UNITED STATES DISTRICT COURT
DISTRICT COURT OF MASSACHUSETTS

JANE DOE, *individually and on behalf of all others similarly situated*, Plaintiff, v. MATTHEW WEISS; the TRUSTEES OF SIMMONS UNIVERSITY; SIMMONS UNIVERSITY; and KEFFER DEVELOPMENT SERVICES, LLC, Defendants.	**CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL** Civil Action No.

Plaintiff Jane Doe[1] brings this lawsuit on behalf of herself and all others who have been subjected to an unlawful breach of privacy, stemming from former University of Michigan and Baltimore Ravens coach Matthew Weiss' unauthorized access of athletic trainer databases maintained by a third-party vendor, Keffer Development Services, LLC. Plaintiff files this class action complaint and alleges the following.

NATURE OF THE ACTION

Students and alumni connected to Simmons University from 2015 to 2023—many of them student-athletes—have been subjected to a deeply troubling and unlawful breach of privacy, stemming from the actions of former University of Michigan and Baltimore Ravens coach Matthew Weiss, whose gross and despicable violations of their privacy were facilitated by institutional negligence. This class action lawsuit, filed against Matthew Weiss, Simmons

[1] Jane Doe is a pseudonym. Plaintiff's motion seeking leave to proceed pseudonymously is forthcoming.

University and its Trustees, and Keffer Development Services, LLC, seeks justice for the unauthorized access and misuse of personal information—an abuse so severe that students and student-athletes across the nation are now receiving formal notification from the U.S. Department of Justice that their private information, including intimate photos and videos, have been exposed, including Plaintiff Jane Doe. This action is brought to hold the Defendants accountable for failing to protect their students from foreseeable harm.

PARTIES

1. Plaintiff Jane Doe was a student athlete at Simmons University between 2012 and 2016 and was a member of the Cross Country Team.

2. Plaintiff Jane Doe is domiciled in Plymouth County, Massachusetts.

3. Defendant Simmons University ("Simmons") is a school incorporated in Massachusetts with its principal place of business located at 300 The Fenway, Boston, Massachusetts. Simmons University was Simmons College and renamed Simmons University in or around 2017.

4. Defendant Trustees of Simmons University are sued in their official capacity as Trustees of Simmons University.

5. Defendant Keffer Development Services, LLC ("Keffer") is a Pennsylvania limited liability company with its principal place of business in Grove City, PA, that has continuously and systemically conducted business in Massachusetts by directly providing services to residents and entities within the Commonwealth of Massachusetts, thereby availing itself of protections of the law of the Commonwealth of Massachusetts. Defendant Keffer is a technology and data vendor operating an electronic medical record and student athlete training system, which stored the personally identifiable information ("PII") and protected health information ("PHI") of Plaintiff

and Class Members across the country. Any wrongful conduct and legal violations committed by Defendant Keffer that are subsequently outlined in this Complaint occurred specifically with respect to the Plaintiff during the time of the incident alleged in this Complaint.

6. Matthew Weiss ("Weiss") is an individual domiciled in the State of Michigan, who had affirmative contacts with the Commonwealth of Massachusetts in that he conducted illegally activity in the Commonwealth of Massachusetts, by hacking into the personal property of Plaintiff and putative Class Members of the Commonwealth of Massachusetts during the applicable time period at issue in this Complaint and said activities of which this Complaint arises from.

7. On March 20, 2025, Defendant Weiss was indicted on 24 counts of unauthorized access to computers and aggravated identity theft by the U.S. Attorney for the Eastern District of Michigan.

JURISDICTION AND VENUE

8. Jurisdiction is proper in this Court under 28 U.S.C. §§ 1331 and 1367 as this matter involves a claim under the Stored Communications Act, 18 U.S.C. § 2701(a) *et seq*.; the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; Title IX, 20 U.S.C. § 1681(A) *et seq.*; and this Court has supplemental jurisdiction of all additional causes of action alleged in this Complaint pursuant to 28 U.S.C. §1367(a).

9. This Court also has subject matter jurisdiction pursuant to 28 U.S.C. §1332(d) under the Class Action Fairness Act ("CAFA") as a class action lawsuit in which the amount in controversy exceeds $5,000,000.00, there are more than one-hundred putative Class Members, and the majority of the putative Class Members are citizens of a state different than the state of which Defendants are citizens.

10. The Court has personal jurisdiction over Defendants named in this action because Defendant Simmons is located and created under the laws of the Commonwealth of Massachusetts, Defendant Weiss had minimum contacts with the Commonwealth of Massachusetts as set forth above, thus purposefully availing himself of the privilege of conducting activities in the Commonwealth of Massachusetts. Defendant Keffer directs business at the Commonwealth of Massachusetts, conducts substantial business in Massachusetts, and has availed itself of the protections of Massachusetts state law. The conduct by Defendant Keffer which gives rise to the claims against Defendant Keffer in this Complaint was directed at and occurred in the Commonwealth of Massachusetts.

11. Venue is appropriate in this District Court under 28 U.S.C. §1391(b) since Defendant Simmons University resides within this District and a substantial part of the events or omissions giving rise to these claims occurred within this District.

12. Plaintiff's injuries are redressable by monetary compensation, and all alleged injuries of Plaintiff and Class Members can be traced to Defendants' conduct.

COMMON ALLEGATIONS

A. Weiss's Data Breach and Cyber Voyeurism of Thousands of Students were Enabled by Defendant Keffer's Failures

13. Plaintiff brings this class action against Defendants Simmons and Keffer for their failure to properly secure the highly sensitive personally identifiable information ("PII") and protected health information ("PHI") of more than 150,000 students, including herself, which Matthew Weiss, former University of Michigan and Baltimore Ravens coach and sexual predator, targeted, unauthorizedly accessed, and stole over the course of nearly a decade.

14. Between 2015 and January 2023, Defendant Weiss gained unauthorized access to databases used by athletic trainers at more than 100 colleges and universities, some of which were maintained by Defendant Keffer, a third-party vendor contracted by these colleges and universities.

15. Upon information and belief, Defendant Simmons contracted with Defendant Keffer.

16. After gaining access to these databases, Weiss downloaded the PII and PHI of more than 150,000 athletes.

17. Using the information that Weiss obtained from the Athletic Trainer System, Weiss was able to target more than 2,000 student athletes and hack their social media, email, and/or cloud storage accounts. Defendant Weiss also illegally obtained access to the social media, email, and/or cloud storage accounts of more than 1,300 additional students and/or alumni from universities and colleges across the country.

