source DEFENSE

The Payment Service Provider & eCommerce Platform Playbook for eSkimming Security and PCI DSS 4.0.1 Compliance

Turn Security & Compliance into a Competitive Advantage

INTRODUCTION

Payment Service Providers (PSPs), eCommerce platform providers and the merchants they serve are all bracing for the full enforcement of new requirements for eSkimming security found in version 4.01.of the Payment Card Industry Data Security Standard (PCI DSS). These requirements, which have been future dated for the past two years, technically took effect at midnight on April 1, 2025.

Despite this deadline, a majority of organizations across the payments ecosystem have yet to address the required security controls and compliance processes outlined under PCI DSS sections 6.4.3 and11.6.1. Confusion on scope, on roles and responsibilities, a good bit of procrastination, and a misunderstanding of just how easy it is to address these requirements are to blame.

This eBook is designed to give you all the information you need to understand your own requirements for security and compliance; to define a simple, easy and cost effective path to take; to explain the expanded role you may now play for the merchants you serve; and to outline an opportunity to turn security and compliance into both a competitive advantage and revenue generating opportunity for your organization.

Executive Summary (The TLDR)

eSkimming is driving fraud
It's front and center for card brands, acquirers, and the PCI Council. Visa keeps sounding the alarm. MasterCard made it a key focus of its C-VEP program.

JavaScript is the risk surface
Modern eCommerce depends on it—from analytics to payments—but most of that code, especially third-party scripts, goes unmonitored. That's how attackers steal sensitive data—right as users type it into online forms.

You must implement new controls
PCI DSS 4.0 now requires you to manage the JavaScript running on your payment pages. You need to inventory it, justify its use, monitor for tampering or malicious behavior, and respond quickly to threats.

You need to act
The deadline may have passed, but assessments are happening now. If 6.4.3 and 11.6.1 controls aren't in place, you're at risk of failing.

This doesn't need to be hard or expensive
There's a proven, easy-to-deploy solution that addresses the problem out of the box. It includes behavior-based controls, real-time protection, and push-button compliance reporting.

Shared responsibility
Your merchants have their own PCI obligations. Their compliance depends on their size and validation type—but your ability to support them depends on having the right tools and processes in place.

ESKIMMING

A PRIMARY AND GROWING SOURCE OF PAYMENTS FRAUD

Cyber criminals are increasingly targeting the first and third-party scripts that power the modern website to conduct eSkimming attacks. They exploit vulnerabilities in these scripts - and the fact that virtually no monitoring or security controls are in place - to inject malicious code.

Once injected, this malicious code enables attackers to steal data at the point of input by either sniffing legitimate forms, introducing attacker controlled fields that ask for sensitive information, or completely redirecting traffic during the checkout process to attacker controlled websites spoofed to look legitimate. eSkimming represents a shift in focus from traditional data targets—data in transit or at rest—to the point where users first input their data.

These attacks may be referred to as Magecart, eSkimming, digital skimming, clickjacking, credential harvesting and other terms, but they are all synonymous with a major threat confronting consumer personally identifiable information (PII), credentials and payment card data.

Visa's biannual threat reports continually highlight the issue of eSkimming. From June of 2022 they have warned that, "The targeting of eCommerce platforms and third-party code integrations are among the most common tactics utilized by threat actors ... threat actors are targeting supply chains and third-party service providers with high frequency and exhibiting continued interest in payment account data and personally identifiable information."

It is important to note that while PCI DSS 4.0.1 specifically calls for eSkimming controls to be placed on payment pages, eSkimming attacks are increasingly targeting non-payments website infrastructure as well. Visa's Fall 2024 bi-annual report highlights the need to think about protecting the entire Merchant website, not just payment pages themselves "As nonpayments infrastructure may lack stringent security controls, threat actors can more easily gain initial access into the victim's environment, and from there, deploy digital skimming malware into the checkout environment to obtain payment data.

This trend in the targeting of non-payments infrastructure by threat actors reinforces the importance of ensuring all code deployed onto web environments is routinely reviewed."

UNDERSTANDING ESKIMMING ATTACKS

IT'S ALL ABOUT THE SCRIPTS

The ability of cybercriminals to target this data in real time, exposing potentially billions of online consumer sessions to their illicit activities, stems from the evolution of the modern website and a fundamental weakness in website design, security and third-party risk management. JavaScript powers the vast majority of the world's websites.

