BARCLAYS

# *外部供应商控制义务*

# 支付卡行业数据安全标准 (PCI DSS)

版本 13.0，日期 2023 年 9 月

| 控制标题 | 说明 | 为什么这很重要 |
| --- | --- | --- |
| 达到卡片数据合规 | 供应商应遵守支付安全标准委员会发布的最新版支付卡行业数据安全标准，例如 PCI DSS、PA-DSS、PCI-P2PE、PCI-PTS、PCI 卡片生产。 | 保护持卡人数据：实现这一目标的公认标准是 PCI DSS，它是全球行业法规要求。PCI 安全标准是支付卡行业安全标准委员会为保护持卡人数据而制定的技术和操作要求。 |
| 供应商和商家证明 | 在签署合同前以及签署后每年，供应商都必须提供现场评估合规证明 (AoC)，或者在适用的情况下提供适用于向巴克莱所提供服务范围的自我评估问卷 (SAQ)。这必须符合 PCI DSS 要求 - 请参阅 **www.pcisecuritystandards.org/**<br><br>如果在审核 AoC 时有问题提出，例如与服务范围、环境描述或供应商 PCI 合规性相关的问题，则可能我们可能会索取并审查相关合规性报告 (RoC) 以获得更多信息。如果确认 PCI 认证的范围适用于所提供服务的范围，或巴克莱在审核 AoC 后提出的其他问题，则经修订的 RoC 也许是可接受的。<br><br>供应商必须在不合规时通知巴克莱，即尽快通知，不晚于验证文件到期之日起 30 天内。 | 证明供应商或商家已就向巴克莱所提供的服务范围达到相关的卡片数据合规性，并遵守要求。证明供应商提供的证实 AoC/RoC 或 SAQ 与所提供的服务相关。<br><br>如果巴克莱使用任何不符合 PCI DSS 的供应商或商家，他们将需要通过电子邮件联系 Visa Europe 第三方风险团队 (agentcompliance@visa.com)，以确认该供应商或商家正在实施 PCI DSS，并向 Visa Europe 提供了 PCI DSS 状态计划（使用 Visa Europe 模板），供 Visa Europe 审查和批准。 |

| | | |
|---|---|---|
| 供应商确认 | 供应商必须在签订合同前以书面形式向巴克莱确认，他们对其拥有/存储/处理/传输的或者可能影响巴克莱客户的持卡人数据环境的以下服务的持卡人数据安全负责，例如安全服务（如身份验证服务器）、Web 托管等。<br><br>对所提供服务的任何变更都必须以书面形式向巴克莱确认，然后再实施变更。 | **来自 PCI DSS v3.2.1**<br><br>**12.8.2 检测程序：**遵守书面协议，并确认这些协议包括服务提供商的确认，表明他们对服务提供商所拥有或以其他方式代表客户存储、处理或传输的持卡人数据安全负责，或者在他们可能影响客户的持卡人数据环境安全性的情况下对持卡人数据安全负责。注意：结合要求 12.9，针对组织和服务提供商之间书面协议的这一要求旨在促进双方对其适用的 PCI DSS 责任的一致理解。例如，协议可能包括遵守适用的 PCI DSS 要求作为所提供服务的一部分。<br><br>**12.8.2 指南：**服务提供商的确认证明他们致力于维护由其客户获取的持卡人数据的适当安全。<br>服务提供商与客户参与流程相关的内部政策和程序，以及用于书面协议的任何模板，都应包括向其客户提供适用的 PCI DSS 确认。服务提供商提供书面确认的方法应由提供商与其客户商定。 |

***使用第三方服务提供商/外包***

服务提供商或商家可以使用第三方服务提供商代表他们存储、处理或传输持卡人数据，或管理路由器、防火墙、数据库、物理安全和/或服务器等组件。如果这样做，可能会影响持卡人数据环境的安全性。

各方应明确确定服务提供商 PCI DSS 评估范围内的服务和系统组件、服务提供商负责的特定 PCI DSS 要求，以及服务提供商的客户有责任在其自己的 PCI DSS 审查中包含的任何要求。例如，受管理的托管提供商应明确定义在其季度漏洞扫描过程中扫描哪些 IP 地址、其客户有责任在其季度扫描中包括哪些 IP 地址。

服务提供商有责任证明其 PCI DSS 合规性，支付品牌可能会要求这样做。服务提供商应联系其收购方和/或支付品牌，以确定适当的合规性验证。

第三方服务提供商可通过两种方式验证合规性：

1) **年度评估**：服务提供商可以自行进行年度 PCI DSS 评估，并向其客户提供证明其合规性的证据；或者

2) **多项按需评估**：如果服务提供商不进行自己的年度 PCI DSS 评估，则必须根据客户的要求进行评估并/或参与客户的每次 PCI DSS 审查，并向相应客户提供每次审查的结果。

如果第三方进行自己的 PCI DSS 评估，则他们应向其客户提供充足的证据，以验证服务提供商的 PCI DSS 评估范围涵盖了适用于客户的服务，并且已检查且确定符合相关 PCI DSS 要求。服务提供商向其客户提供的特定类型的证据，取决于双方之间的协议/合同。例如，提供服务提供商 RoC 的 AoC 和/或相关部分（为保护任何机密信息而进行了修订）有助于提供全部或部分信息。

此外，商家和服务提供商必须管理和监控有权访问持卡人数据的所有关联第三方服务提供商的 PCI DSS 合规性。*请参阅本文档中的“要求 12.8”以了解详细信息。*