Exhibit A1

IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE

MICHAEL HARRIS, CHRISTOPHER VAUGHT, LUCRESIA CAMPBELL, CALEB NABORS, KATELYN BUTLER, BRITTANY KUBBA, AND DENNIS GOODINE, *individually and on behalf of all others similarly situated,* Plaintiffs, v. **LEE UNIVERSITY**, Defendant.	Case No.: 1:25-cv-107 Class Action Hon. Curtis Collier **JURY TRIAL DEMANDED**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Michael Harris, Christopher Vaught, Lucresia Campbell, Caleb Nabors, Katelyn Butler, Brittany Kubba, and Dennis Goodine ("Plaintiffs"), individually and on behalf of all others similarly situated (collectively, "Class Members"), by and through the undersigned attorneys, bring this Consolidated Class Action Complaint against Defendant Lee University, ("Defendant"), and alleging as follows, based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to them, which is based on personal knowledge:

NATURE OF THE CASE

1. Plaintiffs bring this class action against Defendant for its failure to secure and safeguard personally identifiable information ("PII") including full names, Social Security numbers, driver's license numbers, government-issued ID number (e.g. passport, state ID card), financial information (e.g. account number, credit or debit card number), and medical information belonging to approximately 136,928 individuals, including Plaintiffs.[1]

[1] https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage.

2. Defendant is a private Christian university based in Cleveland, Tennessee.[2]

3. On or about March 25, 2025, Defendant began sending Plaintiffs and other Data Breach victims a Notice of Data Security Incident letter (the "Notice Letter"), informing them that:

> On March 19, 2025, Lee University learned that some personal information relating to its students, donors, and current or former employees was contained within a data set which was subject to a data security incident. Lee University discovered a cybersecurity incident on March 22, 2024, and immediately began an investigation of the matter with the assistance of engaged independent cybersecurity experts. The investigation determined that files containing personal information may have been accessed or acquired without authorization. Lee University then undertook an investigation to understand whether data was potentially involved and, if so, what that data was so that notification could be provided. The comprehensive review and processes needed to identify contact information for potentially affected concluded on March 19, 2025. As a result of that investigation, Lee University learned that some personal information of individuals was contained within the involved data.[3]

4. Omitted from the Notice Letter were the identity of the cybercriminals who perpetrated this Data Breach, the date(s) of the Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their PII remains protected.

5. Concerningly, the cybercriminals that obtained Plaintiffs' and Class Members' PII appear to be the notorious ransomware group "Medusa."[4]

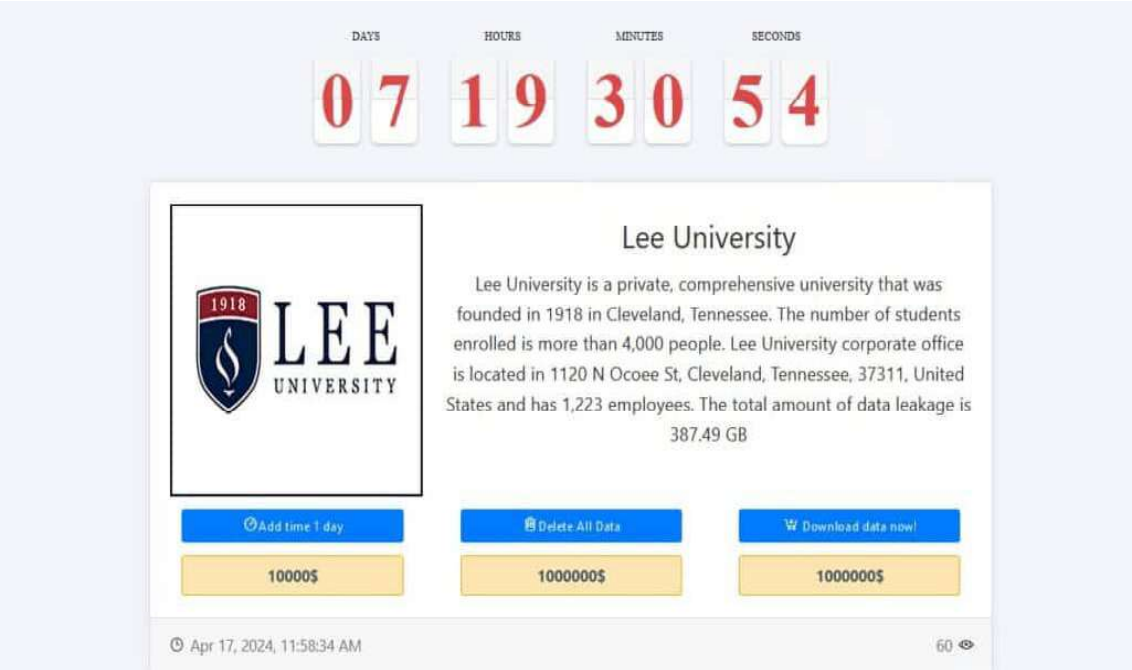
---

[2] https://www.leeuniversity.edu/about/.

[3] https://mm.nh.gov/files/uploads/doj/remote-docs/lee-university-20250325.pdf (last accessed August 19, 2025).

[4] Medusa is a Ransomware as-a-Service (RaaS) variant that has become a top ten ransomware actor since 2023. Check Point, *Medusa Ransomware Group: A Rising Threat in 2025*, https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/medusa-ransomware-group/ (last accessed August 19, 2025). RaaS operators maintain the ransomware malware, offer a payment portal for victims, and may provide the "customer service" that victims might need (since many ransoms are demanded in Bitcoin or other cryptocurrencies). Their affiliates are responsible for spreading the ransomware, and any ransoms paid are split between the operators

6. Medusa claimed responsibility for the attack in April of 2024, saying it stole nearly 388 GB of data from the school and demanding $1 million in ransom:[5]



7. As part of its business, and to generate profit, Defendant obtains and stores Plaintiffs' and Class Members' Private Information.[6]

8. By taking possession and control of Plaintiffs' and Class Members' Private Information, Defendant assumed a duty to securely store and protect Plaintiffs' and Class Members' Private Information.

---

and the affiliate. Check Point, *Ransomware as-a-Service (RaaS)*, https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/ransomware-as-a-service-raas/(last accessed August 19, 2025).

[5] Paul Bischoff, *Lee University notifies 137K people of data breach that compromised SSNs, credit cards, and medical info*, COMPARITECH (Apr. 11, 2025) https://www.comparitech.com/news/lee-university-notifies-137k-people-of-data-breach-that-compromised-ssns-credit-cards-and-medical-info/ (last accessed August 19, 2025).

[6] *See, e.g.*, *Privacy Policy,* https://www.leeuniversity.edu/privacy-policy/ (providing "We may use your personal information for our own business purposes, such as for undertaking internal research for technological development and demonstration," and "We may share or transfer your information in connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of our business to another company."

9. Defendant breached this duty and betrayed Plaintiffs' and Class Members' trust by failing to properly safeguard and protect their Private Information, thus enabling cybercriminals to access, acquire, appropriate, compromise, disclose, encumber, exfiltrate, release, steal, misuse, and/or view it.

