jscrambler

PCI DSS for Merchants and E-Commerce Websites

About the new PCI DSS version 4.0

E-commerce skimming or “Magecart” attacks have become the criminals’ favorite way of stealing payment card data. All e-commerce companies are at risk. Recognizing the inherent vulnerability of web forms to skimming attacks, **the new version of PCI DSS contains two requirements to prevent and detect e-commerce skimming attacks:**

Requirement 6.4.3

Aims to reduce the attack surface by ensuring that all JavaScript contained in a payment page is necessary, is included in an inventory, and has been explicitly approved. It also requires assurance of the integrity of all JavaScript.

Requirement 11.6.1

Aims to detect any tampering of JavaScript included in payment pages. It requires changes to scripts and page headers to be detected, and the appropriate alerts generated.

Merchants and E-commerce companies will need to be able to:

- Have full visibility and management of all scripts loaded on the payment page.
- Detect changes to existing first and third-party scripts.
- Create alerts flagging changes to existing scripts.
- Detect and evaluate changes to ensure they are not trying to steal cardholder data.

Start your compliance journey now

The new requirements are mandatory after 31 March 2025. However, it is vital that merchants **gain visibility, risk management capabilities, and control of JavaScript** before the standard requires it. Criminals are using this attack now and it is expected that they will increase its frequency and sophistication before the new requirements become widely deployed throughout the payment ecosystem.

Protect payment card data and guarantee compliance with the new PCI DSS requirements with Jscrambler

Key benefits

Protect cardholder data by preventing client-side data leakage attacks like Magecart in real-time.

Learn about the risks
By including a Jscrambler's tamper-resistant JavaScript agent on each page, an inventory of all scripts running is collected in real-time from every single browser session.

Gain complete visibility and control of the behavior of every script running on your website.

Assess the risks
Understand the risk when new scripts appear or existing scripts change on your website while considering risk factors to make informed decisions.

Improve compliance with PCI DSS 4.0 and other standards, laws and regulations such as: ISO 27001, NIST CSF, PSD2, GDPR, HIPAA, and CCPA.

Mitigate the risks
Going above and beyond the PCI DSS requirements, Jscrambler's Webpage Integrity can block all unwanted activity with an automatic rules engine that applies granular controls to different sections of the website, especially sections where payment data is present. It will block all unwanted activity such as reading form fields and exfiltrating cardholder data.

OWASP NIST ISO 27001 GDPR.EU CCPA