小型商户支付保护资源

要请教供应商的若干问题

1.0 版 | 2016 年 7 月

PCI Security Standards Council®

简介

编制本文档旨在为小型商户业主和经营者提供支持。本文档通过提供要请教供应商和服务提供商的若干问题，旨在帮助您了解这些实体如何保护客户卡数据。

*编制《要请教供应商的若干问题》*作为对*《安全支付指南》*（小型商户支付保护资源的一部分）的补充。请访问以下网站，参阅*《安全支付指南》*及其他小型商户支付保护资源：

资源	网址
安全支付指南	https://zh.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf
常见支付系统	https://zh.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf
支付和信息安全术语词汇表	https://zh.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf

供应商和服务提供商，及其运作方式

小型企业/商户可能会接触到许多支付供应商或服务提供商，了解合作供应商属于哪种类型，并确保该供应商已采取适当的措施保护卡数据对商户来说至关重要。

第 2 页上的表格描述了最常见的几类支付供应商和服务提供商，以及商户应对每一类供应商分别抱有怎样的期待。

从第 3 页开始的表格为商户提供了若干可以请教其供应商或服务提供商的问题，从而帮助他们了解相关供应商或服务提供商在保护卡数据方面发挥的作用。

2016 PCI 安全标准委员会版权所有。保留所有权利。

供应商和服务提供商

下表描述了最常见的几种支付供应商和服务提供商类型，以及商户应对每一类供应商分别抱有怎样的期待。

供应商/服务提供商类型	职责	PCI 标准或程序	可寻求的帮助:
支付应用程序供应商	销售并支持可存储、处理和/或传输持卡人数据的应用程序。	支付应用程序数据安全标准 (PA-DSS)	应用程序在 List of PCI PA-DSS of Validated Payment Applications (认证支付应用程序的 PCI PA-DSS 列表)上。
支付终端供应商	销售并支持用于接受实卡支付的设备（例如支付终端）。	PIN 交易安全 (PTS)	支付终端在 List of PCI Approved PTS Devices (PCI 认可的 PTS 设备列表)上。
支付处理商、电子商务托管服务提供商/处理商	代表您存储、处理或传输持卡人数据。 还可以托管并管理您的电子商务服务器/网站，和/或开发并支持您的网站。	PCI 数据安全标准 (PCI DSS)	向他们索要 PCI DSS 遵从性证明书，并询问其评估是否包含您正在使用的服务。 服务提供商在下列任一列表上: MasterCard's List of Compliant Service Providers (MasterCard 的合规服务提供商列表) Visa's Global Registry of Service Providers (Visa 的全球服务提供商登记簿) Visa Europe's Registered Member Agents (Visa 欧洲地区的注册会员代理商)
软件即服务提供商	开发、托管和/或管理基于云的网络应用程序或支付应用程序（例如网上售票或预订应用程序）。	PCI DSS	向他们索要 PCI DSS 遵从性证明书，并询问其评估是否包含您正在使用的服务。 服务提供商在下列任一列表上: MasterCard's List of Compliant Service Providers (MasterCard 的合规服务提供商列表) Visa's Global Registry of Service Providers (Visa 的全球服务提供商登记簿) Visa Europe's Registered Member Agents (Visa 欧洲地区的注册会员代理商)
集成商/经销商	代表您安装经 PA-DSS 认证的支付应用程序。	合格的集成商和经销商 (QIR)	询问供应商是否为 PCI 合格集成商或经销商 (QIR)。 供应商在 List of PCI QIRs (PCI QIR 列表)上。
满足 PCI DSS 要求的服务提供商	代表您管理/运营系统或服务（例如防火墙管理、安装补丁/AV 服务）。	PCI DSS	向他们索要 PCI DSS 遵从性证明书，并询问其评估是否包含您正在使用的服务。 服务提供商在下列任一列表上: MasterCard's List of Compliant Service Providers (MasterCard 的合规服务提供商列表) Visa's Global Registry of Service Providers (Visa 的全球服务提供商登记簿) Visa Europe's Registered Member Agents (Visa 欧洲地区的注册会员代理商)