10. According to Defendant's Notice, Defendant discovered the cyberattack on March 22, 2024. At that time, Defendant retained experts who conducted a forensic investigation which confirmed that "some personal information of individuals" was contained "within a data set which was subject to a data security incident."[7]

11. However, despite apparently learning of the Data Breach on or about March 22, 2024, Defendant did not begin informing Plaintiffs, Class Members or other current and former students of the Data Breach until March 25, 2025—a astonishing ***368 days*** after the Data Breach**.**

12. Furthermore, Defendant's delay in notifying Plaintiffs and Class members of the Data Breach is in direct violation of Defendant's responsibilities under the data breach notification statute in Tennessee. *See* TN Code § 47-18-2107 which requires that the disclosure notification be made "no later than forty-five (45) days from the discovery or notification of the breach." Defendant failed to meet this requirement by well over 300 days.

13. In the context of notice of data breach letters of this type, Defendant's use of the phrase "potentially involved information" is misleading lawyer language. Companies only send notice letters because data breach notification laws require them to do so. And such letters are only sent to those persons who Defendant itself has a reasonable belief that such personal information was accessed or acquired by an unauthorized individual or entity. Defendant cannot hide behind legalese – by sending a notice of data breach letter to Plaintiffs and Class Members, it

[7] https://mm.nh.gov/files/uploads/doj/remote-docs/lee-university-20250325.pdf.

admits that Defendant itself has a reasonable belief that Plaintiffs' and Class Members' names, Social Security numbers, and other sensitive information was accessed or acquired by an unknown actor – aka cybercriminals.

14. Due to Defendant's data security failures which resulted in the Data Breach, cybercriminals were able to target Defendant's computer systems and exfiltrate Plaintiffs' and Class Members' highly sensitive PII. As a result of this Data Breach, Plaintiffs' and Class Members' Private Information remains in the hands of those cybercriminals.

15. Though Defendant has not revealed the vulnerabilities that Medusa exploited, such that Plaintiffs cannot allege those specific details with discovery, the known facts make clear that Defendant's cybersecurity posture was woefully inadequate.

16. For example, Defendant apparently did not realize that Medusa had infiltrated its systems until after the hacker group was able to exfiltrate a tremendous amount of data—nearly 388 GB of data. In other words, Medusa was able to look for a way in to Defendant's information system; exploit that vulnerability and gain access to Defendant's information system; perform the necessary reconnaissance measures required for it to know where Defendant stored these valuable files; likely perform measures like installing additional malware that require administrative privileges (as these steps are standard for such hacker groups); and then download that data from Defendant's information systems all without being caught.

17. These measures are noisy and would have been identified as malicious activity if Defendant had implemented any serious systems designed to identify malicious activity—such as endpoint detection and response, extended detection and response, intrusion detection systems, anomaly detection systems, or centralized alerting systems.

18. If Defendant had taken even the minimal effort to employ some or all of these

systems necessary to detect malicious activity, then it would have at least noticed when the hacker group walked out the door with a massive amount of data—indeed, it is hard to imagine how anyone can miss such a spike in network activity.[8]

19. Defendant's misconduct, including failing to implement adequate and reasonable measures to protect Plaintiffs' and Class Members' Private Information, failing to timely detect the Data Breach, failing to take adequate steps to prevent and stop the Data Breach, failing to disclose the material facts that it did not have adequate security practices in place to safeguard the Private Information, and failing to provide timely and adequate notice of the Data Breach – caused substantial harm and injuries to Plaintiffs and Class Members across the United States.

20. Due to Defendant's negligence and failures, cyber criminals obtained and now possess everything they need to commit personal identity theft and wreak havoc on the financial and personal lives of thousands of individuals, for decades to come.

21. For example, now that their Private Information has been released onto the dark web, Plaintiffs are now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their health privacy, and similar forms of criminal mischief, and such risk may last for the rest of their lives. Consequently, Plaintiffs must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

22. Plaintiffs bring this class action lawsuit to hold Defendant responsible for its grossly negligent—indeed, reckless—failure to use statutorily required or reasonable industry

[8] To put into perspective the staggering amount of data Medusa stole from Defendant, 1 GB is equivalent to 1,000,000 KB. This Consolidated Complaint—61 pages long, containing 16,378 words—is approximately 115 KB of data in a Word Document format. Medusa looted 387,490,000 KB worth of data—***three million, three hundred sixty-nine thousand, four hundred seventy-eight times*** the amount of data contained in this Complaint.

cybersecurity measures to protect Class Members' Private Information.

23. Plaintiffs bring this action individually and on behalf of the Class and seeks actual damages and restitution. Plaintiffs also seek declaratory and injunctive relief, including significant improvements to Defendant's data security systems and protocols, future annual audits, Defendant-funded long-term credit monitoring services, and other remedies as the Court sees necessary and proper.

JURISDICTION AND VENUE

24. The Class Action Fairness Act (CAFA) confers diversity jurisdiction to a class action where (1) the "matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs," and (2) "*any* member of a class of Plaintiffs is a citizen of a State different from any defendant." 28 U.S.C. § 1332(d)(2) (emphasis added).

25. This Court has diversity jurisdiction over this action under CAFA, 28 U.S.C. § 1332(d), because this is a class action consisting of more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and at least one member of the Class is a citizen of a State that differs from any Defendant.

26. This Court has personal jurisdiction over the parties in this case. Defendant conducts business in this District and is a citizen of this District by virtue of having its principal place of business located in this District.

27. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

PARTIES

Plaintiffs

28. Plaintiff Harris is a citizen and resident of North Carolina. Plaintiff is a victim of the Data Breach.

29. Plaintiff Harris is former prospective student at Defendant and Defendant stored and handled his Private Information because of his dealings with Defendant.

30. Plaintiff Vaught is an adult individual and, at all relevant times herein, a resident and citizen of Kentucky, residing in Union, Kentucky. Plaintiff is a victim of the Data Breach.

31. Plaintiff Vaught is a former student at Defendant and Defendant stored and handled his Private Information because of his dealings with Defendant.

32. Plaintiff Campbell is an adult individual and, at all relevant times herein, a resident and citizen of West Park, Florida. Plaintiff is a victim of the Data Breach.

33. Plaintiff Campbell is a former student at Defendant and Defendant stored and handled her Private Information because of her dealings with Defendant.

34. Plaintiff Nabors is an adult individual and, at all relevant times herein, a resident and citizen of Chattanooga, Tennessee. Plaintiff is a victim of the Data Breach.

35. Plaintiff Nabors is a former student at Defendant and Defendant stored and handled his Private Information because of his dealings with Defendant.

36. Plaintiff Butler is an adult individual and, at all relevant times herein, a resident and citizen of Cleveland, Tennessee. Plaintiff is a victim of the Data Breach.

37. Plaintiff Butler is a former student at Defendant and Defendant stored and handled her Private Information because of her dealings with Defendant.

38. Plaintiff Kubba is an adult individual and, at all relevant times herein, a resident

and citizen of Cleveland, Tennessee. Plaintiff is a victim of the Data Breach.

39. Plaintiff Kubba is a student at Defendant and Defendant stored and handled her Private Information because of her dealings with Defendant.

40. Plaintiff Dennis Goodine is an adult individual and, at all relevant times herein, a resident and citizen of Calhoun, Tennessee. Plaintiff is a victim of the Data Breach.

41. Plaintiff Goodine is a former student at Defendant and Defendant stored and handled his Private Information because of his dealings with Defendant.

Defendant

42. Defendant is a Tennessee corporation with its principal place of business located at 1120 N Ocoee Street, Cleveland, Tennessee 37311.

