



# HUMAN PCI DSS Compliance by Client-side Defense

## Streamline Payment Page Script Management

Payment Card Industry Data Security Standard (PCI DSS) 4.0 is live. Online merchants who accept payment cards must meet new client-side payment page protection requirements by March 31, 2025.

To protect cardholder data from the risks introduced by scripts, **requirement 6.4.3** states that all payment page scripts 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 justification as to why each is necessary.

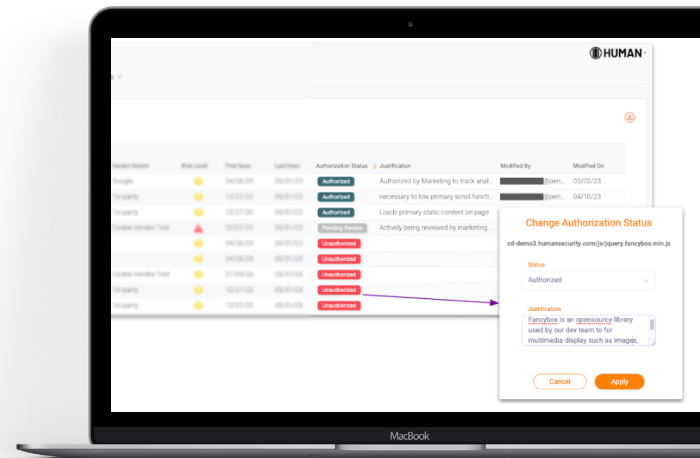
To further protect from skimming, **requirement 11.6.1**<sup>1</sup> states that a change- and tamper-detection mechanism is deployed as follows:

- To alert personnel to unauthorized modification to the HTTP headers and the contents of payment pages as received by the consumer browser.

Even merchants who fully outsource payment processing to third-party payment service providers must implement these requirements.

### Benefits

- Simplify compliance with the payment page script management requirements of PCI DSS 4.0
- Authorize and justify scripts for their business value, while blocking their access to cardholder data
- Base business, security, and compliance decisions on scripts' actual behavior in your real consumers' browsers



Client-side Defense streamlines payment page script management for PCI DSS 4.0, by auto-maintaining the script inventory, recording authorization and justification, and assuring the integrity of scripts as received in your real consumers' browser.

**“The solution pays for itself by reducing our risk from client-side data breaches and helping avoid fines and the subsequent negative impact to our brand.”**

— CISO, Top 5 Global Airline



<sup>1</sup>Please find the complete requirements at [https://www.pcisecuritystandards.org/documents/PCI-DSS-v4\\_0.pdf](https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf).

# HUMAN Client-side Defense for PCI DSS 4.0 Compliance simplifies payment page protection and script management

Modern websites rely on dynamically sourced code from across the Internet, which may bypass security controls and put user data at risk. HUMAN simplifies cardholder data protection in compliance with the relevant PCI DSS 4.0 requirements.

Deploy a single line of JavaScript to receive a risk-scored inventory of all scripts, a simple method to authorize and justify scripts, and audit reports to demonstrate your compliance. The solution will alert on unauthorized changes and risky script behavior, enable investigation, and surgically block undesired actions at-a-click.

## Break the Tradeoff Between Script Value and Risk

PCI DSS 4.0 introduces a dilemma: do you authorize and justify important scripts that access cardholder data at will?

With HUMAN, you can benefit from scripts' business value, while mitigating their inherent risk. You can authorize, justify, and enable the normal operation of scripts, while blocking their access to cardholder data.

As a result, your GRC and Security teams can spend more time on other threats, while enabling your business and developers to leverage third-party scripts freely.

---

## How it Works

*Deploy a simple Javascript snippet (tag)*



### PROTECT

The HUMAN Sensor automatically inventories scripts, assures their integrity, enables authorization and justification, and blocks undesired cardholder data access (6.4.3)



### DETECT

The HUMAN Sensor runs in your real consumers' browsers to detect tampering and unauthorized changes, and alert on unauthorized modification to the HTTP Headers (11.6.1)



### COMPLY

The cloud back-end and UI provide not only visibility, intelligence, and one-click-mitigation, but also evidence of compliance for on-demand audit reports.

---

## About HUMAN

HUMAN is a cybersecurity company that protects organizations by disrupting digital fraud and abuse. We leverage modern defense to disrupt the economics of cybercrime by increasing the cost to cybercriminals while simultaneously reducing the cost of collective defense. Today we verify the humanity of more than 20 trillion digital interactions per week across advertising, marketing, e-commerce, government, education and enterprise security, putting us in a position to win against cybercriminals. Protect your digital business with HUMAN.

**To Know Who's Real, visit [www.humansecurity.com](http://www.humansecurity.com).**