2016 PCI 安全标准委员会版权所有。保留所有权利。

问题

下表包含了一系列商户可询问其供应商/服务提供商的问题，以便确定保护卡数据的适当控制是否实施到位。

问题 *由商户向供应商提出*	**期望从供应商那里得到的答案**	**建议采取的行动** *基于供应商的回复*
您的解决方案或产品的安全程度如何?		
1. 您的解决方案/产品能否确保安全捕获并传输持卡人数据?	**针对面对面实卡支付交易:** **是** • 单击此处，了解支付终端是否获得了 PCI PTS 的批准: List of PCI Approved PTS Devices (PCI 认可的 PTS 设备列表) 和/或 • 单击此处，了解支付应用程序是否经过 PCI PA-DSS 的认证: List of PCI PA-DSS of Validated Payment Applications (认证支付应用程序的 PCI PA-DSS 列表) 或 • 单击此处，了解加密解决方案是否经过 PCI P2PE 的认证: List of PCI P2PE Validated Solutions (PCI P2PE 认证解决方案列表) **针对无实卡支付交易（包括电子商务、邮件/电话订购）:** **是** • 单击此处，了解支付应用程序是否经过 PCI PA-DSS 的认证: List of PCI PA-DSS of Validated Payment Applications (认证支付应用程序的 PCI PA-DSS 列表) 或 • 单击此处，了解服务提供商是否为符合 PCI DSS 的服务提供商: MasterCard's List of Compliant Service Providers (MasterCard 的合规服务提供商列表) Visa's Global Registry of Service Providers (Visa 的全球服务提供商登记簿) Visa Europe's Registered Member Agents (Visa 欧洲地区的注册会员代理商)	如果回答为**否**，请询问问题 2。

2016 PCI 安全标准委员会版权所有。保留所有权利。

问题

问题 *由商户向供应商提出*	**期望从供应商那里得到的答案**	**建议采取的行动** *基于供应商的回复*
您的解决方案或产品的安全程度如何？ *续*		
2. 我们与您（供应商）签订的协议是否包含声明您将维持产品/服务的 PCI DSS 遵从性（或者成为经过 PCI DSS 认证的产品/服务）的条款？	**是** 拥有现已符合或未来将符合 PCI DSS 的产品/解决方案的供应商应该非常乐意将此情形纳入书面协议中。 有关要寻找的关于符合 PCI DSS 的产品/解决方案的证据的其他信息，请参阅上面的问题 1。	如果回答为**否**，请考虑另一个供应商或解决方案。
3. 您的产品/解决方案是否在本地存储支付卡信息（在我的商店/店铺位置）？	**否** 如果确实是这样，商户可以考虑令牌化或加密解决方案，以便更好地保护卡数据。参见*《安全支付指南》*，了解有关加密和令牌化的更多信息。	如果回答为**是**，商户应与供应商确认根据 PCI DSS 要求存储数据。否则，请考虑另一个供应商。
4. 您的产品/解决方案是否通过强效加密保护支付卡信息？	**是** 加密是保护信息的一种方式，可以减小信息被盗的可能性。如果可以，请从 List of PCI P2PE Validated Solutions (PCI P2PE 认证解决方案列表)中进行选择，这些解决方案能够在您接收卡数据后立即对其实施保护，并在数据在网络中传输时为其提供保护。	如果回答为**否**，请考虑另一个供应商或解决方案。

2016 PCI 安全标准委员会版权所有。保留所有权利。

问题

问题 *由商户向供应商提出*	期望从供应商那里得到的答案	建议采取的行动 *基于供应商的回复*
我的产品的安全程度如何?		
5. 如果供应商将安装 PCI 委员会 List of Validated Payment Applications (认证支付应用程序列表)中的支付应用程序，则询问: 您是否为 PCI 合格集成商或经销商 (QIR)?	**是** QIR 经过委员会的培训，并且获得了安装和集成 PA-DSS 支付应用程序的资质，他们的安装工作可确保 PA-DSS 支付应用程序已以支持 PCI DSS 遵从性的方式实施。 单击此处，了解该供应商是否列于: List of PCI QIRs (PCI QIR 列表)上。	如果回答为**否**，则请询问左边的这些后续问题。
如果对上述问题的回答为否，则提出以下后续问题: 如果该供应商将安装的应用程序未经 PCI SSC 认证，或者如果该供应商不是 QIR，则请询问: • 您在安装期间是否提供支持，以确保我们的实施满足 PCI DSS 要求? • 您是否提供实施指南? • 您是否提供有关如何确保卡数据在任何地方进行存储、处理或传输时均受到保护的安装指南?	**是** 供应商应该已定义相关流程，以帮助您依照 PCI DSS 要求安装解决方案。安装不当可导致解决方案易受到数据威胁。 您请求供应商做出相关声明，具体说明将如何帮助您确保产品/解决方案符合或能够符合 PCI DSS 要求。	如果回答为**否**，请考虑另一个供应商。

2016 PCI 安全标准委员会版权所有。保留所有权利。

问题

问题 *由商户向供应商提出*	**期望从供应商那里得到的答案**	**建议采取的行动** *基于供应商的回复*
您是否向我提供关于产品/解决方案的持续支持和维护？ 如果是，将如何进行？		
6. 您的产品/解决方案是否安装在我的网络或系统中?	**是** 供应商应提供有关软件更新和安全补丁的持续维护和支持。此外，他们还应提供未来版本发布相关支持。 供应商/供货商完全支持其产品并且协助您实施安装/补丁，以确保对系统进行的任何更改均符合 PCI 要求，这符合您的最大利益。	如果回复为**是**，请参见左侧的后续问题。 如果回答为**否**，请前往问题 7。
如果对上述问题的回答为 是: • 您是否为系统/解决方案安装了补丁和更新程序? • 您是否以符合 PCI DSS 要求的方式执行了该操作? • 您将如何通知我；将如何提供补丁；以及将提供哪些支持?	**是** 如果解决方案从未更新过，可能将变得易受到未来的威胁。	如果回答为**否**，请考虑另一个供应商。
7. 安装在系统中的解决方案是否归服务提供商所有，并由其实施维护（托管）?	**是** 这被视为托管服务。如果服务提供商将托管解决方案，向他们索要 PCI DSS 遵从性证明书，并询问其评估是否包含您正在使用的服务。 查看服务提供商是否在下列任一列表上: MasterCard's List of Compliant Service Providers (MasterCard 的合规服务提供商列表) Visa's Global Registry of Service Providers (Visa 的全球服务提供商登记簿) Visa Europe's Registered Member Agents (Visa 欧洲地区的注册会员代理商)	如果回答为**是**，则请询问左边的这些后续问题。 如果回答为**否**—如果托管的服务不符合 PCI DSS—请考虑另一个解决方案。
如果对上述问题的回答为**是**: 该服务提供商的环境是否符合 PCI DSS?		