43. Defendant can be served through its registered agent, Chris H. Conine, located at 1120 N Ocoee Street, Cleveland, Tennessee 37311.

FACTUAL BACKGROUND

A. Defendant and the Services it Provides.

44. Defendant, an undergraduate and graduate Christian university, "is one of the largest Christ-centered private institutions in Tennessee and in the Appalachian College Association." [9]

45. While administering its services, Defendant receives and handles PII, which includes, *inter alia*, current, former, and prospective students' full names, Social Security numbers, driver's license numbers, government-issued ID number (e.g. passport, state ID card), financial information (e.g. account number, credit or debit card number), and medical information.

46. Plaintiffs are required to entrust their highly sensitive PII to Defendant as a

[9] https://www.leeuniversity.edu/about/.

condition of enrollment or to receive information from Defendant. Each Plaintiff entrusted this information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

47. By obtaining, collecting, and storing Plaintiffs' PII, Defendant assumed legal and equitable duties and knew or should have known that Defendant was responsible for protecting Plaintiffs' PII from unauthorized disclosure.

48. And, upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and the Class Members. Upon information and belief, Defendant also uses Plaintiffs' PII to generate additional revenue and profits:

> **WHAT LEGAL BASES DO WE RELY ON TO PROCESS YOUR INFORMATION?**
>
> In Short: We only process your personal information when we believe it is necessary and we have a valid legal reason (i.e., legal basis) to do so under applicable law, like with your consent, to comply with laws, to provide you with services to enter into or fulfill our contractual obligations, to protect your rights, or to fulfill our legitimate business interests.[10]

B. Defendant Knew the Risks of Storing Valuable PII and the Foreseeable Harm to its Students.

49. At all relevant times, Defendant knew it was storing sensitive PII and that, as a result, its system would be an attractive target for cybercriminals.

50. Defendant's Privacy Notice makes clear that it understands that its students' Private Information is personal and must be protected by law.

51. Defendant's own published privacy policy states that, "We have implemented

[10] https://www.leeuniversity.edu/privacy-policy/.

appropriate and reasonable technical and organizational security measures designed to protect the security of any personal information we process," and "[w]e have contracts in place with our third parties, which are designed to help safeguard your personal information. This means that they cannot do anything with your personal information unless we have instructed them to do it. They will also not share your personal information with any organization apart from us. They also commit to protect the data they hold on our behalf and to retain it for the period we instruct."[11]

52. Defendant also knew that a breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised, as well as intrusion into their highly private health information.

53. Defendant agreed to and undertook legal duties to maintain the Private Information Plaintiffs and Class Members entrusted to it safely, confidentially, and in compliance with all applicable laws, including the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

54. Accordingly, Defendant had obligations created by industry standards, common law, statutory law, and its own assurances and representations to keep Plaintiffs' and Class Members' Private Information confidential and to protect such Private Information from unauthorized access.

55. Through its failure to properly secure Plaintiffs' and Class Members' Private Information, Defendant failed to meet its own promises of patient privacy.

56. Nevertheless, Defendant failed to spend sufficient resources on preventing external access, detecting outside infiltration, and training its employees to identify email-borne threats and defend against them.

57. The stolen Private Information at issue has great value to the hackers, due to the

[11] *Id.*

large number of individuals affected and the fact the sensitive information that was part of the data that was compromised.

C. The Data Breach

58. A data breach occurs when cyber criminals intend to access and steal Private Information that has not been adequately secured by a business entity like Defendant.

59. According to Defendant's Notice, Defendant discovered the cyberattack on March 22, 2024. At that time, Defendant retained experts who conducted a forensic investigation which confirmed that "some personal information of individuals" was contained "within a data set which was subject to a data security incident."[12]

60. However, despite apparently learning of the Data Breach on or about March 22, 2024, Defendant did not begin informing Plaintiffs, Class Members or other current and former students of the Data Breach until March 25, 2025—***over a year*** after the Data Breach.

61. Though Defendant has not admitted the cause of the Data Breach, it is clear from Defendant's egregiously delayed response that it lacks some of the most basic cybersecurity safeguards required by every regulation, statute, guideline, and industry standard—a reasonable and tested cybersecurity incident response plan, which is the most basic administrative safeguard companies are expected to implement.

62. Given Defendant's inept response wherein it took Defendant over a year to comply with its 45-day notice requirement, it is clear that Defendant lacks a reasonable cybersecurity incident response plan because those plans in major part are designed to guide companies to properly complying with their notice obligations in addition to restoring technical systems.

63. Given Defendant's failure on this most basic safeguard, it likely failed on the more

[12] https://mm.nh.gov/files/uploads/doj/remote-docs/lee-university-20250325.pdf.

complex technical safeguards as well.

64. According to Defendant, the Private Information accessed by cybercriminals involved a wide variety of PII, including full names, Social Security numbers, driver's license numbers, government-issued ID number (e.g. passport, state ID card), financial information (e.g. account number, credit or debit card number), and medical information.[13]

65. Upon information and belief, the unauthorized third-party cybercriminals that stole Plaintiffs' and Class Members' Private Information has engaged in (and will continue to engage in) misuse of the Private Information, including marketing and selling Plaintiffs' and Class Members' Private Information on the dark web.

66. Despite the breadth and sensitivity of the PII that was exposed, and the attendant consequences to patients as a result of the exposure, Defendant failed to disclose the Data Breach for 12 months. This inexplicable delay further exacerbated the harms to Plaintiffs and Class Members.

67. Presently, however, Defendant has provided no public information on the ransom demand or payment.

D. Defendant had an Obligation to Protect Private Information under the Law and the Applicable Standard of Care.

68. Defendant is prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799

[13] https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage.

F.3d 236 (3d Cir. 2015).

69. The FTC publishes guides for businesses for cybersecurity[14] and protection of PII[15] which includes basic security standards applicable to all types of businesses.

70. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or

[14] Fed. Trade Comm'n, *Start with Security: A Guide for Business*, (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[15] Fed. Trade Comm'n, *Protecting Private Information: A Guide for Business*, (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

71. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[16]

72. Defendant is further required by various states' laws and regulations to protect Plaintiffs' and Class Members' Private Information.

73. Defendant owed a duty to Plaintiffs and the Class to design, maintain, and test its computer and application systems to ensure that the Private Information in its possession was adequately secured and protected.

74. Defendant owed a duty to Plaintiffs and the Class to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees (and others who accessed Private Information within its computer systems) on how to adequately protect Private Information.

75. Defendant owed a duty to Plaintiffs and the Class to implement processes that would detect a breach on its systems in a timely manner.

76. Defendant owed a duty to Plaintiffs and the Class to act upon data security warnings

[16] Fed. Trade Comm'n, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

and alerts in a timely fashion.

77. Defendant owed a duty to Plaintiffs and the Class to disclose if its computer systems and data security practices were inadequate to safeguard individuals' Private Information from theft because such an inadequacy would be a material fact in the decision to entrust Private Information with Defendant.

78. Defendant owed a duty to Plaintiffs and the Class to disclose in a timely and accurate manner when data breaches occurred.

79. Defendant owed a duty of care to Plaintiffs and the Class because it was a foreseeable victim of a data breach.

E. Defendant was on Notice of Cyber Attack Threats and of the Inadequacy of their Data Security.

80. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some of the biggest cybersecurity breaches: Target,[17] Yahoo,[18] Marriott International,[19] Chipotle, Chili's, Arby's,[20] and others.[21]

---

[17] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

[18] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

[19] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/.

