source DEFENSE

PCI DSS 4.0 - Payment Page Responsibility Whitepaper

***New** PCI DSS 4.0 requirements (6.4.3 and 11.6.1) call for enhanced security for web pages that contain credit card information or take online payments. The scope of PCI DSS 4.0 has been expanded to include payment pages as per the guidance of the PCI Council. This includes the use of iFrames and pages that completely redirect to a TPSP/payment processor.

The responsibility of ensuring compliance for payment pages falls to three key types of organizations to whom these rules apply:

- Merchants
- eCommerce Gateway application platform providers
- TPSP/Payment processors

PCI DSS 4.0 and SAQ-A/D definitions of a Payment Page:

- A webpage that contains payment fields for capturing payment information (e.g., credit card details) directly from a customer
- A webpage that incorporates payment fields embedded within an iframe provided by a payment processor
- A web page that redirects customers to a payment processor's page to complete the payment transaction.
- Any non-payment page that collects or requests cardholder data, such as a 'digital wallet' or account information page

Merchant Responsibilities:

For merchants complying with PCI DSS 4.0 and SAQ-A, requirements 6.4.3 and 11.6.1 apply to all payment flows, including:

Merchant Requirements	Merchant Pages with Merchant Hosted Fields	Merchant Pages with iFrame Payment Fields	Merchant Pages with URL Redirects
PCI DSS Req 6.4.3	✓	✓	✓
PCI DSS Req 11.6.1	✓	✓	✗

Regardless of the payment flow used, merchants are required to:

- Maintain an inventory of all scripts included on their payment pages.
- Justify the purpose of each script and why it is necessary for the payment process.
- Monitor the integrity of each script to ensure it has not been tampered with.
- Authorize each script to run on the payment page.

Detailed "Merchant Payment Page" scenarios

1. If a merchant utilizes a self-hosted solution, and thereby collects all payment information before sending the content to a payment processor, the merchant must apply the new PCI DSS 4.0 requirements 6.4.3 and 11.6.1 for their self-hosted payment page.

2. If a merchant utilizes a full payment redirect, the merchant is responsible for requirement 6.4.3 on the page that initiates the redirect to the payment processor. Requirement 11.6.1 does not apply to the merchant but it is required of the payment processor. 11.6.1 requires monitoring HTTP headers and the content of the payment page for any unauthorized changes. The purpose of this requirement, as outlined in the PCI applicability notes, is to prevent attacks on the payment page.

3. If a merchant utilizes an iframe-hosted solution, the merchant is responsible for requirements 6.4.3 and 11.6.1 on the page that contains the iframe. This requires monitoring HTTP headers and the content of the page that contains the iframe for any unauthorized changes. The purpose of this requirement, as outlined in the PCI applicability notes, is to prevent attacks on the page that contains the iframe which can affect payment card data through the manipulation of content outside of the TPSP-provided iframe.

TPSP/Payment Processor Responsibilities:

TPSP/Payment Processor Requirements	Merchant Pages with Merchant Hosted Fields	TPSP/Payment Processor iFrame Payment Fields	TPSP/Payment Processor Pages with Payment Fields
PCI DSS Req 6.4.3	✗	✓	✓
PCI DSS Req 11.6.1	✗	✓	✓

Impact on TPSPs:

TPSPs/payment processors are now held accountable to PCI DSS 4.0 requirements 6.4.3 and 11.6.1 for the payment pages they host. The TPSP/payment processors are responsible for understanding, authorizing, and monitoring any changes to the scripts included on their payment pages.

eCommerce Gateway Application Platform Responsibilities:

The expanded scope under PCI DSS 4.0 also presents a significant opportunity for eCommerce platforms to take a leadership role in securing the payment ecosystem. Under PCI DSS 3.2.1, the merchant nor the eCommerce application had any responsibility. The responsibility rested solely on the TPSP/payment processor.

Detailed eCommerce Gateway application responsibility break down

- If the eCommerce application does not allow their merchants to make any modification to these pages, then the eCommerce application can meet the PCI compliance and eliminate the merchant from scope.
- If the merchant is allowed to make changes, such as adding new scripts, the eCommerce application would be able to eliminate themselves from scope and transfer that burden to the merchant.

Summary:

The expansion of the PCI DSS scope to include payment pages beyond the traditional merchant-controlled environment necessitates collaboration between merchants, TPSPs/payment processors, and potentially the eCommerce Application platforms to ensure complete and proper compliance. It is crucial that all parties conduct a thorough assessment of the scope and clearly understand their respective responsibilities for all payment pages involved in a transaction.