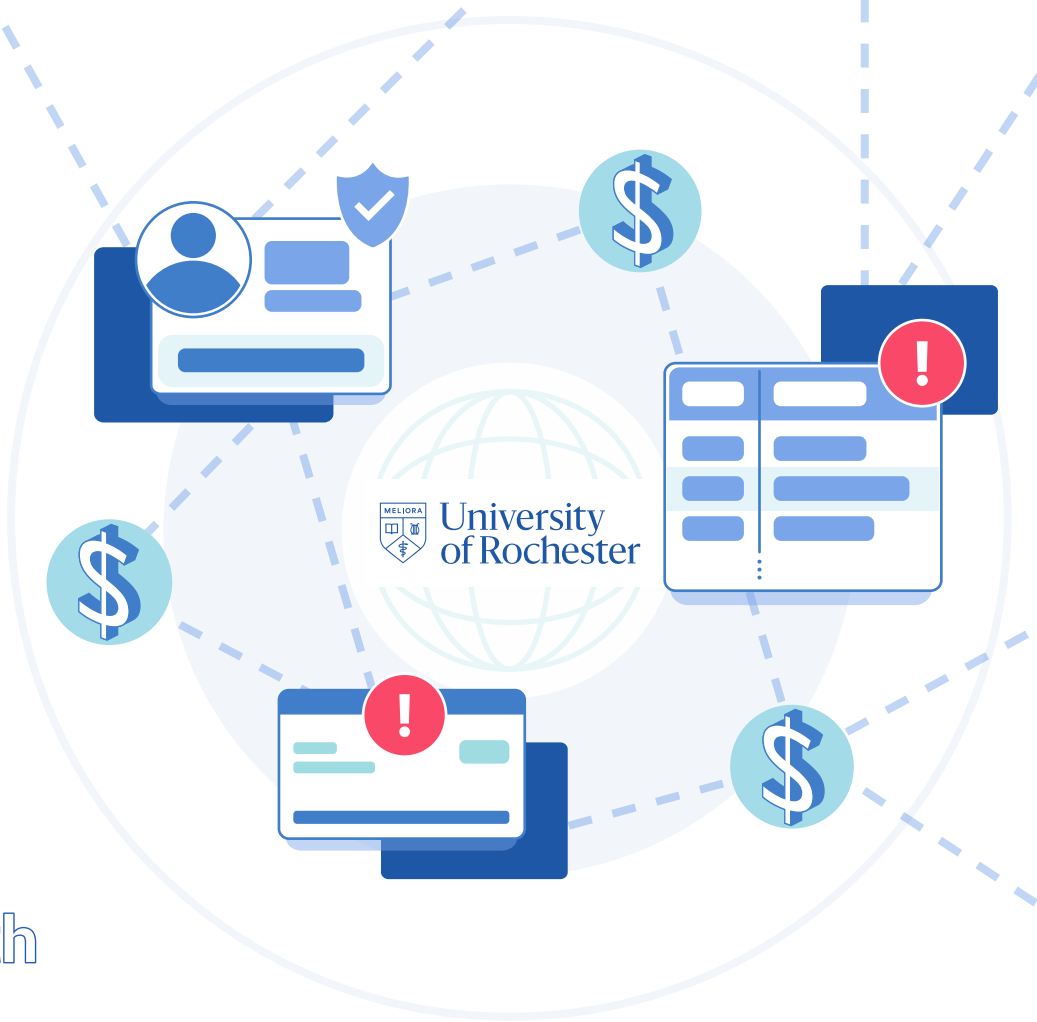


DataStealth

Case Study: University of Rochester

PCI DSS v4.0 Compliance Across a Decentralized Payment Environment, Zero Code Changes

datastealth.io | info@datastealth.io

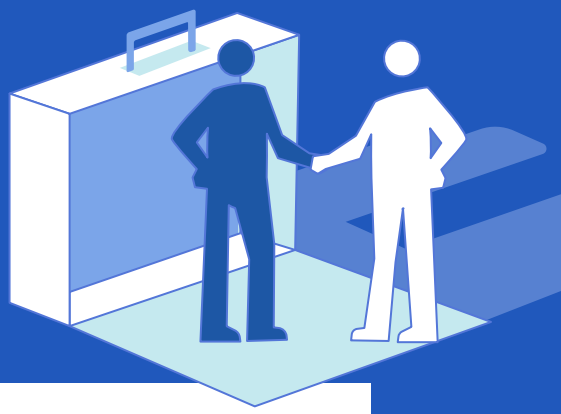
Executive Summary

As a premier research institution with an academic medical center, the University of Rochester manages a complex web of e-commerce touchpoints, from tuition payments, athletic and concert ticketing, cafeterias, parking, to patient payments.