18. Defendant Weiss primarily targeted female college athletes. He researched and targeted these women based on their school affiliation, athletic history, physical characteristics, and sexual preferences.

19. Through this scheme, and unknown to students and student athletes, Defendant Weiss downloaded personal, intimate digital photographs and videos that were never intended to be shared beyond intimate partners. This scheme appears to be the largest incident of cyber voyeurism of student athletes in U.S. history.

20. The data breach and cyber voyeurism of over 150,000 students from university and college databases, including athletic databases maintained by Keffer, and the targeted stealing of intimate, personal, digital photographs and videos of 3,300 students and athletes, continued for

nearly a decade because Defendant Simmons and Defendant Keffer failed to prevent, detect, or stop Weiss from accessing those databases without and in excess of any authorization.

21. In at least several instances, Defendant Weiss exploited vulnerabilities in universities' account authorization processes to gain access to the accounts of students or alumni. Weiss then leveraged his access to these accounts to gain access to other social media, email, and/or cloud storage accounts.

22. On its face, the sheer number of accounts Weiss was able to access over an eight-year period not only shows an egregious and grossly negligent failure of data security, but also the clear lack of reasonable data security policies and procedures.

23. In March 2025, the U.S. Attorney for the Eastern District of Michigan charged Weiss in a 24-count indictment alleging 14 counts of unauthorized access to computers and 10 counts of aggravated identity theft, for Weiss's perpetration of the cyber voyeurism and data breaches.

24. On or about March 31, 2025, Plaintiff Jane Doe received notice from the United States Department of Justice Victim Notification System that she was identified as a victim in the criminal case against University of Michigan's Coach Weiss: *United States v. Defendant(s) Matthew Weiss*.[2]

B. Defendant Keffer and its "Athletic Trainer System"

25. Defendant Keffer is a software development vendor that developed an electronic medical record system known as "The Athletic Trainer System," which is used by many schools, colleges and universities across the United States.[3]

[2] Jane Doe's DOJ Data Breach Notice is attached hereto as **Exhibit A**.
[3] Keffer's Athletic Trainer System sales brochure is attached as **Exhibit B**.

26. Defendant Keffer was founded in 1994 and has collaborated with over 600 clients across 48 states and internationally since that time.[4] Defendant Keffer advertises that it currently serves over 6,500 schools, clinics, and other organizations with over 27,000 users and 2 million athletes.[5]

27. Upon information and belief, the universities served by Keffer include Defendant Simmons, Jane Doe's alma mater.

28. Keffer represents that its Athletic Trainer System tool was "[d]esigned with Athletic Trainers for ALL Medical Professionals," and is designed to store PII and PHI belonging to students including their treatment histories, diagnoses, injuries, photos, insurance information, immunizations, and personal details, like height and weight, mental health information, and demographic information.[6]

29. In Keffer's FAQ, it boasts that "[i]nformation security is a high priority in our company."[7] Keffer further claims that "[o]n top of our Data Center being FedRamp Certified, ATS is also HIPAA and FERPA compliant. We utilize a company called Compliance Helper to ensure we maintain HIPAA and FERPA compliance."[8]

30. In Keffer's Privacy Policy, it acknowledges that it has obligations as a "business associate" under HIPAA: "To the extent that [Keffer] receives or maintains patient medical information in the course of providing the Clinical EMR, that information is secured, used and

[4] Keffer's Company History page on its website is attached as **Exhibit C**.
[5] Keffer's home page on its website is attached as **Exhibit D**.
[6] *Id.*
[7] Keffer's FAQ page on its website is attached as **Exhibit E**.
[8] *Id.*

disclosed only in accordance with [Keffer's] legal obligations as a 'business associate' under HIPAA."[9]

31. Keffer's Privacy Policy further states: "[Keffer] understands that storing our data in a secure manner is essential. KDS stores PII, PHI and other data using industry-standard physical, technical and administrative safeguards to secure data against foreseeable risks, such as unauthorized use, access, disclosure, destruction or modification."[10]

32. Despite touting these obligations, Keffer failed to implement basic industry standards to protect student's—including Jane Doe's—PII and PHI.

33. As an example, while Keffer maintained the option to incorporate two-factor authentication to access its Athletic Trainer System applications, it did not require that institutions and users do so.[11]

34. Two-factor authentication is a basic security measure that requires an additional piece of evidence, known as a factor, such as a code sent via text message or email, before allowing access to the authenticated system.[12]

35. Critically, requiring this security feature could have prevented Defendant Weiss from gaining access to student protected health information with only the access credentials belonging to other administrators and users.

36. Defendants knew that Keffer did not require institutions and users to use two-factor authentication to access the private information and communications accessible through its system, including information maintained in Defendant Simmons's facilities, and thus knowingly and

[9] Keffer's Privacy Policy is attached as **Exhibit F**.
[10] *Id.*
[11] *See* **Exhibit E**.
[12] Microsoft, *The Importance of Two-Factor Authentication*, July 8, 2022, https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/importance-of-two-factor-authentication.

deliberately permitted Plaintiff's confidential information and communications to be accessed, shared, and divulged without authorization from Plaintiff.

37. Recent actions by the Federal Trade Commission ("FTC") underscore the gross negligence and failings of Keffer and Defendant Simmons in failing to ensure that the Athletic Trainer System was configured to default to two-factor or multi-factor authentication for access to its systems containing PII and PHI. In February 2023, the FTC published an article highlighting the importance of multi-factor authentication ("MFA") and stating: "[m]ulti-factor authentication is widely regarded as a critical security practice because it means a compromised password alone is ***not enough*** to take over someone's account."[13]

38. Additionally, the FTC's enforcement actions over the past five years further emphasize the critical and fundamental role MFA plays in an effective data security system, where the FTC has ordered MFA be implemented as part of settlements announced in its data security enforcement actions.[14]

39. Keffer also lacked any effective data auditing controls to monitor activity on its systems, which would have allowed it to detect the massive, years-long data breach on its systems by Defendant Weiss and the resulting cyber voyeurism on Plaintiff Jane Doe and those Class Members similarly situated.

40. Both Keffer and Defendant Simmons had a responsibility and duty to protect the private data of student athletes stored within their systems and to have controls in place to prevent gross invasions of privacy as occurred in this case.

---

[13] Alex Gaynor, *Security Principles: Addressing Underlying Causes of Risk in Complex Systems*, FEDERAL TRADE COMMISSION, Feb. 1, 2023, https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/security-principles-addressing-underlying-causes-risk-complex-systems (emphasis added).

