HIGHER EDUCATION

PCI DSS v4.0 across a decentralized payment environment

How the University of Rochester met Requirements 6.4.3 and 11.6.1 across dozens of payment pages with zero code changes.

CUSTOMER **UNIVERSITY OF ROCHESTER**
SECTOR **HIGHER EDUCATION**
CAPABILITY **ESKIMMING PROTECTION**

© 2026 DataStealth Inc. All Rights Reserved.

01 · EXECUTIVE SUMMARY

Compliance without friction

As a premier research institution with an academic medical centre, 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 eSkimming Protection, operating via a simple DNS update, securing payment pages and minimizing audit scope without rewriting a single line of code.

ATTRIBUTE	DETAIL
Sector	Higher education, R1 research university with an academic medical centre
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

© 2026 DataStealth Inc. All Rights Reserved.

02 · THE CHALLENGE

Requirements 6.4.3 and 11.6.1

E-skimming, also known as Magecart or formjacking, has become a rapidly growing data breach risk. These attacks target online payment transactions by interfering with scripts running in the consumer browser, and modern e-commerce 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 or linking page, must be explicitly authorized, justified, and monitored for integrity before delivery to a consumer 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 STRUCTURAL PROBLEM

The University payment infrastructure spans multiple payment pages distributed across internal schools and organizations, several with their own IT department. Traditional code, agent, or API dependent solutions were difficult to implement across the entire environment.

© 2026 DataStealth Inc. All Rights Reserved.

03 · 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 network layer approach covered the full system without triggering lengthy work for internal IT teams, which mattered in an environment where individual schools and organizations run their own technology functions.

04 · THE OUTCOMES

What the University achieved

Reduced audit scope

Compliance is more analogous to SAQ A, and Requirements 6.4.3 and 11.6.1 become Not Applicable internally.

No code changes, no downtime

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

Stayed with preferred partners

Vendor agnostic, seamlessly protecting iframes and redirected payment flows.

Continuous script inventory

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

© 2026 DataStealth Inc. All Rights Reserved.

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.

- Deployed via a DNS update
- No code changes anywhere
- 6.4.3 and 11.6.1 addressed
- Works with existing payment partners

Book a 15 Minute Assessment

© 2026 DataStealth Inc. All Rights Reserved.