[20] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others.

[21] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

81. Defendant should certainly have been aware, and indeed was aware, that it was at risk for a data breach that could expose the Private Information that it collected and maintained.

82. Defendant was also on notice of the importance of data encryption of Private Information. Defendant knew it kept Private Information in its systems and yet it appears Defendant did not encrypt these systems or the information contained within them.

83. Defendant's notice letters list time-consuming, generic steps that victims of data security incidents can take, such as getting a copy of a credit report or notifying law enforcement about suspicious financial account activity. Also, Plaintiffs would have to affirmatively sign up for a call center number that victims may contact with questions. Defendant offered one year of credit monitoring for members of the class and Defendant offered no other substantive steps to help victims like Plaintiffs and Class Members to protect themselves. On information and belief, Defendant sent a similar generic letter to all other individuals affected by the Data Breach.

84. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

85. Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

86. Defendant had obligations created by the FTC Act, contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

87. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

88. It is well known that PII, including Social Security numbers in particular, is a

valuable commodity and a frequent, intentional target of cyber criminals. Companies that collect such information, including Defendant, are well-aware of the risk of being targeted by cybercriminals.

89. Individuals place a high value on the privacy of their PII. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

90. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, "[a] direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss."[22]

91. Individuals, like Plaintiffs and Class Members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and is likened to accessing one's DNA for hacker's purposes.

92. Data Breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiffs and Class Members cannot obtain new numbers unless they become a victim

[22] U.S. Dep't of Justice, *Victims of Identity Theft, 2018*, (April 2021), https://bjs.ojp.gov/content/pub/pdf/vit18.pdf.

of Social Security number misuse.

93. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So, using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[23]

94. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[24]

95. Additionally in 2021, there was a 15.1% increase in cyberattacks and data breaches from 2020. Over the next two years, in a poll of security executives, they have predicted an increase in attacks from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable cases will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[25]

96. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, and hopefully can ward off a cyberattack.

---

[23] U.S. Social Security Admin, *Identity Theft and Your Social Security Number*, Pub. No. 05-10064 (Oct. 2024), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[24] Bree Fowler, *Data Breaches Break Record in 2021*, CNET (Jan. 24, 2022), https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/.

[25] Chuck Brooks, *Alarming Cyber Statistics for Mid-Year 2022 That You Need to Know*, FORBES (June 3, 2022), https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864.

97. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data." [26] This publication also explains that "[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."[27]

98. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect Plaintiffs' and the proposed Class' PII from being compromised.

F. Plaintiffs' Experiences

Plaintiff Michael Harris

99. Plaintiff Harris is a former prospective student at Defendant, and Defendant stored and handled his Private Information as a result of his dealings with Defendant. Plaintiff is a victim of the Data Breach.

100. On or about March 25, 2024, Plaintiff Harris was notified of the Data Breach and of the impact to his PII via letter from Defendant.

101. Plaintiff Harris is careful to protect his Private Information. Plaintiff has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

102. Since the Data Breach, Plaintiff Harris has tried to mitigate the damage by changing

[26] Fed. Bureau of Investigations, *Common Frauds and Scams*, https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last visited Apr. 8, 2025).
[27] *Id.*

his passwords, contacting the credit bureaus as Defendant instructed, monitoring his financial accounts for hours, and freezing his credit. Having to do this every week not only wastes his time as a result of Defendant's negligence, but it also causes him great anxiety. Since the date of the breach Plaintiff has spent over twenty-four (24) hours taking action to mitigate the harm he has suffered.

103. Soon after the Data Breach, Plaintiff Harris began receiving an excessive number of spam calls on the same cell phone number provided to Defendant on his records. These calls are a distraction and waste time each day. Given the timing of the Data Breach, he believes that the calls are related to his stolen PII.

104. Plaintiff Harris is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

105. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized criminals. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

106. Plaintiff has experienced anxiety and increased concerns arising from the fact that his PII has been or will be misused and from the loss of his privacy.

107. The risk is not hypothetical. Here, a known hacking group intentionally stole the data, misused it, threatened to publish, or has published it on the Dark Web, and the sensitive information, including names and Social Security numbers, is the type that could be used to perpetrate identity theft or fraud.

108. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII —a form of intangible property that Plaintiff entrusted to Defendant,

which was compromised in and because of the Data Breach. Future identity theft monitoring is reasonable and necessary, and such services will include future costs and expenses.

109. Plaintiff has a continuing interest in ensuring that his PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

110. Had Plaintiff Harris been aware that Defendant's computer systems were not secure, he would not have entrusted Defendant with his PII and PHI.

111. As a result of Defendant's conduct, Plaintiff Harris suffered actual damages including, without limitation, time related to monitoring his financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of his personal information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time, efforts, and potentially expenses to review their credit reports, monitor their financial accounts, and monitor for fraud or identify theft – particularly since the compromised information includes Social Security numbers.

Plaintiff Christopher Vaught

112. Plaintiff Vaught is a former student at Defendant, and Defendant stored and handled his Private Information as a result of his dealings with Defendant. Plaintiff is a victim of the Data Breach.

113. On or about March 24, 2025, Plaintiff Vaught was notified of the Data Breach and of the impact to his PII via letter from Defendant.

114. Since the Data Breach, Plaintiff Vaught has tried to mitigate the damage by changing his passwords, contacting the credit bureaus as Defendant instructed, and monitoring his financial accounts.

115. Plaintiff Vaught is careful to protect his Private Information. Plaintiff has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

116. Soon after the Data Breach, Plaintiff Vaught began experiencing a significant amount of spam calls and text messages. These calls are a distraction and waste time each day. Given the timing of the Data Breach, he believes that the calls are related to his stolen PII.

117. Plaintiff Vaught is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

118. Plaintiff Vaught has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized criminals. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

119. Plaintiff Vaught has experienced anxiety and increased concerns arising from the fact that his PII has been or will be misused and from the loss of his privacy.

120. The risk is not hypothetical. Here, a known hacking group intentionally stole the data, misused it, threatened to publish, or has published it on the Dark Web, and the sensitive information, including names and Social Security numbers, is the type that could be used to perpetrate identity theft or fraud.

121. Plaintiff Vaught further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Future identity theft monitoring is reasonable and necessary, and such services will include future costs and expenses.

122. Plaintiff Vaught has a continuing interest in ensuring that his PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded

from future breaches.

123. Had Plaintiff Vaught been aware that Defendant's computer systems were not secure, he would not have entrusted Defendant with her PII.

124. As a result of Defendant's conduct, Plaintiff Vaught suffered actual damages including, without limitation, time related to monitoring her financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of her personal information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time, efforts, and potentially expenses to review their credit reports, monitor their financial accounts, and monitor for fraud or identify theft – particularly since the compromised information includes Social Security numbers.

Plaintiff Lucresia Campbell

125. Plaintiff Campbell is a former student at Defendant and Defendant stored and handled her Private Information as a result of her dealings with Defendant. Plaintiff is a victim of the Data Breach.

126. On or about March 24, 2025, Plaintiff Campbell was notified of the Data Breach and of the impact to her PII via letter from Defendant.

