**IN THE UNITED STATES DISTRICT COURT**
**FOR THE WESTERN DISTRICT OF TEXAS**
**WACO DIVISION**

| | |
|---|---|
| **JANE DOE, individually and on behalf of all others similarly situated,** | **Case No.: 6:26-cv-00295** |
| **Plaintiff,** | |
| **v.** | **CLASS ACTION COMPLAINT** |
| **INSTRUCTURE, INC.,** | |
| **Defendant.** | **JURY TRIAL DEMANDED** |

## CLASS ACTION COMPLAINT

Plaintiff Jane Doe ("Plaintiff"), individually and on behalf of all others similarly situated, by and through her undersigned counsel, brings this Class Action Complaint against Instructure, Inc. ("Instructure" or "Defendant"), based upon personal knowledge as to matters concerning Plaintiff and upon information and belief, including counsel's investigation and review of public documents, as to all other matters, and alleges as follows:

## INTRODUCTION

1. This class action arises from a cybersecurity incident, data breach, and service outage involving Canvas, the learning management system operated by Defendant Instructure, Inc.

2. This case is not merely about whether names, email addresses, or student identification numbers were exposed. It is about the compromise of an education platform that Instructure knew stored student-record communications and that students were required to use during final exams.

3. Canvas is not a peripheral application. For students, faculty, and universities, Canvas is core academic infrastructure used for course materials, assignments, quizzes, exams, grading, accommodations, communications, and student-faculty messaging.

4. Instructure knew that Canvas was used by schools, colleges, universities, students, faculty, staff, and administrators to store and exchange sensitive student information and education-record data.

5. Instructure also knew that students relied on Canvas during finals week for time-sensitive access to course materials, study materials, gradebooks, exam instructions, quizzes, assignments, and final exams.

6. This action pleads two concrete injury categories that distinguish this case from a routine name-and-email data breach. First, students suffered Academic Disruption Damages when Instructure's security failures rendered Canvas unavailable during final exams, depriving students of access to study materials, assignments, course communications, grades, exam instructions, and online examinations. Second, students suffered Sensitive Education Record injuries because Instructure has indicated that the data taken included messages among Canvas users, and Canvas messages often contain confidential student communications about illness, disability accommodations, pregnancy, mental health, harassment, bullying, Title IX matters, discipline, grades, financial hardship, housing insecurity, immigration concerns, family emergencies, and safety issues, among other things.

7. On or about April 29, 2026, Instructure detected unauthorized activity in Canvas. Instructure has since acknowledged that the data taken included names, email addresses, student ID numbers, and messages among Canvas users. Instructure further disclosed that on May 7, 2026, the unauthorized actor made changes to pages that appeared when some students and teachers were

logged in through Canvas. Instructure states that the activity was carried out by exploiting an issue related to its Free-For-Teacher accounts. Instructure's own remediation statements confirm the seriousness of the compromise: Instructure states that it revoked privileged credentials and access tokens, deployed platform-wide protections, rotated certain internal keys, restricted token-creation pathways, added monitoring, and began hardening administrative access, token management, permissions, monitoring, and related workflows.

8. Instructure's incident was not limited to passive data exfiltration. It also resulted in a live platform-integrity and availability failure. Canvas was placed into maintenance mode during finals week, and students were instructed by their institutions not to access Canvas until official guidance was provided. For students, that meant loss of access to course materials, assignments, grades, communications, study materials, and exams during one of the highest-stakes academic periods of the year.

9. Instructure took Canvas offline and placed Canvas into maintenance mode during the final-exam period for many colleges and universities, including Baylor University in Waco, Texas ("Baylor"). Instructure's status page stated that Canvas, Canvas Beta, and Canvas Test were placed in maintenance mode on May 7, 2026.

10. Baylor publicly informed students, faculty, and staff that Canvas was unavailable university-wide, that users should not engage with or respond within Canvas, and that several universities had reported access blocked by a ransom notice before Instructure took Canvas offline. Baylor also confirmed that the Instructure breach impacted Baylor data stored on Instructure servers.

11. Baylor's Provost then informed students and faculty that the nationwide Canvas outage was "seriously disrupting" final-exam preparation, that final exams scheduled for Friday,

May 8 would be delayed, and that students might not be able to access the materials they needed to study.

12. The next day, Baylor announced that finals originally scheduled for May 8 would be conducted online on Thursday, May 14, and instructed users not to accept unrequested downloads under any circumstances. Baylor also recognized that students traveling or facing post-semester commitments needed flexibility and that move-out timing would shift as final exams shifted.

13. Plaintiff Jane Doe is a Baylor University student and nursing major. She relied on Canvas for course materials, final-exam preparation, academic communications, assignments, and exams.

14. Plaintiff was studying in the library for a statistics exam when Canvas became unavailable. Because Canvas was down, she could not access needed study materials and ultimately had to return home without them.