[14] Jim Dempsey, *The FTC's rapidly evolving standards for MFA*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS, Nov. 8, 2022, https://iapp.org/news/a/the-ftcs-rapidly-evolving-standards-for-mfa/.

41. The risk of identity theft and security breaches to access users' private, personal, and confidential information is foreseeable within Simmons and Keffer's information technology systems, and Simmons and Keffer are well aware of the foreseeable risks of data breaches, such as those alleged in this case, that are likely to occur if their practices in detecting, preventing, and mitigating such data breaches are substandard.

C. Defendant Simmons's Failed to Safeguard its Students' Private Information for Nearly a Decade

42. Simmons is a high-level educational institution, with a diverse athletic program, enrolling hundreds of student athletes at any one time across over a dozen sports.

43. In maintaining its highly regarded athletics department and programs, Simmons provides its student athletes with athletic trainers.

44. Simmons had a responsibility and duty to oversee its operations, policies, and procedures, and care for and protect its students.

45. Simmons was required to ensure that students, such as Jane Doe, were not exposed to sexual predators who would invade their privacy.

46. Simmons failed in this duty by failing to take any reasonable action to prevent the harm caused to Jane Doe and other Class Members as alleged in this Complaint.

47. This prolific and egregious breach and violation was entirely preventable by Simmons and Keffer. As noted in a criminal complaint filed by the U.S. Attorney for the Eastern District of Michigan, Defendant Weiss breached the authentication systems of Keffer's and of colleges and universities across this nation by exploiting passwords and other vulnerabilities in their authentication processes. On information and belief, neither Simmons nor Keffer required

that its employees or students implement safeguards like multi-factor authentication to access accounts, a standard practice for all entities collecting PII, especially medical data and PHI.

48. The breach and cyber voyeurism were a direct result of Simmons's and Keffer's failure to implement adequate and reasonable security procedures and protocols necessary to protect Jane Doe and Class Members PII and PHI, leaving the most sensitive and personal information of students, like Jane Doe, vulnerable to exploitation by malicious predators like Defendant Weiss.

49. Simmons was grossly negligent on two fronts: (1) in its hiring and oversight of Keffer, and its entrustment of students' PII and PHI to Keffer; and (2) in its maintenance, oversight, and security of its own internal systems to protect student PII and PHI.

50. Simmons took no reasonable actions to prevent this unauthorized access beforehand despite its duties to students and since discovery of the breaches, has taken no reasonable actions to notify or rectify harm to the victims of Weiss's misconduct and predation.

51. Thousands of students still remain at risk because Simmons and Keffer have failed to undertake any reasonable review of how Jane Doe's private and personal information is secured and who can access such information, and from where.

52. Upon information and belief, to this day, Simmons has not formally informed Class Members impacted by Weiss's cyber voyeurism and misconduct.

D. Simmons was Negligent in Hiring/Contracting with Defendant Keffer and in Entrusting Students PII and PHI to Keffer

53. Simmons provided its student athletes medical treatment, including from athletic trainers.

54. To facilitate that treatment, Simmons contracted with Keffer to use its Athletic Training System application, which required that student athletes provide Simmons and Keffer with sensitive PII and PHI.

55. When collecting that information, Simmons, like Keffer, accepted an obligation to protect that information under contract and statutory principles, including as a "business associate" under HIPAA.

56. Jane Doe and others similar to her entrusted that Simmons and Keffer would safeguard her private information and ensure the security and confidentiality of her data.

57. Simmons and Keffer had, and continue to have, a duty to protect Jane Doe and to take appropriate security measures to protect private, personal, medical and intimate information, communications, and images.

58. Simmons knowingly and deliberately permitted access to and the divulging of Plaintiffs' stored communications through Keffer and failed to take reasonable action to ensure that Keffer protected the privacy of the sensitive information of Jane Doe and others like her.

59. Upon information and belief, Simmons failed to properly investigate Keffer, Keffer's protocols, and failed to adequately monitor or establish safeguards for Keffer's work with the students and their private information to ensure they carried out their duties to safeguard and protect the private information of their students entrusted to them.

60. Simmons was negligent and/or reckless in failing to ensure that media and other private, personal and sensitive information, including but not limited to those of Jane Doe, was securely protected, as Simmons was entrusted to do.

61. Simmons failed to implement security measures necessary to protect their students PII and PHI, including failing to train staff and employees on securing credentials, requiring multi-

or two-factor authentication to use Keffer's Athletic Trainer System, overseeing third-party vendors like Keffer, in which Simmons entrusted students sensitive PII and PHI, and monitoring and auditing access to student files and other private information.

62. In other words, Simmons not only failed to ensure it had implemented sufficient security protocols and procedures across its own systems and staff, but also Simmons failed to ensure Keffer had adequate security measures in place to protect Simmons students' PII and PHI from theft and misuse.

63. Indeed, Simmons lacked adequate training programs to detect and stop breaches like those caused by Defendant Weiss.

64. Simmons and Keffer failed to implement reasonable protective measures to detect Weiss' irregular activity and trespassing, including but not limited to, appropriate authentication tools, behavioral analytics, anomaly detection, machine learning, and real-time monitoring of user activity, looking for deviations from established patterns and suspicious actions, like unusual or repeated login attempts or access to sensitive data, any of which could have prevented Weiss' improper access to private student information.

65. Because both Keffer and Simmons failed to implement basic, industry standard security measures, these Defendants allowed an alleged sexual predator, ex-football coach Matthew Weiss, to access students', particularly female student athletes', most sensitive information for nearly a decade.

66. All Defendants disregarded the rights of Jane Doe and Class Members. Simmons and Keffer knowingly, intentionally, willfully, recklessly and/or negligently provided access to and/or divulged Plaintiffs' private communications stored in their facilities; failed to take adequate and reasonable measures to ensure their data systems were protected against unauthorized

intrusions; failed to disclose that they did not have adequately robust computer systems and security practices to safeguard private information; failed to take standard and reasonably available steps to prevent the data breach and cyber voyeurism; failed to properly train their staff and employees on proper security measures; and failed to provide Jane Doe and the Class Members prompt notice of the data breach and cyber voyeurism.

67. Simmons's and Keffer's conduct amounts to a violation of the duties they owed to Jane Doe under common law tort claims and state and federal statutory law, rendering them liable to Jane Doe and the Class Members for the harms caused by this egregious and preventable cyber voyeurism and invasion of privacy. Defendant Weiss is equally liable for the harms inflicted on Jane Doe and the Class Members by his intentional hacking and theft of their private information under tort and statutory law.

