What is PCI compliance?

Credit card data needs to remain secret to be secure, and becoming PCI compliant establishes that a company will be able to keep that data secret. A person may stop telling their friend information about their private life if that friend can't keep a secret; similarly, credit card companies won't trust a company with card data if that company won't be able to keep it secure.

PCI compliance means obeying a set of security standards for card data, and any company that processes card transactions has to be PCI compliant. Transactions with credit cards, debit cards, and prepaid cards are all included within the scope of PCI compliance.

In other words, any business that accepts card payments from customers – over the Internet, over the phone, in an app, or in person – needs to follow a set of rules for protecting information about those card payments.

Card transaction data includes:

- Primary account number: The account number on the card, typically 16 digits long
- Full name: The name of the cardholder
- Expiration date: The month and year when the card expires
- Service code: The 3-digit or 4-digit code listed on the back of the card

PCI compliance is not required by U.S. federal law. Rather, the credit card industry enforces PCI compliance and charges fees to noncompliant companies. Fraud is a big expense for credit card companies that strong security helps them avoid.

The full name for this set of security standards is PCI-DSS.

What is PCI-DSS?

PCI-DSS stands for "Payment Card Industry Data Security Standard". PCI-DSS is a set of 12 overall information security standards, each with multiple sub-requirements, for keeping card data secure.

Five major credit card companies – American Express, MasterCard, Visa Inc., Discover Financial Services, and JCB International – collaborated to create PCI-DSS. Version 1.0 of PCI-DSS was released in December 2004. As of 2019, the latest version, version 3.2.1, was released in May 2018. However, these standards will continue to be updated over time.

The 12 security standards listed by PCI-DSS are:

1. Install a firewall
2. Change all default passwords on network-connected devices
3. Protect stored cardholder data via encryption, hashing, or other data protection methods
4. Encrypt cardholder data in transit
5. Install malware protection
6. Patch vulnerabilities in all systems and applications
7. Restrict access to cardholder data to authorized personnel
8. Control and restrict system access
9. Control and restrict physical access to cardholder data
10. Monitor access to data
11. Test security systems regularly
12. Maintain an information security policy

(Note: These are summarized versions of the standards only, not the actual standards. See the official PCI-DSS website for more.)

Whom does PCI DSS apply to?

Everyone from the bakery down on the corner to the multinational designer clothing brand needs to be PCI compliant – with the exception of customers who only accept cash. PCI compliance applies to any company that accepts credit cards, debit cards, or even prepaid cards for payment, even if a company uses a third party for processing card transactions or doesn't store card information.

Where do the PCI standards come from?

The PCI standards are developed by the Payment Card Industry Security Standards Council (PCI SSC). The council is made up of representatives from the five companies that initially developed PCI, although it acts independently of those five companies.

How is PCI compliance achieved?

For small- to medium-sized businesses, PCI compliance works on an honor system for the most part. Large enterprises need to be assessed by an auditor to confirm their PCI compliance.

PCI DSS divides companies (or "merchants," as the standards call them) into 4 levels based on the number of card transactions they each year. The levels are:

- Level 4: Fewer than 20,000 transactions per year
- Level 3: Between 20,000 and 1 million transactions per year
- Level 2: Between 1 and 6 million transactions per year
- Level 1: More than 6 million transactions per year

These definitions are mostly accurate, but every credit card company defines the levels slightly differently. It's important for customers to check with each card provider to see which level they are.

The way a customer, or merchant, can get certified as PCI compliant changes based on their level. Level 2-4 merchants have to fill out and submit a self-assessment questionnaire once a year. They also need to have an Authorized Scanning Vendor (ASV) scan their systems for vulnerabilities every quarter.

Level 1 merchants need a certified auditor, either a Qualified Security Assessor or an Internal Security Assessor, to audit their PCI compliance and submit a report. The auditing takes place either once a year or once a quarter (depending on the card company). Level 1 merchants need a quarterly vulnerability scan as well.

Finally, all merchants need to fill out and submit an Attestation of Compliance (AOC) form, which is basically a statement to the credit card company that the merchant is PCI compliant.

Is Cloudflare PCI compliant?

Naturally, data security is of paramount importance for Cloudflare. Cloudflare has been PCI certified as a Level 1 Service Provider since 2014. As of 2019, Cloudflare is compliant with the latest PCI-DSS standards.

How does Cloudflare help customers attain PCI compliance?

Cloudflare has obtained an independent attestation that for four Cloudflare products which comply with PCI DSS and these products can be used by customers to meet their own PCI compliance requirements. Cloudflare's WAF, CDN, Time Service, and Cloudflare Access are Service Provider certified for all Pro, Biz, and Enterprise accounts. Cloudflare Access provides another means of segmentation by using Cloudflare's global network as a VPN service to access internal resources. Access also helps to give those appropriate with access to systems that may store or transmit cardholder information. Additionally, these sessions can be configured to time out after 15 minutes of inactivity to help customers meetsrequirement 8.1.8.

Cloudflare also enables customers to use the latest versions of TLS encryption, another important part of PCI compliance.