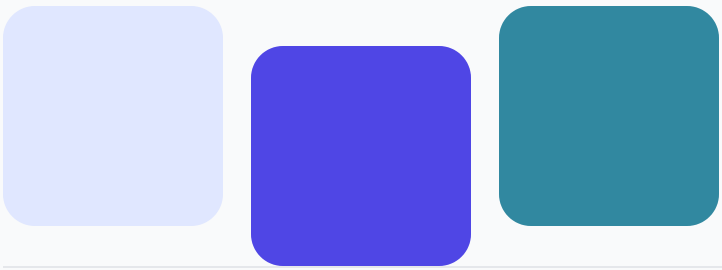
HIGHER EDUCATION · PCI DSS V4.0

University of Rochester

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



EXECUTIVE SUMMARY

As a premier research institution with an academic medical center, the University of Rochester manages a complex web of e-commerce touchpoints — tuition payments, athletic and concert ticketing, cafeterias, parking, and patient payments. With PCI DSS v4.0, the University faced new mandates for script integrity (6.4.3) and tamper detection (11.6.1) without disrupting its vast ecosystem of payment partners and legacy applications.

The University achieved a clear, no-friction compliance victory by implementing DataStealth's eSkimming Protection — operating via a simple DNS update, securing payment pages and minimizing audit scope without rewriting a single line of code.

CUSTOMER PROFILE

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

THE CHALLENGE – REQUIREMENTS 6.4.3 AND 11.6.1

E-skimming (Magecart or formjacking) has become a rapidly growing data-breach risk. E-skimming attacks target online payment transactions by interfering with scripts running in the consumer's browser — modern e-commerce's reliance on external scripts creates a broad attack surface for card data theft.

Requirement 6.4.3

All scripts on payment pages (and any parent/linking page) must be explicitly authorized, justified, and monitored for integrity before delivery to a consumer's browser.

Requirement 11.6.1

A change-and-tamper detection mechanism for HTTP headers and payment page scripts is mandated at least every seven days.

THE SOLUTION — PRE-EMPTIVE DELIVERY PROTECTION

DataStealth operates at the network layer. By rerouting traffic through the platform via a simple DNS update, the University formed a pre-emptive security layer that intercepts threats before they take hold — neutralizing malicious headers and scripts at the edge so only authorized content is ever delivered to a browser.

The University's payment infrastructure spans multiple payment pages distributed across internal schools and organizations, several with their own IT department. Traditional code/agent/API-dependent solutions were difficult to implement across the entire environment — DataStealth's network-layer approach covered the full system without triggering lengthy work for internal IT teams.

The Outcomes

Reduced Audit Scope

Compliance more analogous to SAQ A; requirements 6.4.3 and 11.6.1 become "Not Applicable" internally.

No Code Changes, No Downtime

Monitoring and tamper detection responsibility shifted to DataStealth's PCI-compliant infrastructure.

Stayed With Preferred Partners

Vendor-agnostic — seamlessly protects iFrames and redirected payment flows.

Continuous Script Inventory

A live map of authorized scripts; anything outside it is flagged for review.

Ready to simplify your PCI DSS v4.0 compliance work?

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