68. Jane Doe and the punitive Class Members are current and former students at Simmons and other affected institutions in the United States that were specifically targeted by Weiss and harmed by the violation of their privacy.

69. Jane Doe and the punitive Class Members suffered injury as a result of Defendants' conduct. These injuries included: invasion and loss of privacy, loss of dignity, humiliation, embarrassment, and severe emotional distress.

70. Jane Doe seeks to remedy these harms on behalf of herself and all similarly situated individuals whose private information was accessed by Weiss.

71. Jane Doe seeks remedies including, but not limited to, compensatory damages, nominal damages, punitive damages, and reimbursement of out-of-pocket costs. Jane Doe 1 also seeks injunctive and equitable relief to prevent future injury on behalf of herself and the putative Class Members.

E. Jane Doe's Allegations

72. Plaintiff Jane Doe is a former student athlete at Simmons.

73. While in school at Simmons, Jane Doe participated in the Cross-Country program while Defendant Weiss's data breach and cyber voyeurism was ongoing.

74. As a student athlete, Jane Doe received treatment from Simmons's athletic trainer staff, requiring her to disclose information about her treatment, including height, weight, injuries, medications, treatment plans, and analysis on performance and recovery. To receive treatment, Jane Doe was required to use the Keffer Athletic Trainer System, and the PII and PHI Jane Doe disclosed was saved on the Keffer Athletic Trainer System.

75. As a student, Jane Doe was required to disclose personal information to Simmons and was issued a Simmons email account where she stored sensitive, personal information.

76. Because Keffer and Simmons never implemented the security safeguards needed to protect Jane Doe's PII and PHI, Defendant Weiss compromised the PII and PHI belonging to every student whose information was saved by Simmons and/or Keffer's Athletic Trainer System, including, on information and belief, Jane Doe's private and personal information.

77. Defendant Weiss compromised all information that was saved in Simmons and/or Athletic Trainer System databases, including Plaintiff's treatment information, injury information, height, weight, and other highly sensitive information.

78. Jane Doe has received notice from the U.S. Department of Justice Victim Notification System that she was identified as a potential victim in the federal criminal case against Defendant Weiss.[15]

[15] *See* **Exhibit A**.

79. After receiving notice from the federal government that read: "If you are receiving this notification, it means that information of yours was found in possession of the defendant,"[16] Jane Doe felt violated, deeply disturbed, humiliated, embarrassed, and extremely emotionally distressed; and is experiencing physical manifestations of the stress and anxiety caused by this egregious violation of her privacy, symptoms that are further exacerbated by the fact that Jane Doe still does not have a full and complete understanding of the data breach and cyber voyeurism perpetrated by Defendant Weiss.

80. This cyber voyeurism invaded Plaintiff's privacy and has devastated her personally and emotionally, as her highly sensitive private information was stolen by an alleged predator under circumstances that were entirely preventable by Defendant Simmons and Defendant Keffer.

81. Upon information and belief, the United States Department of Justice is in the process of notifying thousands of potential victims that their privacy was breached.

82. As a direct result of the negligence, recklessness, and misconduct of the Defendants, Jane Doe and those similarly situated have incurred substantial monetary and emotional damages exceeding $5,000,000, exclusive of costs, interest, and fees.

F. Keffer and Simmons Failed to Properly Protect Plaintiff's and Class Members' PII and PHI

83. Defendants Keffer and Simmons did not use reasonable security procedures and practices, including leaving data unencrypted, appropriate to the nature of the sensitive PII and PHI it was maintaining for Plaintiff and Class Members, causing the breach of PII and PHI for 150,000 students and former students, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for approximately 3,330 students and former students.

[16] *Id.*

84. The FTC takes action when companies make promises to safeguard personal information and then fail to live up to those promises, including by promulgating numerous guides which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

85. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelin1es for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[17] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[18]

86. The FTC further recommends that companies not maintain PII and PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

87. Defendants Keffer and Simmons failed to properly implement these basic data security practices explained and set forth by the FTC.

[17] FEDERAL TRADE COMMISSION, *Protecting Personal Information: A Guide for Business*, Oct. 2016, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.
[18] *Id.*

88. Defendants Keffer's and Simmons's failure to employ reasonable and appropriate measures to protect against unauthorized access to PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

89. A systematic, years-long breach such as the ones Defendants Keffer and Simmons experienced is also considered a breach under the HIPAA Rules because there is unauthorized access to PHI that is not permitted under HIPAA.

90. A breach under the HIPAA Rules is defined as, "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." 45 C.F.R. 164.40.

91. Data breaches are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. 45 C.F.R.164.308(a)(6).[19]

92. Defendants Keffer's and Simmons's data breach was the foreseeable consequence of a combination of deficiencies that demonstrate Defendants Keffer and Simmons failed to comply with safeguards mandated by HIPAA.

[19] U.S. DEPT OF HEALTH AND HUM. SERVS., *FACT SHEET: Ransomware and HIPPA*, July 11, 2016, at 4, https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.

G. Defendants Simmons and Keffer Failed to Comply with Industry Standards

93. Defendants Keffer and Simmons did not utilize industry standards, like encryption, appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the breach of PII and PHI for approximately 150,000 students and former students, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for 3,330 students and former students.

94. As explained by the FBI, "[p]revention is the most effective defense against cyberattacks] and it is critical to take precautions for protection."[20]

95. To prevent and detect data breaches, including the breach here that resulted in theft of PII and PHI and cyber voyeurism, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of cyberattacks and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

[20] FEDERAL BUREAU OF INVESTIGATION, *How to Protect Your Networks from RANSOMWARE*, at 3, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Dec. 20, 2024).

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common cyberware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units. [21]

96. To prevent and detect cyberattacks, including the cyberattack that resulted in the data breaches and cyber sexual assaults, Defendants Keffer and Simmons could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure Internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management

[21] *Id*. at 3-4.

- Perform regular audit; remove privileged credentials

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[22]

97. As described above, experts studying cyber security routinely identify medical facilities as being particularly vulnerable to cyberattacks because of the value of the private information they collect and maintain.

98. Several best practices have been identified that at a minimum should be implemented by institutions such as Defendants Keffer and Simmons, including, but not limited to, the following: educating all employees on security; strong passwords; multi-layer security,

[22] MICROSOFT, *Human-Operated Ransomware Attacks: A Preventable Disaster*, Mar. 5, 2020, https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

99. Other standard cybersecurity best practices include installing appropriate malware detection software; monitoring and limiting access to network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

100. Given that Defendants Keffer and Simmons were storing the private information of 150,000 individuals combined, Defendants Keffer and Simmons could and should have implemented all of the above measures to prevent cyberattacks, along with two- or multi-factor authentication as discussed earlier in this Complaint.

