Shumaker

MAY 8, 2026 | PUBLICATION

Client Alert: Instructure Data Breach: What Business Leaders Need to Know

On April 30, 2026, Instructure—the company behind Canvas, the leading learning management system in North America—disclosed a major cybersecurity incident. Canvas supports roughly 41 percent of higher education institutions on the continent and thousands of K–12 districts, making this one of the most consequential breaches that has ever impacted the education sector.

INDUSTRY SECTOR

Public Sector
Technology

SERVICE LINE

Technology, Data Privacy, Cybersecurity & AI

RELATED PROFESSIONALS

C. Jade Davis

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

The extortion group ShinyHunters has claimed responsibility, alleging the theft of approximately 3.65 terabytes of data—roughly 275 million records tied to students, teachers, and staff at nearly 9,000 institutions worldwide. The exposed information reportedly includes names, email addresses, student ID numbers, and private messages sent through Canvas. Instructure has stated that, to date, there is no evidence that passwords, dates of birth, government identifiers, or financial information were accessed.

Instructure's Response

Instructure's Chief Information Security Officer, Steve Proud, has confirmed that the company believes the incident is contained. The response has included deploying security patches, revoking privileged credentials and access tokens, rotating application keys, and enhancing monitoring across its platforms. Canvas and most associated services are back online, though some systems—including Canvas Test—remain under maintenance. Instructure continues to work with outside forensic experts and law enforcement.

The Threat Landscape

ShinyHunters has issued a "pay or leak" ultimatum, threatening to release the stolen data if its demands are not met. The group has a well-documented record of targeting major organizations, with recent breaches linked to Salesforce, Infinite Campus, McGraw Hill, Rockstar Games, and several Ivy League universities. Notably, this is the second time in roughly eight months that ShinyHunters has compromised Instructure; in September 2025, the group used a social engineering attack to breach the company's Salesforce environment.

Key Risks for Affected Institutions

The nature of the stolen data significantly increases the risk of targeted phishing. Because the exposed information includes private messages referencing real courses and conversations, attackers can craft highly convincing communications aimed at students, faculty, and staff. As cybersecurity experts have cautioned, the next wave of phishing will not be generic—it will reference real courses and real conversations, making it far more likely to succeed.

On the regulatory front, affected institutions face substantial compliance obligations. Because Canvas serves K–12 districts, colleges, universities, and education ministries, the breach implicates federal laws such as the Family Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Act (COPPA), along with roughly 130 state student-privacy statutes. Most of these frameworks place the notification burden on the institution rather than the vendor, so affected schools and universities will need to quickly assess what they owe their communities.

How Our Firm Can Help

Given the scale of this breach, any institution that relies on Canvas or other Instructure products should promptly evaluate its exposure. Shumaker's privacy, data security, and litigation teams are ready to help clients assess potential exposure and risk; advise on regulatory and notification obligations under FERPA, COPPA, and applicable state laws; coordinate with Instructure and third-party forensic experts; develop communications for students, staff, and other stakeholders; and implement additional data security and privacy safeguards.

If you have questions about this incident or need support with client communications or incident response, please reach out to our Technology, Data Privacy, Cybersecurity & AI team. We are closely monitoring developments and will continue to provide guidance as the situation evolves.

Shumaker