15. Plaintiff had a Human Development final exam scheduled for May 8, 2026. Baylor later informed students that finals scheduled for that day were postponed and would be administered online on Thursday, May 14, 2026.

16. Plaintiff had planned her finals, move-out, and return to Houston around the original exam schedule. The Instructure-caused Canvas outage disrupted those plans.

17. Plaintiff also spent time changing passwords because her Canvas-related credentials or password practices overlapped with other accounts, and because Instructure acknowledged that unauthorized actors changed pages shown to some logged-in Canvas users.

18. This case is materially different from a routine name-and-email breach. Instructure's own public materials confirm that Canvas processes messages, course content,

assessment results, course results, submission comments, submitted content, media, identifiers, and other education-related records. Instructure's Data Processing Addendum ("DPA") further states that, for U.S. K-12 and higher education customers, Student Data constitutes Education Records and that Instructure operates as a FERPA "School Official" for personally identifiable information from Education Records.

19. Plaintiff brings this action because Instructure failed to safeguard student data, failed to prevent unauthorized access to and manipulation of Canvas systems, failed to maintain the availability and integrity of critical education infrastructure, and failed to provide timely, adequate, and transparent notice and remediation.

20. Plaintiff seeks damages, restitution, declaratory relief, and injunctive relief requiring Instructure to remediate its security failures, protect exposed student data and Canvas messages, preserve evidence, provide adequate notice, and compensate students whose privacy, academic activities, finals, credentials, and educational records were affected.

## PARTIES

21. Plaintiff Jane Doe is a citizen and resident of Texas and a student at Baylor University in Waco, Texas. During the relevant academic period, Plaintiff attended Baylor, used Canvas for Baylor coursework, and suffered injury in McLennan County.

22. Plaintiff proceeds pseudonymously because this action may involve confidential student education records, sensitive academic communications, safety-related matters, accommodation-related matters, and Title IX-related information. Plaintiff will seek leave to proceed under pseudonym or will amend if required by the Court.

23. Defendant Instructure, Inc. is a Delaware corporation with its principal place of business at 6330 South 3000 East, Suite 700, Salt Lake City, Utah 84121. Instructure develops,

operates, hosts, maintains, and sells Canvas LMS to educational institutions throughout the United States, including institutions in Texas. Instructure contracted to provide Canvas to Texas institutions, processed Texas student data, maintained Texas student education records and Canvas messages, and caused injury to Plaintiff and proposed class members in Texas.

## JURISDICTION AND VENUE

24. This Court has subject-matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a putative class action involving more than 100 proposed class members, the aggregate amount in controversy exceeds $5 million exclusive of interest and costs, and minimal diversity exists.

25. This Court has personal jurisdiction over Instructure because Instructure purposefully directed Canvas services into Texas, contracted with Texas educational institutions, processed data of Texas students and users, and caused injury in Texas.

26. Venue is proper in this District under 28 U.S.C. § 1391 because a substantial part of the events giving rise to Plaintiff's claims occurred in this District. Baylor University is located in Waco, Texas, Plaintiff used Canvas for Baylor coursework, Baylor's Canvas instance was affected, Baylor finals were delayed, and Plaintiff suffered injury in Texas.

## FACTUAL ALLEGATIONS

### A. Canvas is critical education infrastructure.

27. Canvas is a web-based learning management system used by educational institutions, educators, students, and administrators to manage course materials, assignments, quizzes, exams, grades, and academic communications.

28. Students are often required to use Canvas as a condition of course participation. They cannot realistically opt out.

29. Instructure knew that Canvas was used during high-stakes academic periods, including final exams.

30. Instructure's own Master Terms state that it will use commercially reasonable efforts to make each service available with an annual uptime percentage of at least 99.9%. Instructure also warrants that it shall implement reasonable administrative, technical, and physical safeguards to secure its systems from unauthorized access and to secure customer content.

31. Instructure's own Trust Center similarly represents that Instructure builds security into its cloud platform, infrastructure, and processes, and that it guarantees and delivers 99.9% uptime.

32. Students, including Plaintiff, reasonably relied on Instructure to provide a secure and available learning-management platform.

**B. Instructure knew Canvas contained sensitive student data and education records.**

33. Instructure's DPA defines Customer Personal Data as personal data provided by or on behalf of a customer and processed by Instructure in connection with providing the services.

34. Instructure's DPA defines a Security Breach as a breach leading to unauthorized disclosure of or access to Customer Personal Data transmitted, stored, or otherwise processed by Instructure.

35. Instructure's DPA requires Instructure to maintain appropriate technical and organizational measures for the protection, security, confidentiality, and integrity of Customer Personal Data and Account Data.

36. Instructure's DPA also requires Instructure to notify customers of a Security Breach without undue delay, investigate the breach, provide information about it, and take commercially reasonable steps to mitigate its effects and minimize resulting damage.