First party scripts are designed in house but increasingly rely upon open source libraries which introduce flaws, security gaps and even (in some cases) malicious code injected into these libraries without being detected. In most cases, the scripts employed on eCommerce sites come from third-party digital supply chain partners, whose code is neither vetted by website owners nor controlled by them with any regularity.

The inception of third-party scripts dates back to the early days of web development, when the need for dynamic content and functionality led to widespread adoption. Initially, these scripts were simple tools for enhancing website aesthetics or tracking basic user interactions. As the internet matured, so did the complexity and capabilities of these scripts, evolving into sophisticated tools integral to eCommerce, social media and data analytics.

Today, third-party scripts are indispensable, powering everything from chatbots and payment gateways to analytics and advertising tools. Scripts can help businesses better understand their customers and tailor their offerings accordingly. However, this reliance poses significant security challenges. These scripts, by nature, can access, modify and transmit sensitive user data, making them prime targets for cyber adversaries.

High Profile Breaches Show What's at Stake

Large Children's Apparel Retailer (2019)
Hackers inserted malicious code into the checkout process, skimming financial data directly from the form. Names, addresses, card numbers, CVVs, and expiration dates were all potentially exposed.

Global Airline (2018)
Malicious third-party scripts on the airline's website captured customer data during payment—impacting 380,000 transactions and resulting in heavy penalties and lasting reputational harm.

Ticket Sales & Distribution Company (2018)
The company website was compromised through a third-party chatbot script. The breach exposed the personal and payment information of thousands of customers.

YOUR REQUIREMENTS

AS A PAYMENTS SERVICE PROVIDER OR ECOMMERCE PLATFORM PROVIDER

If you provide or host payment functionality for eCommerce Merchants, you are required as a Third Party Services Provider (TPSP) to implement eSkimming controls on your own infrastructure.

PCI DSS 4.0.1 places clear and immediate obligations on your organization - particularly with the enforcement of Requirements 6.4.3 and 11.6.1 starting April 1, 2025. These requirements are no longer optional or aspirational; they are foundational controls designed to protect cardholder data in today's threat landscape.

What you must do

Requirement 6.4.3 – Script Management

As a PSP or eCommerce Platform provider, you are required to adopt strict management practices for scripts running on your payment pages.

These requirements apply to all payment pages you control - whether they be stand alone pages a Merchant fully redirects to, or iFrames you supply to Merchants to embed on their sites:

- Maintain a full and complete inventory of all scripts executing on your payment pages - whether authored internally, sourced from a third-party or brought in by nth party dependencies (i.e. called in by a third party script)
- Confirm the script is authorized to be running and document that authorization
- Justify the existence of each script, explaining its purpose and maintain a clear record of this justification
- Assure its integrity—meaning you must be able to detect if the script has been modified without authorization.

If you host or embed the payment form, you are fully responsible for the security of every script within that context.

Requirement 11.6.1 – Tamper Detection and Alerting

You must implement a mechanism to monitor your payment pages and detect unauthorized modifications. At a minimum, this includes:

- Monitoring for changes to the page and its HTTP headers at least once every seven days.
- Generating alerts if malicious scripts are detected.
- Either blocking unauthorized scripts in real-time to prevent the exfiltration of sensitive data, or adopting a rapid response program to manually thwart exfiltration once detected

Together, these requirements aim to prevent and detect client-side attacks—especially eSkimming—by giving you visibility and control over what's running in your users' browsers during a transaction.

Introducing New Complexity

Modern eCommerce sites and payment pages are built from a complex web of first and third-party scripts - for analytics, personalization, advertising, and more. Maintaining full visibility, conducting an active inventory, and monitoring and managing them in real time requires specialized tools and a shift in mindset. A variety of different approaches exist which we will delve into later in this eBook.

Complicating the issue of eSkimming further is the shared responsibility model that exists between PSPs, eCommerce Platform providers and merchants. You have a requirement to ensure your own controls are in place, and to provide proof of PCI Compliance to Merchants as a Third Party Service Provider.

And they should—because they cannot see or secure the scripts running inside your infrastructure, but they are still accountable for ensuring their customers' data is protected.