127. Plaintiff Campbell is careful to protect her Private Information. Plaintiff has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

128. Since the Data Breach, Plaintiff Campbell made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

129. Plaintiff Campbell is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

130. Plaintiff Campbell has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized criminals. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

131. Plaintiff Campbell has experienced anxiety and increased concerns arising from the fact that her PII has been or will be misused and from the loss of his privacy.

132. The risk is not hypothetical. Here, a known hacking group intentionally stole the data, misused it, threatened to publish, or has published it on the Dark Web, and the sensitive information, including names and Social Security numbers, is the type that could be used to perpetrate identity theft or fraud.

133. Plaintiff Campbell further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Future identity theft monitoring is reasonable and necessary, and such services will include future costs and expenses.

134. Plaintiff Campbell has a continuing interest in ensuring that her PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

135. Had Plaintiff Campbell been aware that Defendant's computer systems were not secure, she would not have entrusted Defendant with her PHI.

136. As a result of Defendant's conduct, Plaintiff Campell suffered actual damages including, without limitation, time related to monitoring his financial accounts for fraudulent

activity, facing an increased and imminent risk of fraud and identity theft, the lost value of his personal information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time, efforts, and potentially expenses to review their credit reports, monitor their financial accounts, and monitor for fraud or identify theft – particularly since the compromised information includes Social Security numbers.

Plaintiff Caleb Nabors

137. Plaintiff Nabors is a former student at Defendant and Defendant stored and handled his Private Information as a result of his dealings with Defendant. Plaintiff is a victim of the Data Breach.

138. On or about March, 2024, Plaintiff Nabors was notified of the Data Breach and of the impact to his PII via letter from Defendant.

139. Plaintiff is careful to protect his Private Information. Plaintiff has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

140. Since the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach and monitoring his financial accounts. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

141. Soon after the Data Breach, Plaintiff began receiving an excessive number of spam and scam phone calls. These calls are a distraction and waste time each day. Given the timing of the Data Breach, Plaintiff believes that the calls are related to his stolen PII.

142. Plaintiff is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

143. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized criminals. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

144. Plaintiff has experienced anxiety and increased concerns arising from the fact that his PII has been or will be misused and from the loss of her privacy.

145. The risk is not hypothetical. Here, a known hacking group intentionally stole the data, misused it, threatened to publish, or has published it on the Dark Web, and the sensitive information, including names and Social Security numbers, is the type that could be used to perpetrate identity theft or fraud.

146. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Future identity theft monitoring is reasonable and necessary, and such services will include future costs and expenses.

147. Plaintiff has a continuing interest in ensuring that his PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

148. Had Plaintiff been aware that Defendant's computer systems were not secure, he would not have entrusted Defendant with his PII.

149. As a result of Defendant's conduct, Plaintiff suffered actual damages including, without limitation, time related to monitoring her financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of his personal information, and other economic and non-economic harm. Plaintiff and Class Members will now

be forced to expend additional time, efforts, and potentially expenses to review their credit reports, monitor their financial accounts, and monitor for fraud or identify theft – particularly since the compromised information includes Social Security numbers.

Plaintiff Katelyn Butler

150. Plaintiff Butler is a former student at Defendant and Defendant stored and handled her Private Information as a result of her dealings with Defendant. Plaintiff is a victim of the Data Breach.

151. On or about March 24, 2025, Plaintiff was notified of the Data Breach and of the impact to her PII via letter from Defendant.

152. Plaintiff Butler is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. Plaintiff has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

153. Since the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach. Plaintiff has spent significant hours dealing with the Data Breach–valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

154. Plaintiff is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

155. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized criminals. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

156. After the Data Breach, Plaintiff has experienced a significant amount of spam calls and text messages. These calls are a distraction and waste time each day. Given the timing of the Data Breach, he believes that the calls are related to his stolen PII.

157. Plaintiff has experienced anxiety and increased concerns arising from the fact that her PII has been or will be misused and from the loss of his privacy.

158. The risk is not hypothetical. Here, a known hacking group intentionally stole the data, misused it, threatened to publish, or has published it on the Dark Web, and the sensitive information, including names and Social Security numbers, is the type that could be used to perpetrate identity theft or fraud.

159. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Future identity theft monitoring is reasonable and necessary, and such services will include future costs and expenses.

160. Plaintiff has a continuing interest in ensuring that her PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

161. Had Plaintiff been aware that Defendant's computer systems were not secure, she would not have entrusted Defendant with her PII.

162. As a result of Defendant's conduct, Plaintiff suffered actual damages including, without limitation, time related to monitoring her financial accounts for fraudulent activity for several hours, facing an increased and imminent risk of fraud and identity theft, the lost value of her personal information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time, efforts, and potentially expenses to review

their credit reports, monitor their financial accounts, and monitor for fraud or identify theft – particularly since the compromised information includes Social Security numbers.

Plaintiff Brittany Kubba

163. Plaintiff Kubba is a former student and work-study employee of Defendant, and Defendant stored and handled her Private Information as a result of her dealings with Defendant. Plaintiff is a victim of the Data Breach.

164. On or about March 24, 2025, Plaintiff was notified of the Data Breach and of the impact to her PII via letter from Defendant.

165. Plaintiff is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. Plaintiff has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

166. Since the Data Breach, Plaintiff made reasonable efforts to mitigate the effect of the Data Breach, including, but not limited to, researching the Data Breach, reviewing financial statements, and monitoring her credit information for hours each week—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

167. Plaintiff is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

168. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized criminals. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

169. Plaintiff has suffered actual damages from fraudulent charges to her Venmo

account and her Deposit account with Varo Bank. Plaintiff suffered lost time reversing the charges, replacing her credit and debit cards, and the necessary continued monitoring of her financial accounts.

170. After the Data Breach, Plaintiff has experienced a significant amount of spam calls and text messages. These calls are a distraction and waste time each day. Given the timing of the Data Breach, he believes that the calls are related to his stolen PII.

171. Plaintiff has experienced anxiety and increased concerns arising from the fact that her PII has been or will be misused, from the loss of her privacy, and the potential impacts on future recreational activities.

172. The risk is not hypothetical. Here, a known hacking group intentionally stole the data, misused it, threatened to publish, or has published it on the Dark Web, and the sensitive information, including names and Social Security numbers, is the type that could be used to perpetrate identity theft or fraud.

173. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Future identity theft monitoring is reasonable and necessary, and such services will include future costs and expenses.

174. Plaintiff has a continuing interest in ensuring that her PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

175. Had Plaintiff been aware that Defendant's computer systems were not secure, she would not have entrusted Defendant with her PII and PHI.

176. As a result of Defendant's conduct, Plaintiff suffered actual damages including,

without limitation, time related to monitoring her financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of her personal information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time, efforts, and potentially expenses to review their credit reports, monitor their financial accounts, and monitor for fraud or identify theft – particularly since the compromised information includes Social Security numbers.

Plaintiff Dennis Goodine

177. As a condition of obtaining services from Defendant, Plaintiff Goodine provided his PII to Defendant, and Defendant stored and handled his Private Information as a result of his dealings with Defendant. Plaintiff is a victim of the Data Breach.

178. On or about March 24, 2025, Plaintiff was notified of the Data Breach and of the impact to his PII via letter from Defendant.

179. Since the Data Breach, Plaintiff has tried to mitigate the damage, which included and continues to include: time spent verifying the legitimacy and impact of the Data Breach; time spent exploring credit monitoring and identity theft insurance options; time spent self-monitoring accounts with heightened scrutiny, time spent speaking with his bank and canceling credit cards, and time spent seeking legal counsel regarding their options for remedying and/or mitigating the effects of the Data Breach.