37. Instructure's Schedule of Data for Canvas LMS lists numerous types of personal and student data processed through Canvas, including usernames/IDs, assessment results, calendar events, comments, course content, course results, email addresses, enrollment status, first and last names, IP addresses, messages, media content, pronouns, session IDs, school name, school position, SIS identifiers, submitted content, and Turnitin IDs.

38. Instructure's DPA expressly identifies Canvas "Messages" as including notifications and course conversations.

39. Instructure's U.S. K-12 and Higher Education Addendum defines "Education Records" as records, files, documents, and other materials directly related to a student and maintained by the educational customer or by a person acting for the customer, as defined under FERPA.

40. Instructure's DPA defines "Student Data" broadly to include data descriptive of a student, including education-record information, email address, first and last name, identifiers, videos, test results, special-education data, grades, evaluations, disabilities, socioeconomic information, documents, student identifiers, search activity, photos, voice recordings, geolocation information, and other information that would provide information about a specific student.

41. Instructure's DPA states that Student Data constitutes Education Records and that Instructure operates as a FERPA School Official for customers subject to FERPA.

42. Accordingly, Instructure knew that Canvas stored more than low-value contact information. Canvas contained student education records, grades, assessments, comments, messages, submitted content, and potentially sensitive student communications.

**C. The breach and unauthorized activity.**

43. On April 29, 2026, Instructure detected unauthorized activity in Canvas.

44. Instructure states that it revoked the unauthorized party's access, opened an investigation, engaged outside forensic experts, and notified law enforcement.

45. Instructure later disclosed that the data taken in the April 29 incident included names, email addresses, student ID numbers, and messages among Canvas users.

46. Instructure states that it has found no evidence so far that passwords, dates of birth, government identifiers, or financial information were involved.

47. On May 7, 2026, Instructure identified additional unauthorized activity tied to the same incident.

48. Instructure states that the unauthorized actor made changes to pages that appeared when some students and teachers were logged in through Canvas.

49. Instructure temporarily took Canvas offline into maintenance mode to contain the activity, investigate, and apply additional safeguards.

50. Instructure later stated that the unauthorized actor exploited an issue related to Free-For-Teacher accounts, which Instructure described as the same issue that led to unauthorized access the prior week.

51. Instructure further stated that it temporarily shut down Free-For-Teacher accounts, revoked privileged credentials and access tokens, deployed platform-wide protections, rotated internal keys, restricted token-creation pathways, added monitoring, and was hardening administrative access, token management, permissions, monitoring, and related workflows.

52. These remedial steps demonstrate that the incident implicated core access-control, credential, token, key-management, administrative, and monitoring controls.

53. Instructure's own statements show that the incident was not limited to a passive exposure of data. The unauthorized actor was able to change pages shown to certain logged-in users.

54. That conduct created reasonable concern about credential compromise, credential harvesting, phishing, user impersonation, and account integrity.

55. Plaintiff and class members were therefore reasonable in changing passwords, monitoring accounts, preserving records, and taking other mitigation steps.

**D. Baylor was directly impacted.**

56. Baylor University uses Canvas for academic coursework, assignments, final-exam preparation, communications, gradebooks, and online exams.

57. On May 6, 2026, Baylor ITS stated that it had been notified that a data breach at Instructure impacted Baylor data stored on Instructure servers.

58. Baylor ITS stated that the incident was not directed at Baylor but was part of a larger breach impacting higher-education customers.

59. Baylor ITS stated that Instructure had contracted with a forensics firm to investigate and provide a full accounting to Baylor and other customers.

60. Baylor ITS warned users to beware of phishing messages, not to click links in unsolicited messages claiming to be from Canvas, Instructure, or Baylor ITS, and to access Canvas and other websites directly.

61. On May 7, 2026, Baylor ITS updated users that several universities using Canvas had reported that their access to the system was blocked by a ransom notice and that, in response, Instructure took Canvas offline.

62. Baylor ITS then stated that Canvas was unavailable university-wide, that the issue was nationwide, and that users should not attempt to engage with or respond within Canvas until further notice.

63. Baylor's Provost later recognized that the nationwide Canvas outage was seriously disrupting students' preparations for final exams.

64. Baylor delayed final exams scheduled for Friday, May 8.

65. Baylor stated that it did not know how long Canvas would be unavailable and that students with finals scheduled for the next day might not be able to access the materials they needed to study.

66. Baylor instructed students not to access materials even if Canvas became available until Baylor sent a message that doing so was advisable.

67. Baylor encouraged faculty to send whatever study materials they had on local computers to students as soon as possible.