101. The occurrence, scope, and duration of the breach and cyber voyeurism indicates that Defendants Keffer and Simmons failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the theft of approximately 150,000 students' and former students' PII and PHI, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for 3,330 students and former students.

H. Defendants Keffer and Simmons Failed to Properly Protect PII and PHI

102. Defendants Keffer and Simmons breached their obligations to Jane Doe and Class Members and were otherwise grossly negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches, cyber-attacks, and hacking incidents;

b. Failing to adequately protect students' private information;

c. Failing to properly monitor its own computer networks for existing or prior intrusions;

d. Failing to test and assess the adequacy of its data security system;

e. Failing to develop adequate training programs related to the proper handling of emails and email security best practices;

f. Failing to adequately fund and allocate resources for the necessary design, operation, maintenance, and updating required to meet industry standards for data protection;

g. Failing to require a data security system to ensure the confidentiality and integrity of electronic PHI its network created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

h. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access to only those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

i. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

j. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

k. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 C.F.R. § 164.306(a)(2);

l. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

m. Failing to ensure that it was compliant with HIPAA security standard rules by its workforce, in violation of 45 C.F.R. § 164.306(a)(4);

n. Failing to train all members of its workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its

workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

o. Failing to ensure that the electronic PHI it maintained is unusable, unreadable, or indecipherable to unauthorized individuals, as Defendants had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." (45 C.F.R. § 164.304 definition of encryption);

p. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;

q. Failing to adhere to industry standards for cybersecurity.

103. As the result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendants Keffer and Simmons negligently and unlawfully failed to safeguard Plaintiff's and Class Members' private, sensitive information.

104. Defendant Simmons was also grossly negligent in its failure to oversee the data security practices of third-party vendor—Keffer—in which it entrusted the sensitive private information of its students and former students.

105. Accordingly, as outlined below, Plaintiff and Class Members have already been severely harmed by this egregious violation of their privacy by Defendant Weiss.

CLASS ALLEGATIONS

106. Plaintiff files this lawsuit both individually and as representative of all others similarly situated pursuant to Fed. R. Civ. P. 23 on behalf of the following Class: All students whose personal data, images, information, social media, or videos were accessed by Weiss without authorization ("Class Members").

107. In addition, Plaintiff believes a subclass may be appropriate for all class members who receive notice from the United States Department of Justice as to the likely violation of their

privacy and rights by Weiss. Therefore, Plaintiff pleads a subclass as follows: All students whose personal data, images, information, social media, or videos were accessed by Weiss without authorization and who received a notice letter from the United States Department of Justice as to Weiss ("DOJ Letter Sub-Class").

108. Excluded from the Class are: (a) Defendants and any entity or division in which Defendants have a controlling interest, and their legal representatives, officers, directors, assigns, and successors; (b) the Judge to whom this case is assigned and the Judge's staff; and (c) the attorneys representing any parties to this Class Action.

109. Plaintiff reserves the right to modify or amend the definition of the proposed class and/or sub-classes before the Court determines whether certification is appropriate.

A. Numerosity – Fed. R. Civ. P. 23(a)(1)

110. Law enforcement officials have disclosed that the number of victims is significant and exceeds one thousand satisfying the numerosity requirement. Although the exact number of Class Members is uncertain at this time and it will certainly be ascertained through appropriate discovery, the number is great enough such that joinder is impracticable.

111. The members of the Class are so numerous and geographically dispersed that individual joinder of all members is impracticable.

112. Similarly, Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, Internet postings, and/or published notice.

113. Class Members are readily identifiable from information and records in the possession of the federal and state authorities, Simmons, and Keffer.

114. Electronic records maintained by Simmons and Keffer can confirm the identification of Class Members.

B. Commonality and Predominance – Fed. R. Civ. P. 23(a)(2) and 23(b)(3)

115. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and the other Class Members. Similar or identical violations, practices, and injuries are involved, and the burden of proof to establish violations of those rights involve uniform, objective questions of fact and law, both for Plaintiff and for Defendants.

116. The common questions of fact and law existing as to all Class Members predominate over questions affecting only individual class members. The evidence required to advance Plaintiff's and Class Members' claims are the same, common to all; as is true of the evidence Defendants will likely rely upon in defense of this action. Thus, the elements of commonality and predominance are both met.

117. For example, establishing the facts of how, where, who, when, and through what means the invasions of Plaintiff's and other Class Members occurred are identical.

118. Defendants' actions, inactions, negligence, and recklessness apply commonly to Plaintiff and Class Members.

119. The theft of images and invasions by Weiss and the improper conduct of accessing private information through unsecure systems without permission is common to all Class Members and has caused injury to the Plaintiff and Class Members in common manners.

120. The First Circuit has held that "[a]s long as a sufficient constellation of common issues binds class members together," notwithstanding the existence of some individualized issues, a class may still be certified under Rule 23(b)(3). *Waste Management Holdings, Inc. v. Mowbray*,

208 F.3d 288, 296 (1st Cir. 2000). Liability will be tested under the same standard, equally applicable for all class members, making certification appropriate under Rule 23(b)(3).

121. The majority of legal and factual issues of the Plaintiff and the Class Members predominate over any individual questions, including:

(a) Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members private information;

(b) Whether Defendants Keefer and Simmons failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the hacking incident and cyber sexual assault;

(c) Whether Defendants Keefer and Simmons's data security systems prior to and during the data breach and cyber voyeurism complied with applicable data security laws and regulations;

(d) Whether Defendants Keefer's and Simmons's data security systems prior to and during the data breach and cyber voyeurism were consistent with industry standards;

(e) Whether Defendants Keefer and Simmons owed a duty to Plaintiff and Class Members to safeguard their private information;

(f) Whether Defendants Keefer and Simmons breached their duty to Plaintiff and Class Members to safeguard their private information;

(g) Whether Defendant Simmons was grossly negligent and/or negligent in its oversight of Defendant Keffer;

(h) Whether Defendant Simmons or Keffer knew or should have known that their data security systems and monitoring processes were deficient;

(i) Whether Defendants Keefer and Simmons owed a duty to provide Plaintiff and Class Members timely notice of the data breach and cyber voyeurism, and whether Defendants Keefer and Simmons breached that duty to provide timely notice;

(j) Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

(k) Whether Defendants' conduct was negligent or grossly negligent;

(l) Whether Defendants' conduct was per se negligent;

(m) Whether Defendants' conduct violated federal laws;

(n) Whether Defendants' conduct violated state laws;

(o) Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or punitive damages; and

(p) Other common questions of fact and law relative to this case that remain to be discovered.