With the arrival of PCI DSS v4.0, the University faced the challenge of meeting new, stringent mandates for script integrity (6.4.3) and tamper detection (11.6.1) without disrupting its vast ecosystem of payment partners and legacy applications.

In response, the University of Rochester achieved a clear, no-friction compliance victory by implementing DataStealth's eSkimming Protection solution.

Because the platform operates via a simple DNS update, the University secured its payment pages and minimized its audit scope without needing to rewrite a single line of code or alter any third-party workflows.



Customer Profile

Customer	University of Rochester
Sector	Higher Education (R1 Research University) with an academic medical center
Payment Environment	Multiple e-commerce sites across the university, including 17 payment pages inside URMC alone
Core Challenge	PCI DSS v4.0 compliance — Requirements 6.4.3 and 11.6.1
Solution	DataStealth eSkimming Protection
Deployment Model	DNS-level, zero code changes
G2 Rating	5 out of 5

The Challenge

Requirements 6.4.3 and 11.6.1

In recent years, e-skimming (also known as Magecart or Formjacking) has become a rapidly growing data-breach risk in e-commerce environments.

E-skimming attacks target online payment transactions by interfering with or manipulating the scripts running in the consumer's web browser. Because modern e-commerce platforms rely heavily on external and third-party scripts (for functionality, analytics, and marketing), these scripts create a broad attack surface for the theft of payment card data.

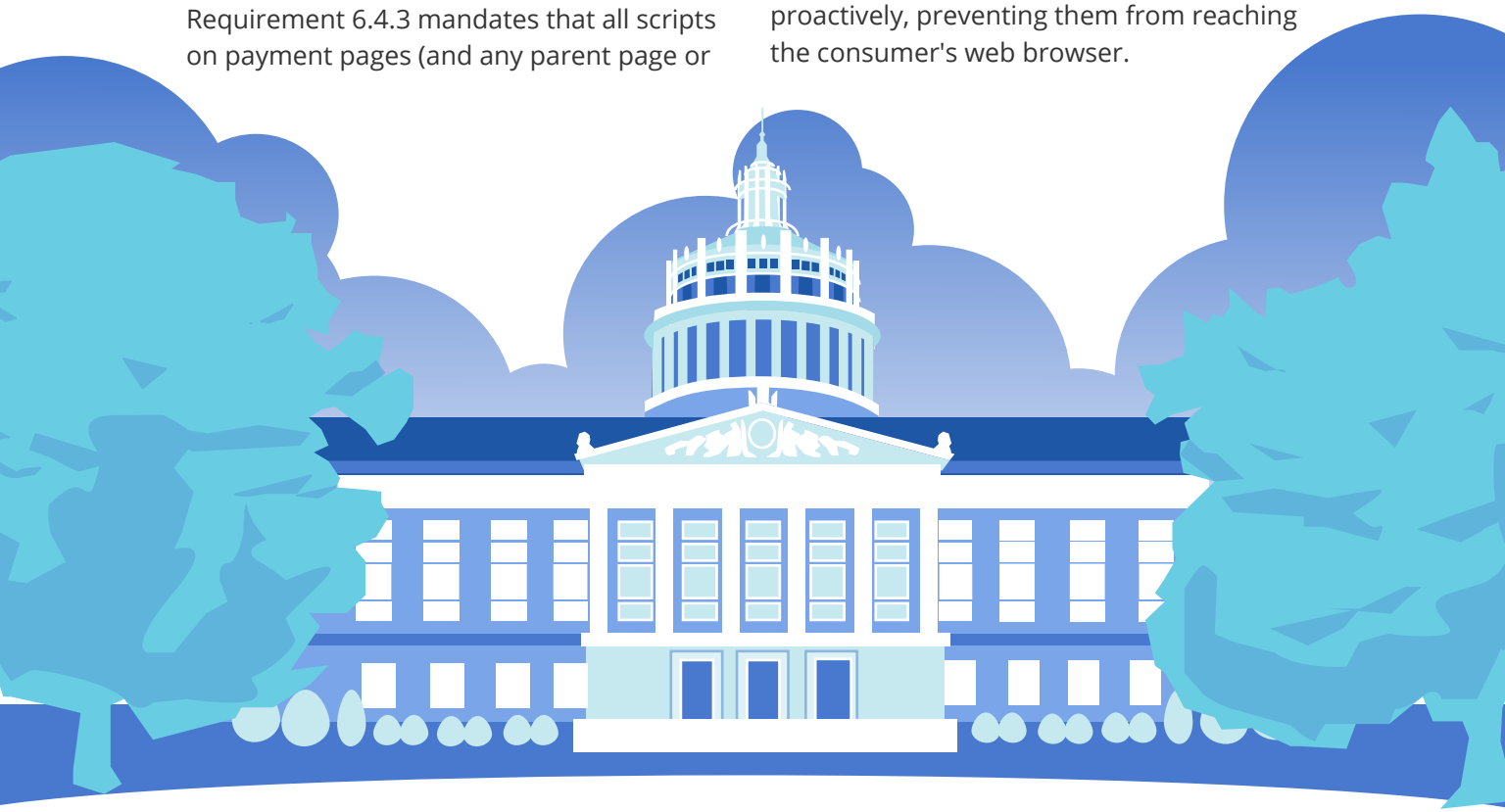
To help e-commerce organizations reduce their vulnerability, the PCI Council mandated two key inclusions for PCI DSS v4.0 compliance, effective April 2025: requirements 6.4.3 and 11.6.1.