68. Baylor recognized that the disruption impacted the educational environment at an incredibly difficult time.

69. Baylor's official notices confirm that the outage caused concrete academic harm. Baylor acknowledged that Canvas being down was seriously disrupting students' preparation for final exams; that students with finals scheduled the next day might not be able to access the materials they needed to study; that faculty should send local copies of study materials where possible; that exams originally scheduled for May 8 would be moved to May 14 and administered online; that online administration created test-security challenges; that students with travel or post-semester commitments would need flexibility; and that move-out deadlines would shift as final exams shifted.

70. On May 8, 2026, Baylor announced that Canvas would be restored at 1:00 p.m. CT.

71. Baylor instructed users not to accept unrequested downloads under any circumstances and to report unusual activity immediately.

72. Baylor announced that final exams originally scheduled for May 8 would be conducted online on Thursday, May 14.

73. Baylor recognized that online administration created test-security challenges.

74. Baylor asked faculty to build in flexibility so students traveling or facing post-semester commitments could complete exams when schedules permitted.

75. Baylor stated that the residence-hall move-out deadline would shift as final exams shifted.

76. Baylor warned that if Canvas was compromised again, it would provide further instructions.

**E. Plaintiff Jane Doe's experience.**

77. Plaintiff Jane Doe is a Baylor student and nursing major.

78. Plaintiff used Canvas for academic coursework, course materials, assignments, exams, study materials, course communications, and final-exam preparation.

79. On May 7, 2026, Plaintiff was studying in the library for a statistics exam when Canvas became unavailable.

80. Plaintiff depended on Canvas to access course materials and study materials needed for finals.

81. Plaintiff was dependent on Instructure's Canvas platform and on information Instructure provided to Baylor regarding whether Canvas was available, whether it was secure, and whether it could be used safely.

82. Because Instructure controlled Canvas, the incident investigation, the restoration timeline, and the technical facts necessary to determine whether Canvas could be accessed safely, Plaintiff did not receive timely and complete information sufficient to know when Canvas would be restored, whether it was safe to access, or how she could obtain needed course materials.

83. Because Canvas remained unavailable and Plaintiff could not access needed materials, Plaintiff had to leave the library and return home without the study materials she needed.

84. Plaintiff had a Human Development final exam scheduled for May 8, 2026.

85. On May 8, 2026, Baylor notified students that finals scheduled for that day would be postponed.

86. Plaintiff's Human Development final was postponed to Thursday, May 14, 2026.

87. Baylor stated that the postponed exam would be conducted online.

88. Baylor's plan to administer the postponed final online required Plaintiff to continue relying on Canvas, the same platform that had just been compromised and taken offline.

89. Plaintiff's last final was scheduled for the following Tuesday, May 12, 2026.

90. Plaintiff had planned to complete finals, move out or otherwise leave campus, and travel back to Houston.

91. The Instructure incident disrupted Plaintiff's exam schedule, study schedule, move-out plans, travel plans, and academic preparation.

92. Because Plaintiff is a nursing major, final grades and minimum passing requirements are especially significant to her academic progression.

93. Plaintiff intends to seek, or may need to seek, minimum-passing-grade consideration or other academic relief because the Instructure incident impaired her access to study materials and delayed exams during finals.

94. Plaintiff spent time changing passwords and securing accounts because the same or similar password practices were connected to her Canvas account and other accounts.

95. Plaintiff's mitigation steps were reasonable because Instructure acknowledged that unauthorized actors changed pages shown to some logged-in Canvas users.

96. Plaintiff also became aware of reports that some users experienced account-not-found, ID-not-working, or similar account-access issues, increasing her concern about account integrity.

97. Plaintiff suffered stress, anxiety, lost study time, lost access to academic materials, disruption of exam preparation, delay of a final exam, travel and move-out disruption, academic uncertainty, and time spent securing accounts.

98. Plaintiff used Canvas messages, comments, submissions, and/or other Canvas communications to discuss requested academic supportive measures and sensitive academic matters.

99. Plaintiff also had contemporaneous safety, harassment, retaliation, and Title IX-related concerns. Because those facts are highly sensitive and identifying, Plaintiff does not plead the underlying details publicly and will submit additional details under seal or in camera if necessary.

100. Because Instructure has acknowledged that messages among Canvas users were taken, Plaintiff's Canvas communications concerning supportive measures, safety, academic participation, and related sensitive matters fall within the category of Canvas communications Instructure has identified as involved in the incident.

101. Plaintiff does not allege at this time that ordinary emails, Title IX portal communications, or other non-Canvas communications were included in the Canvas breach unless

discovery shows those communications were copied into, integrated with, attached to, or stored within Canvas.

102. Plaintiff would not have entrusted information to Canvas or relied on Canvas in the same manner had she known Instructure's security and availability controls were inadequate to prevent unauthorized access, page manipulation, data theft, and finals-week service disruption.