122. Resolving the claims of these Class Members in a single action will provide benefit to all parties and the Court by preserving resources, avoiding potentially inconsistent results, and providing a fair and efficient manner to adjudicate the claims.

123. Predominance does not require Plaintiff to prove an absence of individualized damage questions. *In re Suffolk Univ. COVID Refund Litig.*, No. 20-10985-WGY, 2022 U.S. Dist. LEXIS 185297, at *5-6 (D. Mass. Oct. 11, 2022) (finding that "the need for individualized damage decisions does not ordinarily defeat predominance where there are still disputed common issues as to liability.") (citing *Tardiff v. Knox Cty.*, 365 F.3d 1, 6 (2004)).

C. Typicality – Fed. R. Civ. P. 23(a)(3)

124. Plaintiff's claims are typical of those of other Class Members because all had their private information compromised as a result of the breach and cyber voyeurism and Defendants' malfeasance.

125. Plaintiff's claims are typical of the Class Members because they are highly similar and the same and related in timing, circumstance, and harm suffered. To be sure, there are no defenses available to Defendants that are unique to individual Plaintiffs. The injury and causes of actions are common to the Class as all arising from the same statutory and privacy interests.

126. In *Halliburton Co. v. Erica P. John Fund, Inc.,* 573 U.S. 258, 276 (2014) the Supreme Court concluded that so long as plaintiffs could show that their evidence is capable of proving the key elements to plaintiffs' claim on a class-wide basis, the fact that the defendants would have the opportunity at trial to rebut that presumption as to some of the plaintiffs did not raise individualized questions sufficient to defeat predominance. "That the defendant might attempt to pick off the occasional class member here or there through individualized rebuttal does not cause individual questions to predominate." *Id.*

127. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

128. The need to conduct additional post certification stage discovery, such as further file review or class member surveys, to eliminate uninjured persons after trial, does not act as a bar to certification. *Astrazeneca AB v. UFCW (In re Nexium Antitrust Litig.),* 777 F.3d 9, 19 (1st Cir. 2015). "At the class certification stage, the court must be satisfied that, prior to judgment, it will be possible to establish a mechanism for distinguishing the injured from the uninjured class members. The court may proceed with certification so long as this mechanism will be 'administratively feasible,' and protective of defendants' Seventh Amendment and due process rights. *Id.*; *see also* American Law Institute, Principles of the Law: Aggregate Litigation, §§ 2.02(a)(3), 2.07(d) cmt. j (2009) (indicating that the court should exercise discretion to authorize aggregate treatment only if it would "not compromise the fairness of procedures for resolving any remaining issues presented by such claims" and that "due process in aggregation . . . extend[s] to persons opposing the aggregate group litigating related claims on an aggregate basis."). By placing

the validation of injury step at the end of the class trial process, no injured class members are left out, and at the same time, Defendants are not at risk for paying any uninjured class members.

D. Adequacy of Representation – Fed. R. Civ. P. 23(a)(4)

129. Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that she has no interests that are in conflict with those of the Class Members. In addition, she has retained counsel competent and experienced in complex class action litigation, and she will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and her counsel.

E. Superiority of Class Treatment – Fed. R. Civ. P. 23(b)(3)

130. The class action is superior to any other available procedures for the fair and efficient adjudication of these claims, and no unusual difficulties are likely to be encountered in the management of this class action.

131. The superiority analysis required to certify a class looks at pertinent factors in assessing superiority, such as "the class members' interests in individually controlling the prosecution or defense of separate actions" and "the likely difficulties in managing a class action." *Barrett v. H&R Block, Inc.*, No. 08-10157-RWZ, 2011 U.S. Dist. LEXIS 30713, at *25 (D. Mass Mar. 25, 2011) (citing Fed. R. Civ. P. 23(b)(3)). Superiority exists where "there is a real question whether the putative class members could sensibly litigate on their own for these amounts of damages, especially with the prospect of expert testimony required." *Gintis v. Bouchard Transp. Co., Inc.*, 596 F.3d 64, 68 (1st Cir. 2010).

132. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable.

133. It would be an unnecessary burden upon the court system to require these individual Class Members to institute separate actions. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

134. Pursuing this matter as a class action is superior to individual actions because:

(a) Separate actions by Class Members could lead to inconsistent or varying adjudications that would confront Defendants with potentially incompatible standards of conduct;

(b) Many victims will not come forward without a certified class;

(c) Final equitable relief will be appropriate with respect to the entire Class as a whole for monitoring, protection, therapy and other equitable forms of relief that may be provided;

(d) This action is manageable as a class action and would be impractical to adjudicate any other way;

(e) Absent the class action, individual Class Members may not know if their privacy was invaded; where such images are currently being stored, or are accessible by others; and their injuries are likely to go unaddressed and unremedied; and,

(f) Individual Class members may not have the ability or incentive to pursue individual legal action on their own.

F. Particular Issues – Fed. R. Civ. P. 23(c)(4)

135. In the event unforeseen issues preclude class certification under Fed. R. Civ. P. 23(b)(3), the case is still appropriate for class certification under Fed. R. Civ. P. 23(c)(4), as to the particular issues of liability.

136. Defendants have acted or refused to act on grounds generally applicable to Plaintiff and the other members of the Class, thereby making declaratory relief, as described below, with respect to the Class as a whole.

COUNT I
VIOLATIONS OF THE COMPUTER FRAUD AND ABUSE ACT – 18 U.S.C. § 1030
(DEFENDANT WEISS)

137. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

138. Weiss violated the Computer Fraud and Abuse Act by unlawfully accessing Plaintiff's private information without authorization.

139. Weiss' actions constituted a violation of the Act because by entering Plaintiff's social media, email, and/or cloud storage accounts, and extracting sensitive private information of students, he "intentionally access[ed] a computer without authorization." 18 U.S.C. § 1030(a)(2)(C).

140. Weiss's actions were deliberate because he knew he was unauthorized and proceeded nevertheless.

141. Under 18 U.S.C. § 1030(g), Plaintiffs may recover damages in this civil action from Weiss along with injunctive relief or other equitable relief.

142. Given the willful violations committed by Weiss, resulting in significant damage, harm, humiliation, and distress to Plaintiffs and other Class Members, Plaintiffs should be awarded all appropriate damages in this matter.

