PCI DSS at Cloudflare

What is PCI?

Members of the PCI Security Standards Council (MasterCard, Discover, Visa, JCB International, and American Express) organized on September 7, 2006 to create PCI DSS which helps these payment processors and financial institutions mitigate the risk of credit card fraud. When a merchant (e.g., someone who accepts payment cards as a payment method for goods and services) makes a certain number of payment card transactions per year OR a company wishes to provide a product to help organizations meet their PCI compliance requirements, they are required to complete a full PCI DSS Report on Compliance.

Why is PCI important to Cloudflare?

PCI is important to Cloudflare because it serves as an independent report that customers can use to **gain trust** that we securely handle their and their customer's Card Holder Data (CHD). Many of our customers that wish to do business with us require that we provide a copy of our Attestation of Compliance (AoC). If we did not have this certification we would not be able to compete with our competitors, win larger customers, nor would our acquiring bank allow us to use payment cards as a payment method for our services!

What is in-scope for our Merchant Environment?

- Our Merchant scope consists of the following:
- The billing backend services
- v4 API/Dash
- TRACT
- Boomi
- BrainTree Payment Services
- TSYS
- Any metals/servers and network devices that support these systems and services.

What is in-scope for our Service Provider Environment?

Our Service provider environment consists of:

- Our entire Core production environment
- Our entire Edge production environment (excluding our China network).
- This includes **all metals/servers/network devices** that comprise our production Core and Edge environments.

How do I get a copy of Cloudflare's Attestation of Compliance (AoC) to a customer?

Your account executive or a member of the sales team can help you get a copy. Cloudflare requires an NDA to see our AoC.

How can Cloudflare help me meet PCI requirements?

If you use our WAF, enable the OWASP ruleset, and tune rules for your environment you will meet the need to protect web-facing applications and satisfy PCI requirement 6.6.

Cloudflare Access is changing the game and your relationship with your corporate VPN. Many organizations rely on VPNs and other segmentation tools to reduce the scope of their cardholder data environment. Cloudflare Access provides another means of segmentation by using Cloudflare's global network as a VPN service to access internal resources. Additionally, these sessions can be configured to time out after 15 minutes of inactivity to help customers meet requirement 8.1.8.

Cloudflare has given our customers the opportunity to configure higher levels of TLS. Currently, you can enable up to TLS 1.3 within your Cloudflare Dash, which exceeds the requirement to use the latest versions of TLS 1.1 or higher referenced in requirement 4.1.

In 2019 Cloudflare announced our time.cloudflare.com NTP service. The benefits of using our time service rely on the use of our CDN and our global network to provide an advantage in latency and accuracy. Our 200 locations around the world all use anycast to route your packets to our closest server. All of our servers are synchronized with stratum 1 time service providers, and then offer NTP to the general public, similar to how other public NTP providers function. Accurate time services are critical to maintaining accurate audit logging and being able to respond to incidents. By changing your time source to time.cloudflare.com we can help you meet requirement 10.4.3.