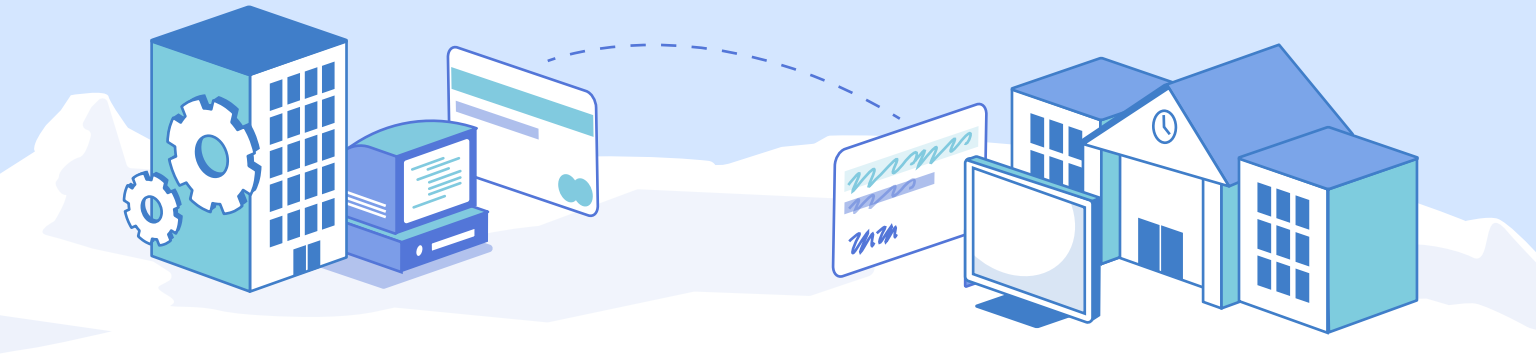
Requirement 6.4.3 mandates that all scripts on payment pages (and any parent page or page linking to the payment page) must be explicitly authorized, justified, and monitored for integrity before they are delivered to a consumer's browser.

So, a university's marketing team might add tracking pixels for analytics, or the IT team may deploy new libraries. However, manually maintaining the authorization, justification, and monitoring work for these changes is a logistical nightmare.

Requirement 11.6.1 mandates a change-and-tamper detection mechanism for HTTP headers and payment page scripts at least every seven days.

Traditional browser-based tools may fail to detect malicious scripts that load early and conceal themselves from detection mechanisms. By validating content at the delivery layer, unauthorized modifications can be detected, alerted, and/or blocked proactively, preventing them from reaching the consumer's web browser.





