[ ] Payrix

PCI Compliance

Quick Reference Guide

As digital payments continue to dominate, PCI compliance is not only a necessary part of doing business – it's a strategic imperative. The prevalence of data breaches targeting software companies and their customers continues to grow, further positioning compliance as a defense against the severe consequences of data breaches and a way to bolster trust within the payment ecosystem.

01 What is PCI compliance?

PCI compliance refers to a responsibility to abide by a standard enforced by the Payment Card Industry Security Standards Council (PCI SSC), made up of the major payment card brands – Visa, Mastercard, American Express, Discover, and JCB. The PCI Data Security Standard (DSS) is the Council's set of mandatory technical and operational requirements intended to standardize and protect the handling of sensitive cardholder information.

02 Why is PCI compliance important?

PCI compliance should be taken seriously by every business to prevent the harmful impacts of data breaches, which can be costly and very difficult to overcome. If a business experiences a data breach because they aren't PCI compliant, that business may be at risk of going under.

Avoid financial loss and penalties

According to a report from IBM and the Ponemon Institute, the average cost of a data breach for companies with less than 500 employees is $2.98 million. In addition to the direct loss of capital, there are also hefty non-compliance fees to be paid, some of which can reach $500,000. Ultimately, the costs associated with achieving PCI compliance pale in comparison to the potential financial repercussions of a data breach.

Safeguard your reputation

Businesses that experience a data breach and aren't prepared put their customers in a vulnerable position by exposing sensitive information. This could cause reputational deterioration. Complying with PCI requirements demonstrates a commitment to maintaining a vigilant defense.

Maintain business continuity

A breach can disrupt business operations and lead to significant downtime. In the event of a breach, a company is also required to contact every customer with compromised information, adding to the administrative burden and expense. Maintaining compliance supports the continuity of uninterrupted operations.

03 Who has to manage PCI compliance?

Any business that stores, processes, or transmits credit card information must comply with the PCI DSS. The compliance requirements specific to each business will depend on a company's annual transaction volume – these are generally split into four levels.

04 What's the best way to manage PCI compliance?

PCI compliance is achieved by successfully passing an annual attestation in the form of a PCI audit. This includes the completion of a Self-Assessment Questionnaire (SAQ), which can be complex – especially for businesses trying to complete it on their own – and can result in mistakes.

Give your customers the support they need to effectively manage their PCI compliance. Payrix offers a solution to simplify the attestation process for your customers and keep them protected from data breaches. After all, their business is your business.

SaferPayments is a program that includes:

- Guided support of PCI compliance management
- Customized SAQs for each business
- Access to an intuitive self-service portal for SAQ submission
- Non-compliance cost savings and financial assistance in the event of a breach