Does Private Internet Access Comply with PCI DSS?

Kaneesha Davis - 2019-09-03 - Payments

No, Private Internet Access is not PCI DSS compliant.

The **Payment Card Industry Data Security Standard** (PCI DSS) is a proprietary information security standard for organisations that handle branded credit cards from the major card schemes (including Visa & Mastercard) The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council

Under Requirement 10 of the PCI DSS, to be PCI compliant a user must:

> "***Regularly Monitor and Test Networks***
> ***Requirement 10: Track and monitor all access to network resources and cardholder data***
>
> *Logging mechanisms and the ability to track user activities are critical in preventing, detecting and minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.*"

PCI guidelines regarding data retention state that the logs (access/activity) and protected information documentation proving that the covered entity is adhering to the PCI DSS Rule and is retained for 1 year.

In the event that a breach has occurred or is alleged to have occurred, it is important to be able to prove that the facets of PCI DSS have been followed. PCI DSS requires that internal audits of this data are performed regularly. Furthermore in the event that a breach has occurred, it is required by PCI DSS that the covered entity be able to produce this information when subpoenaed. As Private Internet Access does not log, we cannot provide the required information if subpoenaed by PCI DSS requirements.

And this, in summary, is why Private Internet Access cannot comply with PCI DSS requirements and as such cannot provide VPN for PCI services.

Tags

DSS

PCI