180. Plaintiff is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

181. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized criminals. Plaintiff suffered lost time, annoyance, interference, and inconvenience

because of the Data Breach.

182. Plaintiff has experienced anxiety and increased concerns arising from the fact that his PII has been or will be misused and from the loss of his privacy.

183. The risk is not hypothetical. Here, a known hacking group intentionally stole the data, misused it, threatened to publish, or has published it on the Dark Web, and the sensitive information, including names and Social Security numbers, is the type that could be used to perpetrate identity theft or fraud.

184. Indeed, after the Data Breach, Plaintiff has already suffered fraud and identity theft in the form of unauthorized charges on his credit cards and he was forced to cancel them and request new cards.

185. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Future identity theft monitoring is reasonable and necessary, and such services will include future costs and expenses.

186. Plaintiff has a continuing interest in ensuring that his PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

187. Had Plaintiff been aware that Defendant's computer systems were not secure, he would not have entrusted Defendant with his PII.

188. As a result of Defendant's conduct, Plaintiff suffered actual damages including, without limitation, time related to monitoring her financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of his personal information, and other economic and non-economic harm. Plaintiff and Class Members will now

be forced to expend additional time, efforts, and potentially expenses to review their credit reports, monitor their financial accounts, and monitor for fraud or identify theft – particularly since the compromised information includes Social Security numbers.

G. Cyber Criminals Will Use Plaintiffs' and Class Members' Private Information to Defraud Them.

189. Plaintiffs' and Class Members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and the Class Members and to profit off their misfortune.

190. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[28] For example, with the Private Information stolen in the Data Breach, identity thieves can open financial accounts, apply for credit, collect government benefits, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[29] These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class Members.

191. Private Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.[30]

---

[28] Insurance Info. Inst., *Facts + Statistics: Identity Theft and Cybercrime*, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[29] John Egan, *What Should I Do If My Driver's License Number is Stolen* (June 13, 2024), https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/.

[30] U.S. Gov't Accountability Office, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, (July 5, 2007), https://www.gao.gov/products/gao-07-737.

192. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number and name.

193. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[31]

194. This was a financially motivated Data Breach, as apparent from the discovery of the cyber criminals seeking to profit off the sale of Plaintiffs' and the Class Members' Private Information on the dark web. The Private Information exposed in this Data Breach are valuable to identity thieves for use in the kinds of criminal activity described herein.

195. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to personally identifiable information, they will use it.[32]

196. Hackers may not use the accessed information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[33]

---

[31] Tim Greene, *Anthem Hack: Private Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x- price-of-stolen-credit-card-numbers.html.

[32] Ari Lazarus, *How fast will identity thieves use stolen info?*, (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[33] U.S. Gov't Accountability Office, *Data Breaches Are Frequent, but Evidence of Resulting*

197. As described above, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[34]

198. With this Data Breach, identity thieves have already started to prey on the victims, and one can reasonably anticipate this will continue.

199. Data Breach victims, like Plaintiffs and other Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their credit because of the Data Breach.[35]

200. In fact, as a direct and proximate result of the Data Breach, Plaintiffs and the Class have suffered, and have been placed at an imminent, immediate, and continuing increased risk of suffering, harm from fraud and identity theft. Plaintiffs and the Class must now take the time and effort and spend the money to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

201. Plaintiffs and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Trespass, damage to, and theft of their personal property including Private

Identity Theft Is Limited; However, the Full Extent Is Unknown, (July 5, 2007), https://www.gao.gov/products/gao-07-737.

[34] Fed. Trade Comm'n, *Guide for Assisting Identity Theft Victims*, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

[35] *Id.*

Information;

b. Improper disclosure of their Private Information;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals and having been already misused;

d. The imminent and certainly impending risk of having their Private Information used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the data breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

h. Ascertainable losses in the form of deprivation of the value of patients' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Private Information; and

k. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

202. Moreover, Plaintiffs and Class Members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standards and statutorily compliant security measures and safeguards. Defendant has shown itself to be incapable of protecting Plaintiffs' and Class

Members' Private Information.

203. Plaintiffs and Class Members are desperately trying to mitigate the damage that Defendant has caused them but, given the Private Information Defendant made accessible to hackers, they are certain to incur additional damages. Because identity thieves have their Private Information,

204. Plaintiffs and all Class Members will need to have identity theft monitoring protection for the rest of their lives.

205. None of this should have happened. The Data Breach was preventable.

H. Defendant Could Have Prevented the Data Breach but Failed to Adequately Protect Plaintiffs' and Class Members' Private Information.

206. It is important to note that that data breaches are preventable.[36] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[37] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[38]

207. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs."[39]

208. The FTC has promulgated numerous guides for businesses which highlight the

[36] Lucy L. Thompson, *Despite the Alarming Trends, Data Breaches Are Preventable*, in DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[37] *Id.* at 17.
[38] *Id.* at 28.
[39] *Id.*

importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

209. In 2016, the FTC updated its publication, Protecting Private Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer 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. 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.[40]

210. The FTC further recommends that companies not maintain Private Information 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.

211. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take

[40] Fed. Trade Comm'n, *Protecting Private Information: A Guide for Business*, (Oct. 2016). https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

to meet their data security obligations.

212. These FTC enforcement actions include actions against entities that store Private Information, like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

213. Defendant failed to properly implement basic data security practices, including those set forth by the FTC.

214. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

215. Defendant also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

216. Defendant was entrusted with properly holding, safeguarding, and protecting against unlawful disclosure of Plaintiffs' and Class Members' Private Information.

217. Many failures laid the groundwork for the success ("success" from a cybercriminal's viewpoint) of the Data Breach, starting with Defendant's failure to incur the costs necessary to implement adequate and reasonable cyber security procedures and protocols necessary to protect Plaintiffs' and Class Members' Private Information.

218. Defendant was at all times fully aware of its obligation to protect the Private Information of Plaintiffs and Class Members. Defendant was also aware of the significant repercussions that would result from its failure to do so.

219. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained and/or exchanged, unencrypted, in Defendant's systems and were maintained in a condition vulnerable to cyberattacks.

220. Defendant knew, or reasonably should have known, of the importance of safeguarding Private Information and of the foreseeable consequences that would occur if Plaintiffs' and Class Members' Private Information was stolen, including the significant costs that would be placed on Plaintiffs and Class Members as a result of a breach.

221. The mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take necessary steps to secure Plaintiffs' and Class Members' Private Information from those risks left that information in a dangerous condition.

222. Defendant disregarded the rights of Plaintiffs and Class Members by, inter alia, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its systems were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiffs' and Class Members' Private Information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

I. Plaintiffs' And Class Members' Common Injuries

223. To date, Defendant has done absolutely nothing to compensate Plaintiffs and Class

Members for the damages they sustained in the Data Breach.

224. Defendant offered only one year of credit monitoring services to Class Members.

225. Defendant fails to offer any compensation to victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and it entirely fails to provide any compensation for its unauthorized release and disclosure of Plaintiffs' and Class Members' Private Information, out of pocket costs, and the time they are required to spend attempting to mitigate their injuries.

