3]的迹象。
☐	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：	

[1] 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。

[2] 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。

[3] 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	☐	☐	
2	不要使用供应商提供的默认系统密码和其他安全参数	☐	☐	
3	保护存储的持卡人数据	☐	☐	
4	加密持卡人数据在开放式公共网络中的传输	☐	☐	
5	为所有系统提供恶意软件防护并定期更新杀毒软件或程序	☐	☐	
6	开发并维护安全的系统和应用程序	☐	☐	
7	按业务知情需要限制对持卡人数据的访问	☐	☐	
8	识别并验证对系统组件的访问	☐	☐	
9	限制对持卡人数据的物理访问	☐	☐	
10	跟踪并监控对网络资源和持卡人数据的所有访问	☐	☐	
11	定期测试安全系统和流程	☐	☐	
12	维护针对所有工作人员的信息安全政策	☐	☐	
附录 A2	针对使用 SSL/早期 TLS 进行实卡 POS POI 终端连接的实体的 PCI DSS 附加要求	☐	☐	