globalpayments for platforms

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 risk of data breaches targeting software companies and their customers reinforces the importance of compliance as a way to help protect sensitive information and build trust within the payment ecosystem.



01 What is PCI compliance?

PCI compliance means meeting the requirements of the Payment Card Industry Data Security Standard (PCI DSS). Developed by the PCI Security Standards Council (PCI SSC) made up of the major payment card brands Visa, Mastercard, American Express, Discover and JCB, the standard sets out security requirements to help businesses protect payment account data.

02 Why is PCI compliance important?

PCI compliance should be taken seriously by every business to help prevent the harmful impacts of data breaches, which can be costly and difficult to overcome. If a business experiences a data breach due to non-compliance, the resulting financial, operational and reputational impacts can be significant and long-lasting.

03 Who has to manage PCI compliance?

Any business that stores, processes or transmits payment card data must comply with PCI DSS. This also includes businesses that outsource payment processing. Specific compliance requirements depend on how payments are handled and the business's payment environment.

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

PCI compliance requires ongoing security practices and regular validation. Depending on the business, this may involve completing a Self-Assessment Questionnaire (SAQ) or undergoing a formal PCI assessment. The process can be complex, especially for businesses managing compliance on their own, and can result in mistakes.

Global Payments for Platforms™ offers a solution to simplify the attestation process for your customers and help reduce the risk of data breaches.

Avoid financial loss and penalties

According to IBM's Costof a Data Breach Report, the average cost of a data breach for companies with fewer than 500 employees was US$3.31 million. In addition to the direct loss of capital, there are also significant non-compliance fees, some of which can reach US$500,000. Ultimately, the costs associated with achieving PCI compliance pale in comparison to the potential financial repercussions of a data breach.

LOSS OF CAPITAL

US$3.31m

Average cost of a data breach for organisations with fewer than 500 employees.

And up to **US$500k** in non-compliance fees.

Safeguard your reputation

A data breach can expose sensitive customer information and cause significant reputational damage. Complying with PCI requirements demonstrates a commitment to protecting customer data and maintaining strong security practices.



Maintain business continuity

A breach can disruptbusiness operations andlead 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.

Need help supporting your customers with PCI compliance?

Talk to our team about how Global Payments for Platforms can help simplify the compliance process for your merchants.

Global Payments for Platforms™ partners with software companies to build exceptional commerce experiences. Backed by over 50 years of payments leadership and billions of transactions processed, we help platforms embed payments, grow financial services and navigate what's next with confidence. With the technology, expertise and scale to support every stage of the journey, we empower our partners to become indispensable to the businesses they serve. To learn more, visit platforms.globalpayments.com/en.
M10.1031-D184

©2026 Global Payments Inc. All rights reserved.