Merchants have their own responsibilities which vary depending upon the type of Merchant they are under the PCI DSS Standard (i.e. the predefined PCI Merchant level) and the specific compliance reporting mechanism they utilize. For Small Merchants and those reporting under Self Assessment Questionnaire A (SAQ-A), the PCI DSS creates an opportunity for your firm to both differentiate itself and harness additional revenue

UNDERSTANDING TECHNICAL APPROACHES TO ESKIMMING SECURITY

AVOIDING PITFALLS ON A NOBLE JOURNEY

The new requirements in the PCI DSS recognize this evolving threat and the critical role of script management in safeguarding payment data. Compliance now requires a proactive approach to script security to protect against data breaches. This includes implementing robust monitoring and control measures to ensure that scripts do not become a weak link in payment card data security.

Different approaches can be taken to mitigate the eSkimming risk associated but it is imperative that you understand they are not all created equal.

The PCI DSS references the use of both Subresource Integrity (SRI) and Content Security Policy (CSP) controls as potential ways to address 6.4.3 and 11.6.1 - both would require extensive design from your internal teams, the introduction of other solutions to address other aspects of the requirements, and time consuming, costly and difficult management. Not only that, a majority of players in the industry agree that these controls are inadequate in the face of evolving cyber criminal tactics.

It is for that reason, that 80 members of the "eCommerce Guidance Taskforce," which was created by the PCI Security Standards Council, warned of reliance on SRI and CSP in a recently published information supplement titled "Payment Page Security and Preventing e-Skimming" Specifically, the following warnings were issued:

Disadvantages of SRI

- SRI is not practical for rapidly changing scripts or content that changes unpredictably (for example, dynamic third-party scripts).
- SRI fails silently—there is no native alert mechanism to inform website owners if a script was blocked.
- SRI does not support reporting.

Disadvantages of CSP

- The entity will need to implement additional processes for authorization, alerting, tracking header changes, etc. For example, CSP by itself cannot create a list of unauthorized scripts or alert on changes to security -impacting HTTP headers.
- CSP does not maintain a baseline of normal activity. It is static and cannot track historical or expected states across sessions.
- Maintaining a robust CSP (especially with hashes) can be challenging in dynamic environments.

- CSP is not inherently able to detect deletions of security-impacting headers or confirm whether a malicious script changed its internal functionality unless it also contacts disallowed domains.
- CSP does not provide any native reporting mechanisms. Browsers will generate reports when problems occur, but it is the responsibility of the person implementing CSP to acquire or develop their own system to collect and process reports.

A “do-it-yourself” approach to the problem is going to leave you spending a fortune on a solution that is anything but…and the prospect of taking this on makes little sense when proven solutions exist which address all aspects of requirements 6.4.3 and 11.6.1.

In addition to CSP and SRI, the PCI DSS allows for the use of proprietary script management solutions, such as the pioneering Source Defense platform. This offers another, far more attractive option by providing a comprehensive framework for managing and securing scripts with push button compliance reporting built in.

Source Defense is proven effective and trusted by more than 1,000 of the world’s leading brands, by massive players in the PSP and eCommerce platform ecosystem, and by hundreds of the world’s leading QSAs. Source Defense is easy to deploy, incredibly cost effective, and places no additional burden on your overly burdened teams.

We’ll explore more about the Source Defense solution later in this eBook.

> **CSP is a directive to the browser that tends to break stuff quite often..**
> -Senior QSA from top company.

```
r console.log(''alew');
nction al (){
r getElementById('innerHTML = el;
  innerHTML = r;
turh c;
<scrript>alert('...)script>
```

LAST MINUTE CHANGES, CONFUSION & CLARIFICATION

UNDERSTANDING CHANGES TO SELF ASSESSMENT QUESTIONNAIRE A (SAQ-A)

Despite giving the industry a two year grace period for implementing these new eSkimming controls, a number of concerns raised at the last minute caused the PCI Security Standards Council to introduce some significant changes to scope which left many confused and uncertain of how to proceed. They have since clarified these changes in a series of updates. We break them down here for you to understand so that you know the impact to your organization and to the Merchants you serve.

As a PSP or eCommerce Platform Provider - ***NOTHING CHANGES*** for you directly. You must comply with 6.4.3 and 11.6.1.