COUNT II
VIOLATIONS OF THE STORED COMMUNICATIONS ACT – U.S.C. § 2701
(DEFENDANTS WEISS, KEFFER, AND SIMMONS)

143. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

144. Plaintiffs allege that Defendants Weiss, Keffer, and Simmons violated the Stored Communications Act.

145. The Stored Communications Act, 18 U.S.C. § 2701 et seq., prohibits the unauthorized access of web-based cloud storage, email, and social media accounts such as those at issue and other accounts hosted by Defendants Simmons and Keffer that contain personal, private, and intimate information and communications about and relating to Plaintiffs and others situated similarly to Plaintiffs.

146. Specifically, under 18 U.S.C. § 2701(a), it is unlawful for any person to: (1) intentionally access without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceed an authorization to access that facility; and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such system.

147. Under 18 U.S.C. § 2702, it is unlawful for a person or entity providing an electronic communication service to the public to knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service or to divulge to any person or entity the contents of any communication which is carried or maintained on that service on behalf of a subscriber or customer of such service, solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

148. Plaintiffs' electronic information and communications were in electronic storage and clearly fall within the scope of the statute.

149. Defendant Weiss was not authorized to access or divulge the content of Plaintiffs' private communications by for any purpose.

150. The information, messages, files, and media were accessed by Weiss without authorization.

151. Weiss's access without authorization was deliberate.

152. There is no manner in which Plaintiff's and class member's private information, messages, files, and media could have been obtained without unauthorized access and would not have been obtained without unauthorized access had Defendants Keffer and Simmons not knowingly divulged or permitted access to such information, through Defendants' systems and/or Keffer's ATS application, despite knowing that the information would not be protected.

153. Under Section 2707 of the Stored Communications Act, individuals may bring a civil action for the violation of this statute.

154. This law imposes strict liability on violators.

155. The statute provides that a person aggrieved by a violation of the act may seek appropriate relief including equitable and declaratory relief, actual damages or damages no less than $1,000 punitive damages, and reasonable attorney's fee[s] and other litigation costs reasonably incurred according to 18 U.S.C. § 2707(b)-(c).

156. Defendants' access to and divulging of Plaintiffs' private, personal, and intimate information, messages, files, and media constituted a violation of 18 U.S.C. §§ 2701 and 2702.

157. Defendants Keffer, Simmons, and Weiss knew they did not have authority to access and divulge Plaintiffs' private, personal, and intimate information, messages, files, and media but did so anyway.

158. Defendants' knowing or intentional conduct led to multiple violations of the Stored Communications Act.

159. As a result of these violations, Plaintiffs have incurred significant monetary and nonmonetary damages as a result of these violations of the Stored Communications Act, and Plaintiffs seek appropriate compensation for their damages.

160. Under the statute, Plaintiffs should be granted the greater of (1) the sum of their actual damages suffered and any profits made by Simmons and Weiss as a result of the violations or (2) $1,000 per violation of the Stored Communications Act.

161. Given these violations were deliberate, the Court should assess punitive damages against Defendants as well.

162. Plaintiffs should also be granted reasonable attorney fees and costs.

COUNT III
VIOLATIONS OF TITLE IX – 20 U.S.C. § 1681(A)
(DEFENDANT SIMMONS)

163. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

164. Title IX mandates that "No person in the United States shall on the basis of sex, be ... subject to discrimination under any education program or activity receiving Federal financial assistance ..."

165. Each Plaintiff and Class Member is a "person" under the Title IX statutory language.

166. Weiss specifically targeted women in his unwanted invasions of privacy and his misconduct is discrimination on the basis of sex.

167. Defendant Simmons receives federal financial support for its educational programs and is therefore subject to the provisions of Title IX of the Education Act of 1972, 20 U.S.C. § 1681(a), *et seq.*

168. Defendant Simmons, under Title IX, is obligated to investigate allegations of sexual harassment.

169. Defendant Simmons was aware of the sensitive nature of the private and personal information of Plaintiffs to which Weiss was able to access given his role.

170. Defendant Simmons acted with deliberate indifference to sexual harassment by:

a. Failing to protect Plaintiffs and others as required by Title IX;

b. Neglecting to adequately investigate and address the complaints regarding the deeply sensitive information Plaintiffs provided;

c. Failing to institute corrective measures to prevent Weiss from sexually harassing other students; and

d. Failing to adequately investigate the other multiple acts of deliberate indifference.

171. Simmons and its Trustees acted with deliberate indifference as their lack of response to the sexual harassment was clearly unreasonable in light of the known circumstances.

172. Defendant Simmons' failure to promptly and appropriately protect, investigate, and remedy and respond to the sexual harassment of women has effectively denied them equal educational opportunities at the University, including access to medical care and sports training.

173. At the time the Plaintiff and Class Members received some medical training services from Simmons, they did not know Simmons and Keffer failed to adequately consider their safety including in their engagement, hiring, training, and supervision of Weiss.

174. As a result of Defendant Simmons' deliberate indifference, Plaintiff and Class Members have suffered loss of educational opportunities and/or benefits.

175. Plaintiff and Class Members have and incurred, and will continue to incur, attorney's fees and costs of litigation.

176. At the time of Defendants' misconduct and wrongful actions and inactions, Plaintiff and Class Members were unaware, and or with reasonable diligence could not have been aware, of Defendants' institutional failings with respect to their responsibilities under Title IX.

177. Defendant Simmons maintained a policy and/or practice of deliberate indifference to protection of female student athletes.

178. Defendants' policy and/or practice of deliberate indifference to protection against the invasion of privacy for female athletes created a increased risk of sexual harassment.

179. Despite being able to prevent these privacy violations and acts of harassment, Defendants failed to do so.

180. Because of Defendant Simmons's policy and/or practice of deliberate indifference, Plaintiff and Class Members had their privacy invaded and were sexually harassed by Weiss.

181. Plaintiff and Class Members should be awarded all such forms of damages in this case for Defendant Simmons's conduct that caused great damage, humiliation, and embarrassment to Plaintiffs and the Class.

COUNT IV
INVASION OF PRIVACY INTRUSION UPON SECLUSION

182. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

183. Plaintiff's and Class Members' personal social media files, videos, and other images were each in electronic storage and were intended to be kept private.

184. Weiss unlawfully accessed this information.

185. His actions were not authorized.

186. This information would not have been obtained absent the negligence and misconduct of Simmons and Keffer.

187. Plaintiff and Class Members never granted permission to such access.

188. Plaintiff and Class Members feel embarrassed, ashamed, humiliated, and distressed that their private information has been accessed by strangers and third parties.

