REPORT URI

PCI DSS 6.4.3 & 11.6.1 Evidence Pack

Version 1v1

Last modified 23rd July 2026

> *This document was last modified on 23rd July 2026.*

This evidence pack (1v1) explains how Report URI helps you meet the PCI DSS 4.0 client-side security requirements — 6.4.3 and 11.6.1 — and the audit-ready evidence you can export for each. It is a practical reference, not compliance advice; your Qualified Security Assessor (QSA) remains the authority on what satisfies each requirement in your environment.

1. What this pack covers

PCI DSS 4.0 brought the browser into scope for payment pages. Requirement 6.4.3 governs authorising, assuring the integrity of, and inventorying every script on a payment page. Requirement 11.6.1 governs continuously detecting and alerting on unauthorised change to those pages. This pack maps each requirement to the Report URI capability that addresses it and the evidence you can export to demonstrate it.

2. The requirements in brief

PCI DSS v4.0.1, Requirement 6.4.3. All payment page scripts that are loaded and executed in the consumer's browser are managed as follows: a method is implemented to confirm that each script is authorized; a method is implemented to assure the integrity of each script; an inventory of all scripts is maintained with written business or technical justification as to why each is necessary.

PCI DSS v4.0.1, Requirement 11.6.1. A change- and tamper-detection mechanism is deployed to alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the security-impacting HTTP headers and the script contents of payment pages as received by the consumer browser; the mechanism is configured to evaluate the received HTTP headers and payment pages; and its functions are performed at least weekly, or periodically at a frequency defined in the entity's targeted risk analysis.

3. Requirement 6.4.3 — evidence mapping

6.4.3 element	Report URI capability	Evidence you can export
A method to confirm each script is authorised	Content Security Policy (report-only or enforcing) with a reporting endpoint, plus Script Watch	Script inventory showing authorised sources; CSP violation reports for any unauthorised script, with timestamps
A method to assure the integrity of each script	Subresource Integrity (baseline); CSP Integrity and Integrity Policy to enforce and report SRI coverage	Reports of scripts loaded without SRI; a record that integrity enforcement is in place
An inventory of all scripts with written justification	Script Watch continuous, timestamped inventory per site	Exportable script inventory with first-seen timestamps, to which you attach your business or technical justifications

4. Requirement 11.6.1 — evidence mapping

11.6.1 element	Report URI capability	Evidence you can export
Alert on unauthorised change to security-impacting HTTP headers	Policy Watch	Change log of CSP and security-header changes, with timestamps and alert history
Alert on unauthorised change to payment page script contents	Script Watch, with Data Watch for exfiltration behaviour	Script change log; new-destination and anomaly alerts
Evaluate the received HTTP headers and payment pages	CSP violation reporting via the report-to / report-uri directives	CSP violation report stream captured from real consumer browsers
Perform the checks at least weekly, or per targeted risk analysis	Continuous monitoring — every affected page load is a check	Continuous monitoring record covering the full assessment period, which exceeds the weekly minimum

5. Producing and exporting the evidence

Deploy a Content Security Policy with a Report URI reporting endpoint on your payment page and enable Script Watch, Policy Watch and Data Watch for that site. A report-only policy is sufficient for compliance — it authorises your known-good scripts and reports anything unauthorised without blocking; moving to an enforcing policy is stronger protection you can adopt at your own pace, but it is not required. From your dashboard you can then export the script inventory, the change logs, and the CSP violation history for any period to hand to your assessor.

6. Readiness checklist

Requirement 6.4.3 — authorise, assure integrity, inventory

- Inventory every script on the payment page and remove anything without a written justification
- Authorise the scripts that remain with a Content Security Policy (report-only is sufficient)
- Assure script integrity with Subresource Integrity; optionally enforce SRI coverage with CSP Integrity or Integrity Policy
- Record a business or technical justification for each remaining script

Requirement 11.6.1 — detect and evidence change

- Add a reporting endpoint to your CSP so violations are captured from real browsers
- Enable Script Watch, Policy Watch and Data Watch alerts for the payment page

- Set an appropriate alert threshold and notification address for each watcher
- Confirm you can export the inventory, change logs and violation history for the assessment period

7. What this covers, and what it doesn't

Report URI covers	Doesn't replace
Script inventory and change detection	Penetration testing
CSP violation reporting and logging	Secure code review
Behavioural data exfiltration monitoring	WAF or edge security
Audit-ready evidence generation	Vulnerability remediation

8. Learn more

- Guide: PCI DSS 6.4.3 & 11.6.1 client-side security
- How Report URI helps: PCI DSS Compliance
- Step-by-step docs: Compliance guides