Payment Card Industry Data Security Standard (PCI DSS v4.0.1) Requirements 6.4.3 and 11.6.1

New requirements impacting your website's checkout page security are officially effective starting **April 1, 2025.**

Understanding the Changes

You're likely aware of the threat from **e-skimming** – essentially, digital pickpocketing where hidden malicious code is inserted onto checkout pages to steal customer card details during online transactions. To better combat this, PCI DSS v4.0.1 introduces two specific requirements for e-commerce merchants:

1. **Maintain an Inventory of Payment Page Scripts (Requirement 6.4.3):**
    - **What it means:** Think of your checkout page as a secure environment. This rule requires you to keep a detailed list, or inventory, of every piece of code (script) that runs within that environment (specifically, in the customer's browser).
    - **Action required:** For each script identified, you must document its purpose and confirm why it is essential for the payment process to function correctly and securely. This helps ensure only authorized code is present.
2. **Detect and Respond to Changes on the Payment Page (Requirement 11.6.1):**
    - **What it means:** You need a reliable method to detect if any scripts on your payment page are added, removed, or modified without authorization.
    - **Action required:** Implement a process or tool to monitor these scripts for unauthorized changes. This monitoring must occur **at least once every seven days**, or be handled by an automated solution that provides alerts. Technologies like Subresource Integrity (SRI) or Content Security Policy (CSP) can assist here.

Why This is Important for Your Business

These requirements are crucial for protecting your customers' sensitive payment information and maintaining the trust vital to your business. Preventing e-skimming helps safeguard your reputation, reduces the risk of costly data breaches, and ensures you meet industry security standards.

Action Required & Timeline

- **Effective Immediately:** Compliance with these requirements is necessary starting **today, April 1, 2025.**
- **Ongoing Compliance:** Whether you recently completed your annual PCI compliance review or have one scheduled, these new controls must be implemented and maintained going forward. They will be part of future PCI DSS v4.0.1 assessments.

How Mira Commerce Can Support You

We understand that identifying, inventorying, and justifying every script on your payment page can seem complex, especially when dealing with third-party integrations.

As your e-commerce partner, **Mira Commerce is prepared to assist you in tackling Requirement 6.4.3.** We can help you begin the process of identifying the scripts executing on your checkout page and documenting the necessary inventory and justifications.

An Important Clarification:

Please note that while Mira Commerce provides expert guidance and technical assistance, including help with your script inventory, **we do not perform official PCI DSS compliance certifications.** Validation of compliance must be done by a PCI Qualified Security Assessor (QSA). We are happy to help you understand the process and can point you toward resources for engaging with a QSA.

For more information and the official PCI guidance for these new requirements click here. (Link https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/Guidance-for-PCI-DSS-Requirements-6_4_3-and-11_6_1.pdf)