

PCI DSS v4.0 for Payment Service Providers

PCI DSS v4.0 contains two new requirements aimed at ensuring the integrity of pages where payment is taken on an e-commerce website. These requirements will become mandatory on 1st April, 2025.

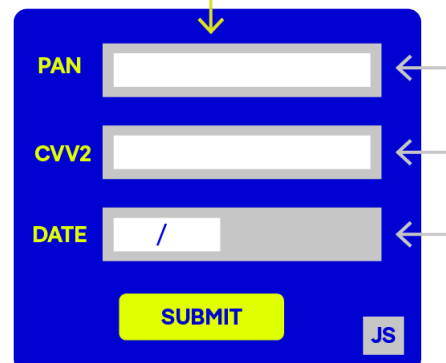
Requirement 6.4.3 is designed to protect an entity against skimming attacks by ensuring that all 1st party and 3rd party JavaScript present in the payment page is actively managed by:

- Maintaining an inventory of all the scripts in a page;
- Documenting why each script needs to be on the payment page;
- Recording that each script is specifically authorized;
- Ensuring the integrity of each script.

Requirement 11.6.1 is designed to alert an entity when a first- or third-party script (or the HTTP headers) of the website change, so that unauthorized changes are detected and quickly rectified.

“Parent page” From the merchant

The new requirements apply to this parent page which is typically the responsibility of the merchant.



A diagram of a payment form. It features three input fields: PAN, CVV2, and DATE. Below these fields is a yellow SUBMIT button and a small JS icon. A yellow arrow points from the 'Parent page' box above to the top of the form. A grey arrow points from the 'Payment page' box below to the bottom of the form. A vertical line on the right side of the form has arrows pointing to each of the three input fields.

“Payment page” From the PSP

The new requirements apply to the payment iframe(s), which are the responsibility of the PSP.



Payment Service Providers (PSPs)/Payment Gateways will need to be able to:

- Meet these new requirements for their own payment pages.
- Support merchants using PSP's solutions that typically would allow the merchant to meet the eligibility criteria for SAQ A and SAQ A-EP.
- Provide an entirely outsourced solution to enable merchants to complete SAQ A.

How Jscrambler can help

Jscrambler has been protecting client-side JavaScript from criminal attacks for over 10 years. Jscrambler's Webpage Integrity (WPI) and Code Integrity (CI) products can help PSPs.

Code Integrity

CI uses polymorphic code obfuscation to combat reverse engineering attempts. At the same time, it makes code tamper resistant, allowing preset reactions such as breaking the code to prevent attackers from analyzing or modifying it at runtime. CI will protect the JavaScript that PSPs provide to merchants to create the payment form.

Webpage Integrity

WPI protects payment pages from multiple types of attacks, like data skimming and form jacking, while also providing a real-time inventory and risk assessment of all JavaScripts running on the payment page.

WPI can be appended to the JavaScript that PSPs provide to their merchants to create the payment page. This allows the merchant to comply with the PCI DSS v4 requirements while providing the PSPs with real-time intelligence about attacks and the parent page environment.

Where PSPs also include third-party JavaScript in the payment page itself, WPI would both protect against malicious scripts and help meet the new requirements.



Jscrambler is a **Principal Participating Organization** of the **PCI Security Standards Council**.