226. Furthermore, Defendant's failure to safeguard Plaintiffs' and Class Members' Private Information, places the burden squarely on Plaintiffs and the Class, rather than on the Defendant, to investigate and protect themselves from Defendant's tortious acts and omissions resulting in the Data Breach. Defendant merely sent instructions to Plaintiffs and Class Members about actions they can affirmatively take to protect themselves.

227. Plaintiffs and Class Members have been damaged by the compromise and exfiltration, by cyber-criminals, of their Private Information as a result of the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

228. Plaintiffs and Class Members were damaged in that their Private Information is now in the hands of cyber criminals being sold and potentially for sale for years into the future.

229. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an actual, imminent, and substantial risk of harm from fraud and identity theft, especially in light of the actual fraudulent misuse of the Private Information that has already taken place, as alleged herein.

230. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach.

231. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

232. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members.

233. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

234. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

235. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Monitoring their medical records for fraudulent charges and data;

e. Addressing their inability to withdraw funds linked to compromised accounts;

f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g. Placing "freezes" and "alerts" with credit reporting agencies;

h. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

i. Contacting financial institutions and closing or modifying financial accounts;

j. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

k. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

l. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

236. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in Defendant's possession, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information as well as health information is not accessible online and that access to such data is password-protected.

237. Further, because of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

238. Defendant's delay in identifying and reporting the Data Breach caused additional

harm. In a data breach, time is of the essence to reduce the imminent misuse of PII. Early notification helps a victim of a Data Breach mitigate their injuries, and in the converse, delayed notification causes more harm and increases the risk of identity theft. Here, Defendant knew of the breach since March 22, 2024, and did not notify the victims until March 25, 2025. Yet Defendant offered no explanation of purpose for the delay. This delay violates Tennessee's statutory notification requirements and increased the injuries to Plaintiffs and the Class.

CLASS ACTION ALLEGATIONS

239. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

240. Plaintiffs bring all counts, as set forth below, individually and as a Class action, pursuant to the provisions of the Fed. R. Civ. P. 23, on behalf of a Class defined as:

> All persons whose Private Information was compromised because of the Data Breach that is the subject of the Notice of Data Breach published by Defendant on or about March 25, 2025 (the "Class" or "Class Members").

241. This proposed Class definition is based on the information available to Plaintiffs at this time. Plaintiffs may modify the Class definition in an amended pleading or when they move for Class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

242. Excluded from the Class are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

243. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

244. N**umerosity** – Fed. R. Civ. P. 23(a)(1): Plaintiffs are informed and believe, and thereon allege, that there are at minimum, approximately 136,928 members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendant's records, including but not limited to the files implicated in the Data Breach.

245. **Commonality** – Fed. R. Civ. P. 23(a)(2): This action involves questions of law and fact common to the Class. Such common questions include, but are not limited to:

a. Whether Defendant had a duty to protect Plaintiffs' and Class Members' PII;

b. Whether Defendant was negligent in collecting and storing Plaintiffs' and Class Members' PII, and breached its duties thereby;

c. Whether Defendant was unjustly enriched;

d. Whether Defendant entered a contract implied in fact with Plaintiffs and the Class;

e. Whether Defendant breached that contract by failing to adequately safeguard Plaintiffs' and Class Members' PII;

f. Whether Defendant violated its own Privacy Practices;

g. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiffs and members of the Class and the general public;

h. Whether Plaintiffs and Class Members are entitled to damages as a result of Defendant's wrongful conduct; and

i. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

246. **Typicality** – Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of the claims of the members of the Class. Plaintiffs' and Class Members' claims are based on the same legal

theories and arise from the same unlawful and willful conduct. Plaintiffs and members of the Class all had information stored in Defendant's system, each having their PII exposed and/or accessed by an unauthorized third party.

247. **Adequacy of Representation** – Fed. R. Civ. P. 23(a)(3): Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other Class Members Plaintiffs seek to represent; Plaintiffs have retained counsel competent and experienced in complex Class action litigation; Plaintiffs intend to prosecute this action vigorously; and Plaintiffs' counsel have adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiffs and Plaintiffs' counsel.

248. **Injunctive Relief**, Fed. R. Civ. P. 23(b)(2): Defendant has acted and/or refused to act on grounds that apply generally to the Class therefore making injunctive and/or declarative relief appropriate with respect to the Class under 23(b)(2).

249. **Superiority**, Fed. R. Civ. P. 23(b)(3): A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and

protects the rights of each Class member.

250. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

251. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely and adequately notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard students' PII; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

252. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

COUNT ONE
NEGLIGENCE
(On Behalf of Plaintiffs and Class Members)

253. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

254. Defendant required Plaintiffs and Class Members to submit non-public personal information as a condition of enrollment/to obtain enrollment information from Defendant.

255. By collecting and storing this data in Defendant's computer network and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer network—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period and to give prompt notice to those affected in the case of a Data Breach.

256. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

257. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its students, which is recognized by laws and regulations including but not limited to the FTC Act, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

258. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

259. Defendant's duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

260. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failure to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

261. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data

breaches.

262. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

263. Moreover, though Defendant has not publicly identified the vulnerability or vulnerabilities that were exploited, its complete failure to identify the malicious activity notwithstanding that the hackers walked out the door with a massive 387.48 GB of data shows that Defendant failed to get even the foundational protections right—implementing tools designed to at least identify malicious activity. Defendant's failure to do even the basics constitutes gross negligence.

COUNT TWO
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and Class Members)

264. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

265. Plaintiffs and the Class bring this claim in the alternative to their breach of implied contract claim, below.

266. Plaintiffs and Class Members conferred a benefit on Defendant in the form of profits to render certain services, a portion of which was intended to have been used by Defendant for data security measures to secure Plaintiffs' and Class Members' PII.

267. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant chose to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct

and proximate result of Defendant's failure to provide adequate security.

268. Under the principles of equity and good conscience, Defendant should not be permitted to retain the full value of its profits resulting from its collection and storage of the Plaintiffs' and Class Members' PII, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

269. If Plaintiffs and Class Members knew that Defendant had not secured their PII, they would not have agreed to disclose their data to Defendant.

270. Defendant, by way of its affirmative actions and omissions, including its knowing violations of its express or implied contracts with the entities that collected Plaintiffs' and the Class Members' Private Information, knowingly and deliberately enriched itself by saving the costs it reasonably and contractually should have expended on reasonable data privacy and security measures to secure Plaintiffs' and Class Members' Private Information.

271. Instead of providing a reasonable level of security, training, and protocols that would have prevented the Data Breach, as described above and as is common industry practice among companies entrusted with similar Private Information, Defendant, upon information and belief, instead consciously and opportunistically calculated to increase its own profits at the expense of Plaintiffs and Class Members.

272. Defendant failed to implement—or adequately implement—data security practices, procedures, and programs to secure sensitive Private Information, including without limitation those industry standard data security practices, procedures, and programs discussed herein.

273. Defendant, upon information and belief, has therefore engaged in opportunistic and unethical conduct by profiting from conduct that it knew would create a significant and highly likely risk of substantial and certainly impending harm to Plaintiffs and the Class in direct violation

of Plaintiffs' and Class Members' interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its wrongful conduct.

274. Plaintiffs have no adequate remedy at law.

275. Accordingly, Plaintiffs and the Class are entitled to relief in the form of restitution and disgorgement of all ill-gotten gains, which should be put into a common fund to be distributed to Plaintiffs and the Class.