**F. Injuries and damages.**

103. Plaintiff and class members suffered concrete injuries including:

a. Loss of privacy;

b. Loss of control over personal information, student data, education records, and Canvas messages;

c. Exposure of names, email addresses, student ID numbers, and Canvas messages;

d. Exposure or threatened exposure of sensitive student communications;

e. Time spent investigating the incident;

f. Time spent changing passwords and securing accounts;

g. Increased phishing, impersonation, and credential-risk exposure;

h. Finals disruption;

i. Lost access to study materials;

j. Exam delay and rescheduling;

k. Travel and move-out disruption;

l. Academic uncertainty and grade-related risk;

m. Emotional distress, stress, and anxiety;

n. Loss of benefit of the bargain;

o. Diminished value of Canvas services and student data; and

p. Need for injunctive relief, monitoring, and remediation.

104. Plaintiff's damages are concrete and particularized. She was personally affected by the Baylor Canvas outage, lost access to needed study materials, had a final postponed, had travel and move-out plans disrupted, spent time changing passwords, and faces continuing concern regarding exposed Canvas data.

105. Class members with sensitive Canvas messages suffered additional privacy harm because Canvas messages can contain medical, disability, pregnancy, mental-health, harassment, bullying, Title IX, disciplinary, financial-hardship, immigration, housing, family-emergency, and safety-related information.

106. Class members whose finals, assignments, or exams were disrupted suffered academic and time-loss damages beyond ordinary data-breach harm.

107. Class members who entered credentials on suspicious or manipulated Canvas pages, or who reasonably secured accounts in response, suffered credential-risk and mitigation damages.

**G. Plaintiff's injuries are concrete, present, and particularized.**

108. Plaintiff does not rely solely on speculative future identity-theft risk. Plaintiff personally lost access to study materials during finals preparation, had a final exam postponed, had travel and move-out plans disrupted, spent time securing accounts and changing passwords, and faces ongoing concern that Canvas messages and student-record communications were exposed.

109. The Academic Disruption Damages suffered by Plaintiff and similarly situated students include lost study time, loss of access to course materials, postponed exams, disrupted

deadlines, travel and move-out disruption, grade-related uncertainty, academic-relief petitions, and time spent navigating school and vendor communications.

110. The Sensitive Education Record injuries suffered by Plaintiff and similarly situated users include loss of control over confidential Canvas communications and student-record information, including messages that may concern health, disability accommodations, pregnancy, mental health, harassment, bullying, Title IX matters, discipline, grades, financial hardship, housing insecurity, immigration concerns, family emergencies, or safety issues.

## CLASS ALLEGATIONS

111. Plaintiff brings this action under Rules 23(a), 23(b)(2), and 23(b)(3) on behalf of the following classes and subclasses, reserving the right to amend, narrow, expand, or refine these definitions as discovery and investigation progress:

> **Nationwide Data Breach Class:** All persons in the United States whose personal information, student data, education records, or Canvas messages were accessed, acquired, exposed, or taken in the Instructure/Canvas cybersecurity incident disclosed in or around May 2026.
>
> **Texas Subclass:** All Texas residents whose personal information, student data, education records, or Canvas messages were accessed, acquired, exposed, or taken in the incident.
>
> **Academic Disruption and Grade Impact Subclass:** All students whose final exams, quizzes, assignments, study materials, grades, deadlines, move-out schedules, travel schedules, academic-progression requirements, or other time-sensitive academic activities were delayed, disrupted, impaired, rescheduled, or materially affected because of the incident or outage.
>
> **Sensitive Education Record Subclass:** All persons whose Canvas messages, comments, submissions, or user communications contained sensitive, non-directory student-record information—including health, disability, pregnancy, academic accommodations, testing accommodations, mental health, harassment, bullying, Title IX, disciplinary, grade-related, financial-hardship, immigration, housing, safety, family-emergency, or similar sensitive information—and were accessed, acquired, exposed, or taken in the incident.
>
> **Credential Page and Account Mitigation Subclass:** All persons who, because of the incident or unauthorized changes to Canvas pages, entered credentials on a suspicious

Canvas page, changed passwords, secured accounts, monitored accounts, or incurred time or expense responding to possible credential compromise.

112. Excluded from all proposed classes and subclasses are Defendant; Defendant's officers, directors, agents, employees, parents, subsidiaries, affiliates, and successors; any entity in which Defendant has a controlling interest; the Court, the Court's staff, and members of their immediate families; and any person who validly opts out of any certified class.

113. Numerosity is satisfied because the proposed classes include thousands, and likely millions, of users.

114. Common questions include:

a. Whether Instructure failed to implement reasonable cybersecurity controls;

b. Whether Instructure failed to maintain reasonable access-token, credential, key-management, administrative-access, monitoring, and Free-For-Teacher account controls;

c. Whether Instructure failed to protect Canvas messages and education-record data;

d. Whether Instructure's security failures caused finals-week academic disruption;

e. Whether unauthorized changes to Canvas pages created credential harvesting, account integrity, or password mitigation risks for users;

f. Whether Instructure's notice and remediation were adequate;

g. Whether Plaintiff and class members suffered legally cognizable damages;

h. Whether Instructure's conduct violated statutory, contractual, common law, and industry standards;

i. Whether class members are entitled to damages, restitution, declaratory relief, and injunctive relief.