That said, in February of 2025, the PCI Security Standards Council issued changes to both eligibility requirements, and compliance requirements for **Merchants** reporting under Self-Assessment Questionnaire A (SAQ-A). In order to ***BE ELIGIBLE*** as a SAQ-A Merchant, the following must now be true:

SAQ A merchants confirm that, for the eCommerce payment channel

1. The merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions;
2. All processing of account data is entirely outsourced to PCI DSS compliant third-party service provider (TPSP)/payment processor;
3. The merchant does not electronically store, process, or transmit any account data on merchant systems or premises, but relies entirely on a TPSP(s) to handle all these functions;
4. The merchant has confirmed that TPSP(s) are PCI DSS compliant for the services being used by the merchant;
5. Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically.

Additionally, for e-commerce channels:

6. All elements of the payment page(s) /form(s) delivered to the customer's browser originate only and directly from a PCI DSS compliant TPSP/payment processor.
7. The merchant has confirmed that their site is not susceptible to attacks from scripts that could affect the merchant's e-commerce system(s).

IF all of these hold true, a Merchant may report under SAQ-A and the explicit controls outlined under **6.4.3 and 11.6.1 are NOT required**. ***HOWEVER***…in order to meet item number 7 above, the following must be true (as clarified by the PCI Security Standards Council in FAQ 1588):

"The merchant can confirm that the merchant's webpage is not susceptible to script attacks by either:

> *Using techniques such as, but not limited to, those detailed in PCI DSS Requirements 6.4.3 and 11.6.1 to protect the merchant's webpage from scripts targeting account data. These techniques may be deployed by the merchant or a third party."*

So - basically, comply with 6.4.3 and 11.6.1 or…

> *"Obtaining confirmation from the merchant's PCI DSS compliant Third-Party Service Providers (TPSPs)/payment processor providing the embedded payment page/form(s) that, when implemented according to the TPSP's/payment processor's instructions, the TPSP's/payment processor's solution includes techniques that protect the merchant's payment page from script attacks."*

A lot of confusion, and perhaps even more confusion in the clarification - with the end result being that either your Merchants adopt 6.4.3 and 11.6.1 controls OR they turn to you for a solution if you have one…

Thus, the introduction of an opportunity to differentiate yourself and capture added revenue if you so wish…

SUPPORTING YOUR MERCHANTS

AN OPPORTUNITY FOR COMPETITIVE ADVANTAGE AND INCREASED REVENUE

Many eCommerce Merchants - especially small Merchants—are overwhelmed by PCI DSS 4.0.1’s technical requirements, particularly around script management (6.4.3) and tamper detection (11.6.1). As their PSP or eCommerce platform provider, you’re in a unique position to simplify this journey for them:

- Start with **your own compliance** - it is required as a TPSP and your Merchants will require documentation of your compliance to support their own compliance. Don’t delay any further, get this taken care of now
- Provide **documentation and attestation** proving that your platform meets PCI 4.0.1 controls, enabling merchants to maintain SAQ-A eligibility - the clock is ticking
- Deliver **implementation guidance** to reduce the risk of misconfigurations that might otherwise jeopardize compliance.
- Consider offering **a solution to help your Merchant clients address 6.4.3 and 11.6.1**

As we learned above, changes to SAQ-A eligibility mean that in order to stay SAQ-A eligible, Merchants must be able to attest to the fact that their websites are not susceptible to eSkimming attacks. They can do so by working with Source Defense directly - OR by turning to their PSP or eCommerce Platform provider for a solution that has controls like Source Defense built in.

Source Defense is not only the pioneer in eSkimming security, its not only trusted by more than 1,000 of the world’s largest brands…it is also a proud partner to PSPs and eCommerce Platform providers.

We have been a member of the PCI Small Merchant Taskforce, have solutions designed specifically for the needs of small Merchants, and are currently engaged in the largest rollout in the industry for this community - addressing the needs of a universe of millions of small merchants. We can build something to help you, help your clients - and we’re ready to talk!

Stand Out as a Trusted, Security-Focused Partner

When every provider claims to be "secure," demonstrating tangible compliance support for PCI DSS 4.0.1 can set you apart. By publicly aligning your platform with the latest requirements—and going a step further to support Merchant-side security—you present yourself as a forward-thinking, trustworthy partner in a threat-filled landscape.