COUNT THREE
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and Class Members)

276. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

277. Plaintiffs and Class Members were required to provide Defendant with their Private Information as a condition of enrollment/to receive enrollment information from Defendant.

278. When Plaintiffs and Class Members provided their Private Information to Defendant when seeking educational services, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties to protect their Private Information and to timely notify them in the event of a Data Breach.

279. Based on Defendant's representations, legal obligations, and acceptance of Plaintiffs' and the Class Members' Private Information, Defendant had an implied duty to safeguard their Private Information through the use of reasonable industry standards. This implied duty was reinforced by Defendant's representations in its Privacy Policy.

280. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' Private Information and failing to provide them with timely and accurate notice

of the Data Breach. Indeed, it took Defendant months to warn Plaintiffs and Class member of their imminent risk of identity theft. Defendant also failed to notify Plaintiffs and the Class Members whether or not their driver's license numbers were compromised, leaving Plaintiffs and Class Members unsure as to the extent of the information that was compromised.

281. As a direct and proximate result of Defendant's breach of implied contract, Plaintiffs and Class Members have suffered damages, including foreseeable consequential damages that Defendant knew about when it requested Plaintiffs' and the Class Members' Private Information.

COUNT FOUR
INVASION OF PRIVACY
(On Behalf of Plaintiffs and Class Members)

282. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

283. Plaintiffs and Class Members took reasonable and appropriate steps to keep their Private Information confidential from the public.

284. Plaintiffs' and Class Members' efforts to safeguard their own Private Information were successful, as their Private Information was not known to the public prior to the Data Breach.

285. Plaintiffs and Class Members had a legitimate expectation of privacy to their Private Information and were entitled to the protection of this information against disclosure to unauthorized third parties.

286. Defendant owed a duty to its students, including Plaintiffs and the proposed Class Members, to keep their Private Information confidential.

287. The unauthorized release of Private Information is highly offensive to any reasonable person.

288. Plaintiffs' and Class Members' Private Information is not of legitimate concern to the public.

289. Defendant knew or should have known that Plaintiffs' and Class Members' Private Information was private.

290. By intentionally failing to keep Plaintiffs' and Class Members' PII safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiffs' and Class Members' privacy by:

a. Intentionally and substantially intruding into Plaintiffs' and Class Members' private affairs in a manner that identifies Plaintiffs and Class Members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiffs and Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiffs and Class Members.

291. As the Restatement explains, as used throughout the Restatement of Torts, intent "has reference to the consequences of an act rather than the act itself." Restatement (Second) of Torts § 8A, cmt. A (1964). "Intent is not, however, limited to consequences which are desired. If the actor knows that the consequences are certain, or substantially certain, to result from his act, and still goes ahead, he is treated by the law as if he had in fact desired to produce the result." *Id.* cmt. B.

292. Indeed, given the foreseeability of the harms inherent in data breaches and the ubiquitous nature of data breaches, Defendant was substantially certain that its failure to implement reasonable cybersecurity standards would lead to an invasion of Plaintiffs' privacy.

293. Defendant knew that an ordinary person in Plaintiffs' or Class Members' position would consider the exposure of their PII to be highly offensive and objectionable.

294. Defendant invaded Plaintiffs' and Class Members' right to privacy and intruded into Plaintiffs' and Class Members' private affairs by intentionally misusing and/or disclosing their PII without their informed, voluntary, affirmative, and clear consent.

295. Moreover, given that stolen PII is then publicized and traded on the dark web and through Telegram channels, Defendant knew or was substantially certain that its failure to implement reasonable cybersecurity safeguards would lead to the publication of Plaintiffs' and the Class Members' PII to a large group of the public and/or to a large group of individuals who are in a special relationship with Plaintiffs and the proposed Class Members, in that those individuals are exactly the type of people that Plaintiffs and the Class Members have a special interest in ensuring their PII is kept confidential from given that those individuals are known identity thieves and fraudsters.

296. The conduct described above was at or directed at Plaintiffs and the Class Members.

297. As a proximate result of such intentional misuse and disclosures, Plaintiffs and Class Members' reasonable expectations of privacy in their PII was unduly frustrated and thwarted. Defendant's conduct amounted to a substantial and serious invasion of Plaintiffs' and Class Members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

298. In failing to protect Plaintiffs' and Class Members' PII, and in intentionally misusing and/or disclosing their PII, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiffs' and Class Members' rights to have such information kept

confidential and private. Plaintiffs, therefore, seek an award of damages on behalf of themselves and the Class.

299. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that Defendant's inadequate data security measures will likely result in additional data breaches. Plaintiffs and Class Members have no adequate remedy at law for the injuries that they will sustain in that a judgment for monetary damages will not prevent further invasions of the Plaintiffs' and Class Members' privacy by Defendant.

COUNT FIVE
DECLARATORY/INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and Class Members)

300. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

301. As previously alleged, Plaintiffs and Class Members entered into an implied contract that required Defendant to provide adequate security for the Private Information it collected from Plaintiffs and the Class.

302. Defendant owes a duty of care to Plaintiffs and Class Members that requires it to adequately secure Private Information.

303. Defendant still possess Private Information regarding Plaintiffs and Class Members.

304. Since the Data Breach, Defendant has announced few if any changes to their data security infrastructure, processes or procedures to fix the vulnerabilities in their computer systems and/or security practices which permitted the Data Breach to occur and go undetected for months and, thereby, prevent further attacks.

305. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and the Class. In fact, now that Defendant's insufficient data security is known to hackers, the Private Information in Defendant's possession is even more vulnerable to cyberattack.

306. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and the members of the Class are at risk of additional or further harm due to the exposure of their Private Information and Defendant's failure to address the security failings that lead to such exposure.

307. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the breach to meet Defendant's contractual obligations and legal duties.

308. Plaintiffs, therefore, seeks a declaration that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security and that to comply with its contractual obligations and duties of care, Defendant must implement and maintain additional security measures.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class requested herein;

b. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including actual damages, restitution, attorney fees, expenses, costs, and such other and further relief as is just and proper.

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class and the general public as requested herein, including, but not limited to:

i. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

ii. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

iii. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

iv. Ordering that Defendant segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

v. Ordering that Defendant cease transmitting Private Information via unencrypted email;

vi. Ordering that Defendant cease storing Private Information in email accounts;

vii. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of

services;

viii. Ordering that Defendant conduct regular database scanning and securing checks;

ix. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

x. Ordering Defendant to meaningfully educate its current, former, and prospective employees and subcontractors about the threats faced as a result of the loss of financial and personal information to third parties, as well as the steps they must take to protect against such occurrences;

d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues so triable.

Dated: August 25, 2025

Respectfully submitted,

/s/ J. Gerard Stranch, IV

J. Gerard Stranch, IV (BPR 23045)
Grayson Wells (BPR 039658)
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203

Tel: (615) 254-8801
gstranch@stranchlaw.com
gwells@stranchlaw.com

Andrew J. Shamis
SHAMIS & GENTILE, PA
14 NE 1st Avenue, Suite 1205
Miami, FL 33132
Tel: (305) 479-2299
ashamis@shamisgentile.com

Interim Class Counsel

CERTIFICATE OF SERVICE

I hereby certify that on this 25th day of August 2025, the foregoing Consolidated Class Action Complaint was electronically filed with the Court, and will be served by operation of the Court's CM/ECF filing system upon all counsel record.

/s/ J. Gerard Stranch, IV
J. Gerard Stranch, IV