115. Plaintiff's claims are typical because she used Canvas, entrusted information to Canvas, suffered finals disruption, lost access to materials, changed passwords, and faces privacy and security risks arising from the same incident.

116. Plaintiff is adequate because she has no conflicts with absent class members and has retained counsel experienced in data-breach, privacy, consumer, and class-action litigation.

117. A class action is superior because individual damages may be too small to litigate separately, while common issues concerning Instructure's breach, security practices, notice, and remediation predominate.

118. Injunctive relief is appropriate because Instructure's security, notice, and remediation practices affect all class members.

## CAUSES OF ACTION

### COUNT I
### NEGLIGENCE
***(On behalf of Plaintiff and all classes)***

119. Plaintiff incorporates the preceding paragraphs.

120. Instructure owed Plaintiff and class members a duty to exercise reasonable care in collecting, storing, maintaining, securing, and protecting personal information, student data, education records, and Canvas messages.

121. Instructure owed Plaintiff and class members a duty to maintain reasonable security and availability of Canvas because it knew students and schools relied on Canvas for finals, assignments, grades, communications, and exams.

122. Instructure's duties arose from its role as the operator of Canvas, its collection and processing of student data, its contractual security undertakings, its public privacy and security representations, its DPA, its role as a FERPA School Official, applicable statutory standards, industry standards, and the foreseeability of harm.

123. Instructure breached its duties by failing to implement reasonable cybersecurity measures, including adequate controls over Free-For-Teacher accounts, administrative access, privileged credentials, access tokens, internal keys, token-creation pathways, monitoring, logging, intrusion detection, vulnerability management, and incident response.

124. Instructure breached its duties by allowing unauthorized actors to access Canvas data and change pages shown to logged-in users.

125. Instructure breached its duties by failing to prevent exposure of Canvas messages and student data.

126. Instructure breached its duties by failing to maintain reasonable platform availability during a critical academic period.

127. Instructure breached its duties by failing to provide adequate, timely, complete, and transparent notice and remediation.

128. Instructure's breaches caused Plaintiff and class members to suffer damages including loss of privacy, loss of control over data, exposure of Canvas messages, finals disruption, lost access to materials, password-mitigation time, emotional distress, academic uncertainty, travel and move-out disruption, and increased risk of phishing and misuse.

## COUNT II
## NEGLIGENCE PER SE AND STATUTORY STANDARDS OF CARE
***(On behalf of Plaintiff and all classes)***

129. Plaintiff incorporates the preceding paragraphs.

130. Instructure was required to comply with statutory, regulatory, contractual, and industry standards governing data security, breach notice, availability, platform integrity, and protection of personal information, student data, education-record information, and Canvas user communications.

131. These standards include, among others, Section 5 of the FTC Act, applicable state data-security and breach-notification laws, Texas data-protection and breach-notification standards, FERPA-related restrictions and education-record confidentiality standards, Instructure's contractual FERPA School Official obligations, and industry standards such as NIST and CIS controls.

132. Plaintiff does not plead FERPA as a standalone private damages cause of action. Plaintiff relies on FERPA, Instructure's FERPA School Official role, and Instructure's own Data Processing Addendum as evidence of duty, sensitivity, foreseeability, confidentiality obligations, and the applicable standard of care.

133. To the extent any statute identified herein does not independently support negligence per se under applicable law, Plaintiff pleads those statutes, regulations, contractual obligations, and industry standards as evidence of the applicable duty of reasonable care and breach.

134. Instructure violated these standards by failing to implement reasonable safeguards, failing to prevent unauthorized access and disclosure, failing to prevent unauthorized manipulation of Canvas pages, and failing to provide timely and adequate notice and remediation.

135. Plaintiff and class members are within the class of persons these standards are designed to protect.

136. The harms suffered by Plaintiff and class members are the type of harms these standards are designed to prevent.

137. Instructure's violations caused Plaintiff and class members damages.

**COUNT III**
**BREACH OF IMPLIED CONTRACT AND/OR INTENDED THIRD-PARTY BENEFICIARY CONTRACT**
***(On behalf of Plaintiff and all classes)***

138. Plaintiff incorporates the preceding paragraphs.

139. Plaintiff and class members used Canvas as required or directed by their educational institutions.

140. Plaintiff and class members provided personal information, student data, education-record information, course content, messages, submissions, and other data to Instructure through Canvas.

141. Instructure accepted and processed that information to provide Canvas services.

142. In exchange for payments from educational institutions, including payments funded directly or indirectly through student tuition and fees, Instructure undertook to provide secure, reliable, and privacy-protective Canvas services.