Security-conscious merchants will gravitate toward providers who can:

- Help them **reduce compliance scope and effort**
- Help them **maintain eligibility** for SAQ-A.
- Provide embedded defenses against eSkimming as a **core feature** of your platform.
- Prevent costly **eSkimming attacks and reputational damage**

Unlock New Revenue Opportunities

Forward-thinking PSPs are already packaging security and compliance capabilities as premium features:

- **Bundle eSkimming security and compliance tools,** such as Source Defense, as value-added services.
- Offer **tiered pricing** based on compliance level and threat monitoring sophistication.
- Provide **merchant dashboards** for script inventory and tamper alerts, turning compliance into a visible, ongoing benefit

Being seen as a compliance ally—not just a payment processor—can become a core pillar of your value proposition. Helping your merchants meet PCI DSS 4.0.1 isn't just good business—it can become a line of business.

> **Seeing risk with clear eyes leads to the best outcomes. Rather than just seeking to achieve compliance with standards, [successful] organizations attempt to manage actual risk.**
>
> -Coalfire White Paper: A Holistic Approach to Protecting Credit Card Payment Flows

SOURCE DEFENSE

SET IT AND FORGET IT ESKIMMING SECURITY

Designed for PSPs, eCommerce Platform Providers and Millions of Merchants Around the Globe
Achieving PCI DSS 4.0.1 compliance and maintaining protection against eSkimming threats doesn't have to be complex, resource-intensive, or disruptive to your business. Source Defense offers a turnkey, behavior-based security platform purpose-built for payment service providers, eCommerce Platforms, and the Merchants they serve. It's the smarter, easier way to meet the mandate and secure against eSkimming - without the headaches.

Behavior-Based Protection That Works in Real Time and Evolves to Threats

Unlike static controls like Content Security Policy (CSP) or Subresource Integrity (SRI), Source Defense monitors and controls actual script behavior in the browser. That means:

- Real-time visibility into what scripts are running and what they're doing
- Automated blocking of suspicious or unauthorized activity
- No false sense of security - you're protected even with dynamic third and fourth-party scripts, and as attacks evolve

This proactive, behavior-based approach eliminates blind spots where eSkimming attacks typically occur—helping prevent data theft before it happens.

The Pioneer and Trusted Leader in eSkimming Security

- Created the eSkimming security market, bringing solutions to market in 2016 as these attacks first took hold
- Trusted by more than 1,000 of the world's leading brands to protect their eCommerce infrastructure
- Engaged with the PCI Council as an Associate Participating and Principal Participating Organization for years - helping shape the PCI DSS 4.0.1 requirements
- Trusted by hundreds of QSACs and thousands of QSAs around the globe
- Reviewed and endorsed by Coalfire and VikingCloud - the top two QSACs in the world
- Working with the world's largest PSPs and eCommerce Platform providers to deliver solutions for Level 3 and Level 4 Merchants
- Appointed to the PCI Board of Advisors for the 2025-2027 session to help shape global standards
- Certified as a PCI Compliant Service Provider via AoC reviewed by IBM

Fully Supports PCI DSS 4.0.1 Requirements

Source Defense's platform was designed from the ground up to align with and simplify compliance with PCI DSS 4.0.1 requirements 6.4.3 and 11.6.1:

- Automatically builds and maintains a script inventory
- Enables you to authorize and justify each script (6.4.3)
- Continuously monitors for tampering and unexpected changes (11.6.1)
- Issues alerts and blocks malicious activity in real time

And it does all of this with a simple deployment, minimal maintenance, and push button reporting - making it easy to demonstrate compliance during audits.

Built for Scale and Flexibility

Whether you're protecting a hosted payment page, an embedded iframe across thousands of merchants, or a white-label ecommerce solution with high transaction volumes, Source Defense scales with you. It's engineered for high-performance environments and designed to deliver:

- Out-of-the-box coverage for every payment page under your control
- Low management overhead (typically <1 hour/month)
- Customizable enforcement policies to fit your unique risk profile

With our "process by design" dashboards and automated script policy recommendations, security becomes a background function—not a bottleneck.

A Strategic Partner, Not Just a Security Vendor

We know that as a PSP or ecommerce platform provider, your reputation depends on delivering secure, reliable payment experiences. That's why we don't just give you tools—we provide:

- A 30-day action plan to achieve your own compliance
- Support for merchant enablement and education
- API integrations and analytics to align with your existing stack
- Custom design and pricing for Level 3 and 4 Merchants to help you drive revenue

We'll focus on stopping the skimmers. You focus on your core business. Together we can focus on your growth.

Schedule a Demo with a Security Expert Today!

https://sourcedefense.com/request-demo/