



One Hundred Nineteenth Congress  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

May 11, 2026

Mr. Steve Daly  
Chief Executive Officer  
Instructure Holdings, Inc.  
6330 South 3000 East, Suite 700  
Salt Lake City, Utah 84121

Dear Mr. Daly:

The Committee on Homeland Security (Committee) is investigating the concerning reports related to recent cybersecurity incidents affecting Instructure Holdings, Inc. and the tens of millions of students, educators, and administrators who rely on its Canvas learning management platform.<sup>1</sup> Within the span of one week, the cybercriminal group known as ShinyHunters breached Instructure twice. The group reportedly first struck on May 1, accessing personal data belonging to students and faculty across thousands of institutions, and struck again on May 7, defacing Canvas login pages nationwide and posting ransom demands directly on students' screens.<sup>2</sup> With students at more than 8,000 institutions navigating final examinations and end of semester deadlines, the disruption of a platform that Instructure itself describes as serving more than 30 million active users globally is a matter of national concern.<sup>3</sup>

Instructure disclosed on May 1, 2026, that it had experienced a cybersecurity incident in which a criminal threat actor accessed personal information belonging to students and faculty.<sup>4</sup> The company confirmed that the compromised information includes student names, personal email addresses, student identification numbers, and messages exchanged between students and faculty through Canvas.<sup>5</sup> Instructure stated that the breach was contained as of May 2 and that passwords, financial information, and government identifiers were not exposed.<sup>6</sup> ShinyHunters subsequently claimed on its data leak site to have accessed records belonging to approximately

---

<sup>1</sup> Instructure Holdings, Inc., *Why Instructure: Customers*, Instructure.com (May 8, 2026), available at <https://www.instructure.com/why-instructure/customers>.

<sup>2</sup> Lorenzo Franceschi-Bicchierai and Zack Whittaker, *Hackers Deface School Login Pages After Claiming Another Instructure Hack*, TechCrunch (May 7, 2026); see also Hannah Ziegler, *Canvas Online Learning Platform Disabled After Breach by Hackers*, N.Y. Times (May 7, 2026).

<sup>3</sup> Ramishah Maruf and Emma Tucker, *Canvas Hack Strands University Students During Finals Week*, CNN (May 7, 2026).

<sup>4</sup> Instructure Holdings, Inc., *Cybersecurity Incident Update* (May 1, 2026), available at <https://status.instructure.com/incidents/9wm4knj2r64z>; see also Lorenzo Franceschi-Bicchierai, *Hackers Steal Students' Data During Breach at Education Tech Giant Instructure*, TechCrunch (May 5, 2026).

<sup>5</sup> Instructure Holdings, Inc., *Cybersecurity Incident Update* (May 2, 2026), available at <https://status.instructure.com>.

<sup>6</sup> Ziegler, *supra* note 2.

275 million students, teachers, and other staff across nearly 9,000 institutions worldwide.<sup>7</sup> Whether or not those figures are fully accurate, the gap between Instructure's public characterization of this event and the scale suggested by the attacker's own claims warrants a full and transparent accounting.

The situation escalated sharply on May 7 when ShinyHunters reportedly compromised Instructure's systems a second time, injecting ransom demands directly into Canvas login pages across institutions nationwide.<sup>8</sup> Universities and school districts across at least eleven states reported the disruption.<sup>9</sup> Institutions in California, Florida, Georgia, Oklahoma, Oregon, Nevada, North Carolina, Tennessee, Utah, Virginia, and Wisconsin were among the confirmed affected parties.<sup>10</sup> In a message posted on affected Canvas pages, ShinyHunters stated that it had breached Instructure again because the company had ignored its outreach and issued security patches rather than engaging with the group's demands.<sup>11</sup> The group has threatened to publicly release the stolen data on May 12, 2026, if Instructure does not negotiate a resolution.<sup>12</sup>

ShinyHunters is a well-documented criminal threat actor with an extensive record of large-scale data theft and extortion targeting major organizations across multiple sectors.<sup>13</sup> The group has previously claimed responsibility for breaches at Ticketmaster, AT&T, and several other organizations.<sup>14</sup> They consistently employ the same operational playbook where they exploit a vulnerability, exfiltrate sensitive records, publicize the theft, and pressure the victim into paying a ransom to prevent public disclosure.<sup>15</sup> The group has increasingly targeted the education sector, including a separate breach at Infinite Campus, a K-12 student information system, and McGraw Hill, a major educational publisher.<sup>16</sup> The recurrence of an intrusion within days of an initial breach disclosure, and Instructure's apparent failure to fully remediate the underlying vulnerabilities during that window, raise serious questions about the company's incident response capabilities and its obligations to the institutions and individuals whose data it holds.

The Committee has broad jurisdiction over cybersecurity threats to the United States, including the security of critical digital infrastructure and the federal government's efforts to assist the private sector in defending against and responding to such threats. The Cybersecurity and Infrastructure Security Agency (CISA), which this Committee oversees, serves as the nation's lead civilian cybersecurity agency and has a direct role in supporting organizations that have experienced significant cyber incidents. The scale and timing of the Instructure breach, and the demonstrated inability of a major educational technology vendor to contain a threat actor

---

<sup>7</sup> Franceschi-Bicchierai and Whittaker, *supra* note 2; *see also* Emma Roth, *Canvas Is Down as ShinyHunters Threatens to Leak Schools' Data*, The Verge (May 7, 2026).

<sup>8</sup> Franceschi-Bicchierai and Whittaker, *supra* note 2; *see also* Roth, *supra* note 7.

<sup>9</sup> Maruf and Tucker, *supra* note 3; *see also* Ziegler, *supra* note 2.

<sup>10</sup> *Id.*

<sup>11</sup> Roth, *supra* note 7; *see also* Maruf and Tucker, *supra* note 3.

<sup>12</sup> Roth, *supra* note 7; *see also* Ziegler, *supra* note 2.

<sup>13</sup> Ziegler, *supra* note 2; *see also* Franceschi-Bicchierai, *supra* note 4.

<sup>14</sup> Roth, *supra* note 7.

<sup>15</sup> *Id.*

<sup>16</sup> Ziegler, *supra* note 2.

Mr. Steve Daly  
May 11, 2026  
Page 3 of 3

following an initial intrusion, are precisely the kind of systemic vulnerabilities this Committee has a responsibility to examine.

To that end, we request that you or a senior representative of Instructure Holdings participate in a briefing with the Committee, to be scheduled at a mutually convenient time no later than Thursday, May 21, 2026. The briefing should address the circumstances of both intrusions, the nature and volume of data accessed, the steps Instructure has taken and is taking to contain the threat and notify affected institutions, and the adequacy of the company's coordination with federal law enforcement and CISA.

We ask that your staff confirm Instructure's availability for this briefing no later than Thursday, May 14, 2026. Please direct your response and any questions regarding logistics to the Committee on Homeland Security Majority Staff at (202) 226-8417. The Committee takes seriously both the harm to students and educational institutions caused by this incident and the broader implications for how the educational technology sector manages and discloses cybersecurity risks. We look forward to a candid and informative exchange.

Per Rule X of the U.S. House of Representatives, the House Committee on Homeland Security is the principal committee of jurisdiction for overall homeland security policy and has special oversight of "all Government activities relating to homeland security."

Thank you for your attention to this important matter and your prompt reply.

Sincerely,



---

ANDREW R. GARBARINO  
Chairman  
Committee on Homeland Security

cc: The Honorable Bennie Thompson, Ranking Member  
Committee on Homeland Security