AKAMAI CHECKLIST

PCI DSS v4.0 JavaScript Security Checklist with Akamai Client-Side Protection & Compliance

The Payment Card Industry Data Security Standard (PCI DSS) is a global security standard developed to protect payment card data security online and facilitate the broad adoption of consistent data security measures globally. It is one of the most important security standards, and compliance is required by any organization that processes payment card data online.

The latest version of PCI DSS (available in English only), version 4.0, goes into effect in 2025. It includes 12 core data security requirements, updated with guidance to address new and evolving cybersecurity threats. Two major requirements added to PCI DSS v4.0, 6.4.3 and 11.6.1, address JavaScript security and protection against client-side web skimming attacks that steal sensitive end-user information from within the browser. These attacks have grown in popularity over the years and sophisticated techniques have made them increasingly harder to detect. They can have devastating consequences for victimized organizations — including hefty fines, harm to brand reputation, loss in revenue, and diminished customer trust.

Let's run through a checklist of what the new PCI DSS v4.0 script security requirements entail and how Client-Side Protection & Compliance stacks up.

PCI DSS v4.0 Requirements	How Client-Side Protection & Compliance Helps
Requirement 6.4.3 — Public-facing web applications are protected against attacks ☑ A method is implemented to confirm that each script loaded and executed in the browser is authorized ☑ A method is implemented to assure the integrity of each script loaded and executed in the browser ☑ An inventory of all scripts loaded and executed in the browser is maintained with written justification as to why each is necessary	**Authorize with one click** ☑ Easily manage which scripts you allow to execute on your website's payment pages directly within the tool **Assure integrity up front** ☑ Behavioral technology analyzes each script that is executed in the browser to detect and alert on malicious activity or data exfiltration **Track and inventory all scripts automatically** ☑ Predefined justifications and automated rules make it easy to justify the purpose of each script loaded and executed within the browser

PCI DSS v4.0 Requirements	How Client-Side Protection & Compliance Helps
Requirement 11.6.1 — Unauthorized changes on payment pages are detected and responded to **A change- and tamper-detection mechanism is deployed as follows:** ☑ To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser ☑ The mechanism is configured to evaluate the received HTTP header and payment page **The mechanism functions are performed** at least once every seven days or periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1)	**Keep your payment pages protected** ☑ Monitor, analyze, and mitigate malicious tampering of payment pages to ensure your end user's valuable data stays safe **Investigate unauthorized modifications in real-time with immediate, actionable alerts** ☑ With instant detection, security teams can quickly respond to unauthorized changes or modifications to HTTP headers on payment pages **Protect with always-on defense** ☑ Around-the-clock protection safeguards user interactions on your payment pages

Akamai Client-Side Protection & Compliance provides robust protection against JavaScript threats and allows visibility into the client-side attack surface to safeguard sensitive data in the browser. Its purpose-built PCI DSS v4.0 capabilities help security and compliance teams streamline the PCI DSS v4.0 auditing process and provide dedicated workflows to help meet script security requirements 6.4.3 and 11.6.1.

Akamai Client-Side Protection & Compliance has flexible deployment options and does not require Akamai Connected Cloud to be enabled.

Learn more about how these capabilities can help your organization comply with PCI DSS v4.0.

 | Support | Published 09/23