189. Plaintiff's and Class Members' social media data, images, and other media are private information.

190. Plaintiff and Class Members had the right to expect all this information would remain private.

191. The methods Weiss used to access such information was objectively unreasonable.

192. As a result of Weiss' actions, Plaintiff and Class Members have incurred significant damages as a result of Defendants' actions and request the appropriate damages.

COUNT V
NEGLIGENCE and GROSS NEGLIGENCE

193. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

194. Plaintiff's and Class Members' personal and private information, data, and media was in electronic storage and expected to remain private.

195. That private and personal information, data, and media was accessed by Weiss unlawfully.

196. Weiss' actions were not lawful.

197. The information, data, and media could not have been accessed but for the Non-Individual Defendants' lack of monitoring and supervision of Weiss.

198. Plaintiff and Class Members did not authorize the access to such information, data, and media.

199. Plaintiff and Class Members are embarrassed, ashamed, humiliated, and mortified that their private information has been accessed by total strangers and third parties.

200. Plaintiff's and Class Members' had a right to keep such information, data, and media private.

201. Plaintiff and Class Members entrusted Defendant Simmons and its Trustees to ensure methods were undertaken to secure, safeguard, and protect against authorized access to their private information.

202. Keffer was entrusted to keep Plaintiff's and Class Members' private information private.

203. Upon information and belief, Simmons and Keffer admitted that Plaintiff and Class Members expected each of them to take reasonable measures to maintain the privacy of their private information.

204. Defendant Simmons breached their duties to Plaintiff and Class Members by failing to consider, implement, or follow a policy to oversee how or whether Keffer conducted its operations in a manner that would have in any manner monitored, supervised, and ensured that

engagement. retention and/or employment of Weiss would not result in a breach of the privacy Plaintiff and Class Members entrusted to Defendant Simmons.

205. Plaintiff and Class Members entrusted Defendant Simmons and its Trustees to take measures to ensure Weiss did not gain unauthorized access to their private information, data, and media.

206. Defendant Simmons failed in this duty by failing to take any action to prevent the harm caused to Plaintiff and Class Members as alleged in this Complaint, including but not limited to the inaction of failing to implement a policy to monitor, supervise, and oversee Weiss, or ensure more than one person is verifying that such sensitive and personal and private information is kept confidential.

207. Defendant Simmons were supposed to, but failed, to establish a policy, including to monitor personnel, including but not limited to Weiss, so that students on the campus are protected from their privacy being invaded.

208. Defendant Simmons failed to provide security to Plaintiffs and to other student athletes to be able to be treated by athletic professionals who do not invade their privacy.

209. Keffer recklessly failed to ensure media and information of and pertaining to student athletes including but not limited to Plaintiff and Class Members was safely provided and stored even after Plaintiff and others similar to them entrusted Keffer to do so.

210. Defendant Simmons had an obligation to support Plaintiff and Class Members, and to develop the campus, its operations including student services, and admissions, and financial aid, among others, in a way that at least considered having and executing security measures to protect the personal, private, and intimate images and information of the Plaintiff and others similar to them.

211. Defendant Simmons breached those duties when they failed to implement security measures to protect the private and personal data, information, and media of Plaintiffs was not unlawfully accessed.

212. Defendant Simmons had a duty but failed to learn, enact, or implement any security measures to protect the personal, private, and intimate images and information of the Plaintiff and Class Members.

213. Given the sensitive nature of the Plaintiffs' private information, Simmons and Keffer knew of and, as detailed herein, breached their heightened duties to safeguard and protect Plaintiff's and Class Members' privacy by failing to implement security measures, and that recklessness exposed Plaintiff, the Class, and their private and personal data, information, and media.

214. Defendant Simmons' failures and omissions in these respects was so reckless that it shows a substantial lack of concern for injuries to Plaintiff and the Class.

215. Defendant Simmons's failures and omissions in these respects was so reckless that it shows a substantial lack of concern for injuries to Plaintiff and the Class.

216. Keffer's failures and omissions in these respects was so reckless that it shows a substantial lack of concern for injuries to Plaintiff and the Class.

217. Plaintiff and Class Members have incurred significant damages as a result of Defendants' actions, and should be awarded damages accordingly.

RELIEF

WHEREFORE, Plaintiff prays this Court grant the following relief:

a. Enter a judgment encompassing the relief requested above, plus significant compensatory damages exceeding $5,000,000.00 together with costs, interest and attorney fees, against Defendants, and such other relief to which they are entitled;

b. An order certifying the proposed Class and Subclasses; designating Plaintiff as the named representative of the respective Class Members; and appointing her counsel as Class Counsel;

c. All such equitable relief as the Court deems proper and just, including but not limited to, declaratory relief;

d. Award Plaintiff costs, attorney fees as well as interest from the date of Judgment until paid; and

e. Grant such further relief as is agreeable to equity and good conscience.

JURY DEMAND

For all triable issues, a jury is hereby demanded.

Respectfully Submitted,

Dated: April 28, 2025

The Plaintiff,
Jane Doe
By her attorneys,

/s/ Paula S. Bliss

Paula S. Bliss (BBO# 652361)
Kimberly A. Dougherty (BBO# 658014)
Justice Law Collaborative, LLC
210 Washington Street
North Easton, MA 02356
Telephone: (508) 230-2700
Facsimile: (285) 278-0287
paula@justicelc.com
kim@justicelc.com

Megan Bonanni (P52079)*
Kevin M. Carlson (P67704)*
Beth M. Rivers (P33614)
Danielle Y. Canepa (P82237)
Pitt McGehee Palmer Bonanni & Rivers
117 W. Fourth Street, Suite 200

Royal Oak, MI 48067
(248) 398-9800
mbonnani@pittlawpc.com
kcarlson@pittlawpc.com
brivers@pittlawpc.com
dcanepa@pittlawpc.com

Lisa M. Esser (P70628)*
Richard L. Groffsky (P32992)*
Jason J. Thompson (P47184)*
Matthew G. Curtis (P37999)*
SOMMERS SCHWARTZ, P.C.
One Towne Square, 17th Floor
Southfield, MI 48076
(248) 355-0300
LEsser@sommerspc.com
rgroffsky@sommerspc.com
JThompson@sommerspc.com
MCurtis@sommerspc.com

Ryan Clarkson*
Bryan Thompson*
Timothy Giordano
Yana Hart
Clarkson Law Firm
22525 Pacific Coast Highway
Malibu, CA 90265
(213) 471-2599
rclarkson@clarksonlawfirm.com
bthompson@clarksonlawfirm.com
tgiordano@clarksonlawfirm.com
yhart@clarksonlawfirm.com

**Pro hac vice* forthcoming