The Environment

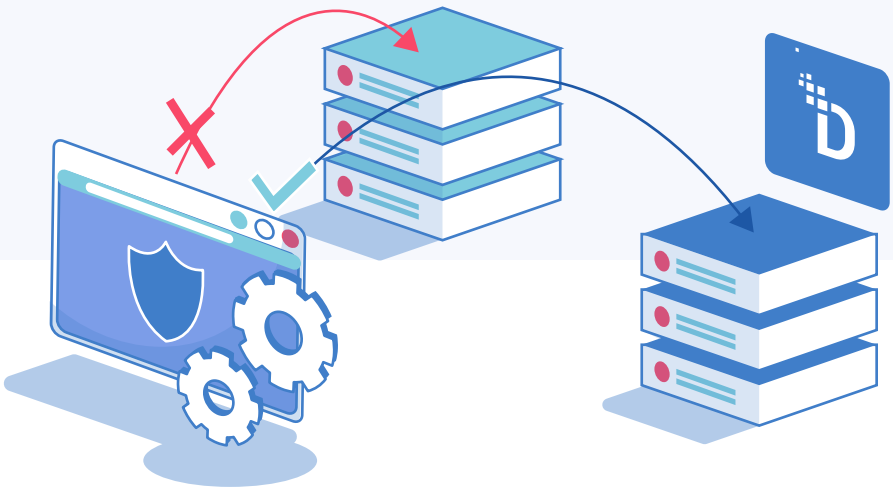
The University's payment infrastructure comprises multiple payment pages distributed across internal schools or organizations, several with their own internal IT department.

Traditional code/agent/API-dependent solutions for the new PCI requirements were difficult to implement across the entire environment. DataStealth's ability to operate at the network layer allowed the University to deploy a scalable security solution, one that not only covered its full system (across many pages and organizations) but did not trigger lengthy or complicated work for its internal IT teams. This made deploying a solution for PCI compliance much easier.

The Solution: Pre-Emptive Delivery Protection

DataStealth operates at the network layer. By rerouting traffic through the DataStealth platform using a simple DNS update, the University formed a pre-emptive security layer that intercepts threats long before they take hold and affect the consumer.

DataStealth acts as a real-time guardian, neutralizing malicious headers and scripts at the edge to ensure only authorized content is ever delivered to a browser.



The Outcomes

PCI DSS v4.0 Compliance With Reduced Audit Scope

The University achieved PCI DSS v4.0 compliance with a greatly reduced audit scope, more analogous to SAQ A.

DataStealth neutralizes script-based risks at the delivery layer, thereby technically making both requirements 6.4.3 and 11.6.1 “Not Applicable” for the University’s internal environment.

The responsibility for continuous monitoring and tamper detection was shifted to DataStealth’s PCI-compliant infrastructure, significantly simplifying the University’s compliance posture.

Stayed With Preferred Payment

The University continues to work with its preferred third-party payment providers. DataStealth’s solution is vendor-agnostic, seamlessly protecting iFrames and redirected payment flows from external providers by ensuring the integrity of the "navigational flow" leading to the transaction.

Partners Continuous Script Inventory,

DataStealth maintains a live map of the scripts authorized on each protected payment page. Anything that appears outside that map, inline, first-party, third-party, or Nth-party, is flagged and surfaced to the university's team for review.

The University gains a continuous, auditor-defensible record of what is running on its payment pages and what has changed, without interfering with any of its applications.

No Code Changes, No Downtime

The University achieved PCI DSS v4.0 compliance with a greatly reduced audit scope, more analogous to SAQ A.

DataStealth neutralizes script-based risks at the delivery layer, thereby technically making both requirements 6.4.3 and 11.6.1 “Not Applicable” for the University’s internal environment.

The responsibility for continuous monitoring and tamper detection was shifted to DataStealth’s PCI-compliant infrastructure, significantly simplifying the University’s compliance posture.

Next Steps

Ready to Simplify Your PCI DSS v4.0 Compliance Work?

The University of Rochester reduced its audit scope, eliminated code changes, and achieved continuous script protection, all through DNS updates.

If your organization manages multiple payment pages across decentralized teams, DataStealth can help you meet Requirements 6.4.3 and 11.6.1 without disrupting your existing payment partners or burdening your IT staff.

Book a 15-minute compliance assessment to see how DataStealth can map your current payment page exposure and identify the fastest path to compliance, with zero code changes.