143. Instructure's contracts, DPA, Master Terms, privacy commitments, and security representations were intended to benefit Canvas users, including students.

144. Plaintiff and class members were intended third-party beneficiaries of Instructure's promises to protect Customer Personal Data, Student Data, Education Records, Customer Content, and Canvas service availability.

145. Instructure's contractual promises concerning security, availability, confidentiality, Student Data, Customer Personal Data, Education Records, Customer Content, and Canvas service reliability were not abstract vendor promises. They were made for the benefit of the students,

faculty, staff, and users whose data and academic work Instructure processed and whose course participation depended on Canvas.

146. Alternatively, an implied contract existed between Instructure and users requiring Instructure to protect user data and provide a reasonably secure and available platform.

147. Instructure breached those contracts by failing to safeguard student data and messages, failing to prevent unauthorized access, failing to prevent unauthorized page manipulation, failing to maintain reasonable availability, and failing to provide adequate notice and remediation.

148. Plaintiff and class members suffered damages as a result.

**COUNT IV**
**BREACH OF CONFIDENCE**
***(On behalf of Plaintiff and all classes)***

149. Plaintiff incorporates the preceding paragraphs.

150. Plaintiff and class members entrusted Instructure with personal information, student data, education records, Canvas messages, submitted content, and academic communications.

151. Instructure knew this information was confidential.

152. Instructure voluntarily received the information with the understanding that it would protect it from unauthorized access, disclosure, and misuse.

153. Instructure's relationship with educational institutions and users was governed by confidentiality obligations, privacy policies, DPA provisions, FERPA-related duties, and reasonable expectations of confidence.

154. Instructure breached that confidence by failing to prevent unauthorized actors from accessing and taking data, including messages among Canvas users.

155. Plaintiff and class members suffered damages including loss of privacy, loss of control, emotional distress, time loss, mitigation costs, and continuing risk.

**COUNT V**
**UNJUST ENRICHMENT**
***(In the alternative, on behalf of Plaintiff and all classes)***

156. Plaintiff incorporates the preceding paragraphs.

157. Instructure received substantial benefits and payments for providing Canvas as a secure and reliable learning-management platform.

158. Instructure also benefited from collecting, processing, and deriving operational value from user data and usage data in connection with its services.

159. Instructure retained those benefits while failing to provide the security, privacy, reliability, and availability that users and institutions reasonably expected.

160. It would be unjust for Instructure to retain the full value of payments, data, and benefits received while shifting the costs of its security failures to students and users.

161. Plaintiff and class members are entitled to restitution, disgorgement, and other equitable relief.

**COUNT VI**
**TEXAS DECEPTIVE TRADE PRACTICES ACT**
***(On behalf of Plaintiff and the Texas Subclass, pleaded in the alternative)***

162. Plaintiff incorporates the preceding paragraphs.

163. Plaintiff and Texas class members were consumers of education-related services in which Canvas was a required or integrated component.

164. Instructure represented, directly and indirectly, that Canvas was secure, reliable, privacy-protective, and suitable for use in academic instruction, communications, assignments, exams, and finals.

165. Instructure represented that it implemented reasonable safeguards and maintained high availability.

166. Instructure's representations and omissions were false, misleading, or deceptive under, among other provisions, Texas Business & Commerce Code §§ 17.46(b)(5), 17.46(b)(7), and 17.46(b)(24), because Instructure failed to maintain reasonable security, failed to prevent unauthorized access and page manipulation, failed to protect Canvas messages and education-record communications, failed to maintain promised availability during finals, and failed to disclose material facts concerning security and availability risks.

167. Instructure's conduct was producing cause of Plaintiff's and Texas class members' damages.

168. Plaintiff pleads this count in the alternative and reserves the right to refine it after reviewing Baylor's contract documents, tuition/fee structure, and any limitations or disclaimers applicable to end users.

169. Plaintiff is providing written notice under Texas Business & Commerce Code § 17.505 contemporaneously with this filing. To the extent the Court determines any additional notice period is required, Plaintiff pleads this claim in the alternative and consents to statutory abatement of the DTPA damages claim while preserving all non-DTPA claims and requests for injunctive relief.

## COUNT VII
## DECLARATORY AND INJUNCTIVE RELIEF
***(On behalf of Plaintiff and all classes)***

170. Plaintiff incorporates the preceding paragraphs.

171. An actual controversy exists regarding Instructure's duties to protect student data, preserve Canvas messages, remediate security failures, provide adequate notice, and prevent recurrence.

172. Plaintiff and class members remain at risk because the full scope of the incident is unknown, the full content of the message corpus has not been disclosed, and Instructure's remedial measures require verification.

173. Plaintiff seeks declaratory relief that Instructure's conduct was unlawful and that Instructure has continuing duties to remediate the breach.

