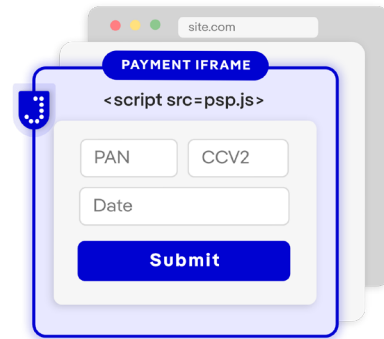**jscrambler**

Jscrambler's Iframe Integrity for Payment Service Providers

New PCI DSS updates that include new **SAQ A criteria** are making compliance more complex for

PSPs and their merchants by requiring protection against script-based attacks. Jscrambler's Iframe Integrity solves this challenge by securing payment pages with a controlled, tamper-proof environment. It streamlines compliance while enhancing security and trust for both PSPs and their merchants.

Harden your iframes to simplify PCI DSS v4 compliance requirements for your merchants

Ease PCI DSS compliance

The Iframe Integrity product prevents attacks against the iframe and potential skimming of payment card data, which is the objective of PCI DSS requirements 6.4.3 and 11.6.

Help your merchants achieve SAQ A eligibility

Iframe Integrity facilitates meeting the SAQ A requirements of obtaining confirmation that the TPSP's or payment processor's solution includes techniques that protect the merchant's payment page from script attacks.

Protect your competitive edge and unlock new revenue

With Iframe Integrity, PSPs can better differentiate themselves from the competition, boosting merchant retention while standing out from larger players. It also unlocks new revenue streams, through premium pricing or upselling, for hassle-free merchant PCI DSS compliance.

Key business benefits

An innovative solution for payment processors to simplify PCI DSS v4 Requirements 6.4.3 and 11.6.1 and SAQ A eligibility for their merchants

Potential for business expansion and new revenue by offering hassle-free PCI DSS compliance and covering the needs of merchants of all sizes

Smooth Plug'n'Play integration with zero disruptions— Iframe Integrity seamlessly integrates into your existing setup, requiring no changes for PSPs or merchants

Enhanced Protection against payment card data skimming and data leakage prevention

Powerful suite of features to help you excel at client-side protection

PSP Script Hardening	Makes the PSP script tamper-resistant, protecting against reverse engineering and automated threats.
Iframe Hijacking Protection	Prevents Iframe Hijacking attacks by isolating DOM methods that can be used to tamper with the iframe creation process (on the parent page).
Iframe Overlay Protection	Prevents Iframe Hijacking attacks by isolating DOM methods that can be used to create new iframes or to tamper with existing ones (on the parent page).
Form Overlay Protection	Prevents Iframe Hijacking attacks by isolating DOM methods that can be used to create new Forms or to tamper with existing ones (on the parent page).
Function Hijacking Protection	Applies monkey-patching protection in privileged functions (on the parent page).
Iframe Control	Provides fine-grained control over how iframes can be used by scripts (on the parent page).
Form Control	Provides fine-grained control over how forms can be used by scripts (on the parent page).

Jscrambler is the most comprehensive solution for client-side protection
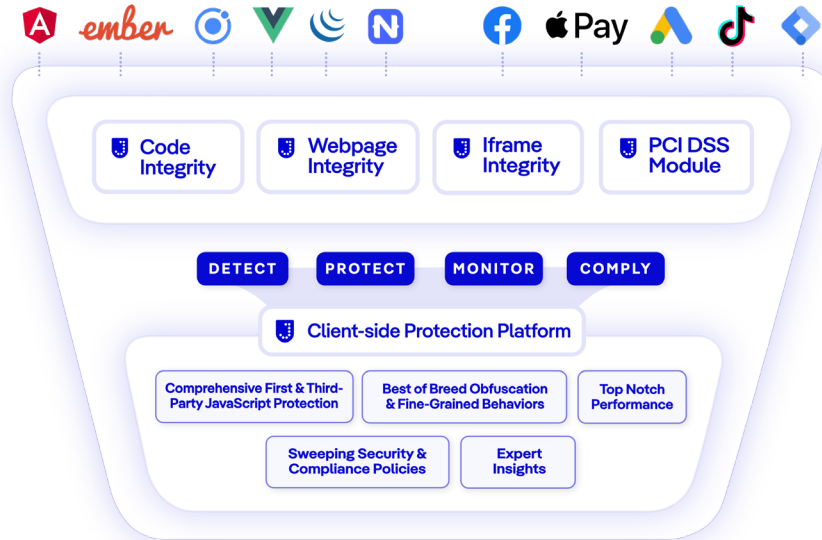
Jscrambler is a Principal Participating Organization of the PCI Security Standards Council and a PCI DSS compliant service provider.

Want to see Jscrambler's Iframe Integrity in action and deliver instant PCI DSS compliance to your merchants?

Book a demo ›

About Jscrambler

Jscrambler is the leader in Client-Side Protection and Compliance. Jscrambler is the first to merge advanced polymorphic JavaScript obfuscation with fine-grained third-party tag protection in a unified Client-Side Protection and Compliance Platform. Jscrambler's integrated solution ensures a robust defense against current and emerging client-side cyber threats, data leaks, misconfigurations, and IP theft, empowering software development and digital teams to securely innovate online with JavaScript. Jscrambler's technology is trusted by the Fortune 500 and thousands of companies globally.

If you want to know more about how Jscrambler can help you prevent client-side attacks, don't hesitate to contact us: hello@jscrambler.com | +1 650 999 0010