2016 PCI 安全标准委员会版权所有。保留所有权利。

问题 *由商户向供应商提出*	**期望从供应商那里得到的答案**	**建议采取的行动** *基于供应商的回复*
您是否向我提供关于产品/解决方案的持续支持和维护？ *续*		
8. 您是否需要远程访问我的支付系统/解决方案以便为其提供支持？	**否** 不法分子经常会利用远程访问窃取支付数据。远程访问功能应仅限于短期使用，所有其他时间内都应禁用。	如果回答为**否**，请前往问题 9。 如果回答为**是**，请询问左边的这些后续问题。
如果对上述问题的回答为 是： • 您是否需要始终激活远程访问？	**否** 远程访问功能应仅限于短期使用，所有其他时间内都应禁用。	如果回答为**是**—如果需要始终激活远程访问—请考虑另一个供应商或解决方案。
• 您将采取哪些措施来保护远程访问连接？	**远程访问每名客户时，您的供应商应使用多因素验证以及不同的用户名和密码。** 可以通过针对每个系统用户使用独一无二的用户 ID 和密码来保护远程访问。此外，应使用多种身份验证方法（多因素验证）来识别访问系统的用户身份。 针对每个客户使用独一无二的用户名/密码的供应商通过使用常见用户名和密码防止某一客户受到威胁导致许多或所有其他客户也受到威胁。	如果产品/解决方案无法为远程访问提供多因素验证，请考虑另一个解决方案。
9. 解决方案/产品是否需要与我的其他系统集成—例如，支付终端、应收账款，或其他含有持卡人数据的系统？	**否** 相较于可能拥有许多互连系统的较复杂支付系统，独立支付终端更易于保护。 如果解决方案确实需要与其他系统集成，这样是否简化了您的处理环境，以及/或者将如何为您的企业增加价值？ 您应该对集成有着强大的业务需求，因为使用集成解决方案将扩大 PCI DSS 范围，这样您将拥有更大并且更复杂的持卡人数据环境。	如果回答为**是**，请考虑另一个供应商或产品，除非对与其他系统互连的更复杂的解决方案有强大的业务需求。

2016 PCI 安全标准委员会版权所有。保留所有权利。

问题

问题 *由商户向供应商提出*	**期望从供应商那里得到的答案**	**建议采取的行动** *基于供应商的回复*
如果发生数据泄露会怎么样?		
10. 如果发生数据泄露，并且涉及到您的产品/解决方案: • 如果我受到处罚，您是否会提供支持和保护? • 如果存在漏洞，您将如何以及在何时通知我? • 您将提供何种数据泄露和可疑活动监控?	**是** 如果持卡人数据泄露，供应商/服务提供商应提供支持。 如果对托管服务或解决方案有所疑问，供应商/服务提供商应同意配合取证调查机构开展工作。 如果存在漏洞，并且确定供应商解决方案是根本原因，供应商/服务提供商应赔偿商户为此支付的罚款。	如果回答为**否**，请考虑另一个供应商或解决方案。
11. 供应商/服务提供商是否为与其产品/解决方案相关的数据泄露购买了保险?	**是** 购买保险之行为说明供应商/服务提供商充分考虑了自己需承担的与卡数据泄露相关的义务和责任。 如果回答为**是**，请询问保险范围，以及是否将涵盖您的实施的相关事宜。	如果回答为**否**—如果供应商未购买保险，或者不愿意自保—请考虑自行购买保险，或者雇用另一个供应商。
12. 如果发生数据泄露，并且证明产品解决方案是根本原因，供应商/服务提供商是否会协助通知我的客户?	**是** 当支付系统是造成漏洞的根本原因时，供应商/服务提供商应乐于协助商户传达数据漏洞通知。	如果回答为**是**，请询问左边的这些后续问题。 如果回答为**否**—如果供应商不协助传达通知—您应制定通知计划，并/或考虑另一个供应商。
如果回答为**是**，您将在多大程度上协助传达通知? • 您是否承担费用? • 您是否会发送通知? • 您是否会为受影响的客户提供信用监控?		

2016 PCI 安全标准委员会版权所有。保留所有权利。