174. Plaintiff seeks injunctive relief requiring Instructure to:

a. Preserve all logs, forensic images, incident reports, threat-actor communications, internal communications, and customer communications;

b. Complete and disclose a forensic investigation sufficient to identify affected users, affected institutions, data categories, and affected Canvas messages;

c. Provide direct notice to affected users where possible;

d. Create a mechanism for users to determine whether their Canvas messages were accessed or taken;

e. Provide identity protection, phishing protection, and dark-web monitoring services;

f. Reimburse reasonable mitigation costs;

g. Preserve and restore course materials and academic records;

h. Provide institutions with information needed to remediate finals disruption;

i. Harden administrative access, Free-For-Teacher account controls, token management, key management, credential management, logging, monitoring, and permissions;

j. Undergo independent security audits;

k. Provide periodic compliance reports; and

l. Implement reasonable breach-notification and end-user-warning protocols.

**REQUEST FOR RELIEF**

Plaintiff, individually and on behalf of the proposed classes, respectfully requests that the Court enter judgment in her favor and in favor of the proposed classes against Defendant as follows:

A. Certify this action under Rule 23, appointing Plaintiff as class representative, and appointing Plaintiff's counsel as class counsel;

B. Award compensatory, consequential, nominal, statutory damages where available, restitution, disgorgement, and other damages or monetary relief permitted by law;

C. Award declaratory and injunctive relief;

D. Order Defendant to provide notice, remediation, monitoring, security improvements, and academic support services;

E. Award pre- and post-judgment interest as allowed by law;

F. Award attorneys' fees, costs, and expenses as permitted by law; and

G. Grant such other and further relief as the Court deems just and proper.

**JURY DEMAND**

Plaintiff demands a trial by jury on all issues so triable.

Dated: May 8, 2026

Respectfully submitted,

**HALL ATTORNEYS, P.C.**

By: */s/ Nicholas Andrew Hall*

Nicholas Andrew Hall
State Bar No. 24069863
nhall@hallattorneys.com
P.O. Box 1370
Edna, Texas 77957
+1 713 428 8967

**ATTORNEY FOR PLAINTIFF AND PUTATIVE CLASSES**

JS 44 (Rev. 04/21)

# CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

## I. (a) PLAINTIFFS

Jane Doe, individually and on behalf of all others

**(b)** County of Residence of First Listed Plaintiff Harris County, Texas
*(EXCEPT IN U.S. PLAINTIFF CASES)*

**(c)** Attorneys *(Firm Name, Address, and Telephone Number)*

Hall Attorneys, P.C.
P.O. Box 1370, Edna, TX 77957
(713) 428-8967

## DEFENDANTS

Instructure, Inc.

County of Residence of First Listed Defendant Salt Lake County, Utah
*(IN U.S. PLAINTIFF CASES ONLY)*

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

## II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

## III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

*(For Diversity Cases Only)*

| | PTF | DEF | | PTF | DEF |
|---|---|---|---|---|---|
| Citizen of This State | ☒ 1 | ☐ 1 | Incorporated *or* Principal Place of Business In This State | ☐ 4 | ☐ 4 |
| Citizen of Another State | ☐ 2 | ☐ 2 | Incorporated *and* Principal Place of Business In Another State | ☐ 5 | ☒ 5 |
| Citizen or Subject of a Foreign Country | ☐ 3 | ☐ 3 | Foreign Nation | ☐ 6 | ☐ 6 |

## IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

**CONTRACT**
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☒ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

**TORTS**

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

**FORFEITURE/PENALTY**
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

**LABOR**
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

**IMMIGRATION**
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

**BANKRUPTCY**
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

**INTELLECTUAL PROPERTY RIGHTS**
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

**SOCIAL SECURITY**
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

**FEDERAL TAX SUITS**
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

**OTHER STATUTES**
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

**REAL PROPERTY**
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

**CIVIL RIGHTS**
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

**PRISONER PETITIONS**

**Habeas Corpus:**
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

**Other:**
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

## V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

## VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
Negligence; negligence per se and statutory standards of care; BREACH OF IMPLIED CONTRACT AND/OR INTENDED THIRD-PARTY BENEFICIARY CONTRACT; BREACH OF CONFIDENCE; unjust enrichment; Tex. DTPA; declaratory & injunctive

Brief description of cause:
Cybersecurity incident, data breach, and service outage involving Canvas, the learning management system operated by Defendant

## VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

**DEMAND $** 5,000,000

CHECK YES only if demanded in complaint:
**JURY DEMAND:** ☒ Yes ☐ No

## VIII. RELATED CASE(S) IF ANY

*(See instructions):* JUDGE _____ DOCKET NUMBER _____

DATE May 8, 2026

SIGNATURE OF ATTORNEY OF RECORD /s/ Nicholas Andrew Hall

**FOR OFFICE USE ONLY**

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____