Insights, News & Events

THE CANVAS BREACH: WHAT EDUCATIONAL INSTITUTIONS NEED TO KNOW AND HOW YOU CAN RESPOND

Insights
May 8, 2026

The Canvas Breach: What Educational Institutions Need to Know and How You Can Respond

The public learned on May 7 that Instructure, the company that manages Canvas, suffered a massive data breach that could impact a huge swath of schools and students across the country. Canvas is the most widely employed ed-tech platform in the US, used by 41% of educational institutions and tens of millions of students. Here's what we know about the breach and the immediate steps your school should consider taking now.

What Happened

ShinyHunters, a well-known threat actor which has repeatedly targeted the education industry, breached Instructure's systems on April 25. The hacking group claims to have stolen over 275 million records – names, email addresses, student ID numbers, and private messages. The data is over 4 terabytes and covers over 9,000 schools. ShinyHunters has threatened to release the data if Instructure fails to pay ransom by May 12.

Additionally, some educational institutions that use Canvas have reported that they have received their own ransom messages when logging onto the platform, with the threat actor demanding that they pay ransom to prevent their students' data from being released.

Related People

Logan S. Booth, CIPP/US

Of Counsel

720.644.2889

Jennifer B. Carroll

Partner, Co-chair K-12 Institutions

What Steps Has Instructure Taken

According to Instructure, they contained the breach on May 5. The company is disputing the scope of information that was stolen, claiming that there is no evidence that financial information, government IDs, or student passwords were compromised.

ShinyHunters has publicly stated that Instructure is not negotiating and has threatened the company with a "PAY OR LEAK" warning. As of the evening of May 7, Canvas was inoperable, although it's not immediately clear what caused this most recent outage.

What Schools Should Do

Given the scope and scale of the attack, the nature of the potentially compromised information, and the fact that the information may contain student data, it is a virtual certainty that a myriad of legal action will follow. Your school needs to be thinking about what comes next.

Short-Term Action

In the short term, your stakeholders will demand to know what happened, when you learned about it, and what you did to prevent further harm. If the threat actor ultimately releases the data, you're going to face a torrent of inquiries from your students, parents, community, and faculty about how they should respond. All of this requires dynamic and responsive communication that can be operationalized as events unfold.

Additionally, if ShinyHunters has demanded ransom from your school, there are additional requirements to navigate. Law enforcement may need to be notified, cyber insurance policies may be triggered, and your institution will need to decide how to proceed with respect to the threat actor's demands.

After-Action Steps

Once the imminency of the crisis has abated, your school should conduct an after-action report. Educational institution leaders will need to address the following questions over the summer to ensure that your school is ready for when students return in the fall:

954.847.4716

Daniel Pepper, CIPP/US

Partner

303.218.3661

Kristin L. Smith

Partner, Co-chair K-12 Institutions

713.292.5621

Shiloh Theberge

Partner, Chair Higher Education

207.477.7004

- Were there any steps you could have taken to enhance protection of your data on Canvas?
- Will you maintain your relationship with Instructure?
- Will you require any additional protections from Instructure if you do maintain your relationship?
- How should you evaluate the other ed-tech platforms that you use to mitigate the risks of future harm?

Longer-Term Actions

In the longer term, class action lawsuits are likely. Data privacy and cybersecurity laws in the US are a patchwork of federal, state, and local regulations, and the pervasiveness of Canvas's utilization means that parties across a range of jurisdictions will have causes of action. While Instructure will surely be a major target of any litigation, plaintiffs' attorneys often include a wide spectrum of potential defendants in their pleadings to see where liability sticks. It's likely that schools will also be named in suits, under the theory that they could, and should, have done more to protect student information.

At the same time, schools themselves may have a cause of action against Instructure, if the company's negligence contributed to the success of the attack, or if the company failed to address known vulnerabilities in its security architecture. Educational institutions should stay abreast of information as it becomes available to determine if they have a legitimate claim against the company for breach of contract or duty of care.

Considering these variables, you should consult with your FP legal counsel to help you triage the near- and medium-term legal requirements, including reporting, remediation, and, if applicable, how to handle a ransom demand. Our Data Protection and Cybersecurity Practice Group attorneys can assist, and our Reputation and Crisis Management Team can also help you communicate with your stakeholders throughout this incident.

Conclusion

Fisher Phillips will continue to monitor developments and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. If you have

Service Focus

Counseling and Advice

Data Protection and Cybersecurity

Privacy and Cyber

Industry Focus

Education

Higher Education

K-12 Schools

questions, please contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Education Practice Group or Data Protection and Cybersecurity Practice Group.