UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT

JOSEPH VERRIERE, on behalf of himself and all others similarly situated, *Plaintiff*, v. CIERANT CORPORATION, and BLUE CROSS BLUE SHIELD OF MASSACHUSETTS, *Defendants*.	No. **COMPLAINT – Class Action** JURY TRIAL DEMANDED

Plaintiff, Joseph Verriere ("Plaintiff"), on behalf of himself and on behalf of all others similarly situated, alleges the following against Cierant Corporation ("Cierant") and Blue Cross Blue Shield of Massachusetts ("BCBS MA") (collectively, "Defendants") upon personal knowledge as to his own acts, and based upon his investigation, his counsel's investigation, and information and belief as to all other matters.

INTRODUCTION

1. This class action arises out of the recent data security incident and data breach that was perpetrated against Defendants (the "Data Breach"), which held in their possession certain personally identifiable information ("PII") and protected health information ("PHI") (collectively, the "Private Information") of Plaintiff and Class Members.

2. Defendant Cierant is a "distributed marketing software and services company"[1] that works with health insurance and publishing companies as well as stores.[2]

[1]https://www.cierant.com (last accessed Aug. 13, 2025).

[2]https://www.cierant.com/industries-served/ (last accessed Aug. 13, 2025).

3. Defendant BCBS MA is a health insurance plan headquartered in Boston, Massachusetts.[3]

4. Defendants owe Plaintiff and Class Members an affirmative duty to adequately protect and safeguard this private information against theft and misuse. Despite such duties created by statute, regulation, and common law, at all relevant times, Defendants utilized deficient data security practices, thereby allowing sensitive and private data to fall into the hands of strangers.

5. On December 10, 2024, Defendant Cierant became aware of suspicious activity on its CleoVLTrader file transfer system.[4]

6. Defendant Cierant then "determined that an unauthorized actor exploited the third-party vulnerability to gain limited access to Cierant systems that may have compromised personal or health data."[5]

7. Defendant Cierant disclosed that it processed the compromised personal data "on behalf of third-party health plans."[6] Defendant has not disclosed which health plans were affected by the Data Breach.

8. Through the Data Breach, the cybercriminal gained unauthorized access to highly sensitive Private Information, including "name, address, date of birth, treatment-related dates, a generic description of services received, provider name, medical record number, health plan

[3]Our Company at a Glance, BLUE CROSS BLUE SHIELD OF MASSACHUSETTS, https://www.bluecrossma.org/sites/g/files/csphws1866/files/acquiadam-assets/2024-Fact%20Sheet.pdf (last accessed Aug. 13, 2025).

[4]Data Incident, CIERANT CORPORATION, https://www.cierant.com/notice-of-data-incident/ (last accessed Aug. 13, 2025).

[5]*Id.*

[6]*Id.*

beneficiary number, claims number, and/or plan member account number, premium information."[7]

9. Defendant Cierant began notifying affected individuals such as Plaintiff on or around July 3, 2025.[8]

10. But for Defendants' failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect PII and PHI, the Data Breach would not have occurred.

11. Defendants are well-aware that they are at high risk of attempted cyberattack due to the high value of the sensitive data.

12. Despite Defendants' awareness of both the value and sensitivity of the data they safeguarded and serious risk presented by insufficient security practices, Defendants did not take sufficient steps to ensure that their systems were secure. Defendants knew or should have known about the risk to the data they stored and processed, and the critical importance of adequate security measures in the face of increasing threats.

13. The Data Breach was directly and proximately caused by Defendants' failure to implement reasonable and industry-standard data security practices necessary to protect their systems from a foreseeable and preventable cyberattack. Through this wrongful conduct, the sensitive PII and PHI of Plaintiff and Class Members is now in the hands of cybercriminals, who target this sensitive data for its value to identity thieves. Plaintiff and Class Members are now at a significantly increased and impending risk of fraud, identity theft, and similar forms of criminal mischief—risks which may last the rest of their lives. Consequently, Plaintiff and Class

[7] *Id.*

[8] *See* Exhibit A.

Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes. Moreover, Plaintiff and Class Members have lost the inherent value of their private data.

14. By aggregating information obtained from the Data Breach with other sources or other methods, criminals can assemble a full dossier of private information on an individual to facilitate a wide variety of frauds, thefts, and scams.

15. Defendants' failure to notify Plaintiff and Class Members that they had been impacted by this data breach for nearly seven months after Defendants became aware of the breach harmed Plaintiff and made it more difficult for Plaintiff to take swift action to respond to the breach.

16. Plaintiff and Class Members have been harmed because they are at immediate risk of having their personal information used against them. Indeed, they have been at risk well before Defendant Cierant even notified Plaintiff of the breach. Plaintiff does not know if his data has been sold, transferred, replicated, or irrevocably disseminated and exposed. He suffered harm in the loss of the value of his data which cannot be easily recovered, if ever.

17. Defendant Cierant has also not offered identity theft monitoring services to affected individuals as a result of the breach.[9] This creates uncertainty about the extent to which patients have been harmed and the need to engage in various services and efforts in the wake of the data breach, including but not limited to examining whether their PII or PHI has been sold on the dark web, taking measures to protect against identity theft crimes, expenses, and/or time spent on credit monitoring and identity theft insurance, time spent examining bank statements, time spent initiating fraud alerts, and other consequential harms.

[9] *See* Exhibit A.

18. Plaintiff, individually and on behalf of a nationwide class, alleges claims of (1) Negligence, (2) Negligence *Per Se*, (3) Breach of Implied Contract; and (4) Unjust Enrichment. Plaintiff also seeks declaratory and injunctive relief. Plaintiff asks the Court to compel Defendants to adopt reasonable information security practices to secure the sensitive PII and PHI that Defendants collect and store in their databases and to grant such other relief as the Court deems just and proper.

PARTIES

Plaintiff

19. Plaintiff is and at all times mentioned herein a resident and citizen of Glendale, Colorado.

Defendants

20. Defendant Cierant is Connecticut-based domestic public corporation with its headquarters and principal place of business at 34 Executive Drive, Danbury, Connecticut 06810.

21. Defendant BCBS MA is a major Massachusetts insurer, with its principal place of business located at 101 Huntington Avenue, Suite 1300, Boston Massachusetts 02199.

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Defendants. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

23. This Court has personal jurisdiction over Defendant Cierant through its business operations in this District, including the conduct giving rise to this Action. Defendant Cierant's principal place of business is in this District. Defendant Cierant intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

24. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Defendant Cierant is also based in this District, maintains Plaintiff's and Class Members' Private Information in this District, and has caused harm to Plaintiff and Class Members from or within this District.

FACTUAL ALLEGATIONS

I. Background

25. Defendant Cierant is a "distributed marketing software and services company"[10] founded in 1987.[11]

26. Defendant Cierant "found [itself] perfectly positioned to trailblaze new paths to cross-media marketing and campaign automation."[12] It represents itself as having "expertise in Web-based custom software development and programming [which] allowed [Cierant] to rapidly deploy new and exciting forms of engagement across media and windows never before available into consumer channel activity."[13]

[10] https://www.cierant.com (last accessed Aug. 13, 2025).

[11] *Shaking Things Up Since '87*, CIERANT CORPORATION, https://www.cierant.com/who-we-are/history/ (last accessed Aug. 13, 2025).

[12] *Id.*

[13] *Id.*

27. Defendant Cierant "supports health insurers with high-volume member communications"[14] such as Defendant BCBS MA.[15]

28. Upon information and belief, each of Cierant's clients, including BCBS MA, stores PII and PHI of their customers on Cierant's platform through the use of Cierant's offered services and software.

29. Defendant Cierant's Privacy Policy solely applies to information collected by its website, thus its data privacy protocols and practices involving subscriber data provided by insurers such as Defendant BCBS MA are unknown.[16]

30. Defendant Blue Cross Blue Shield Massachusetts's Privacy Policy claims that it "employs some of the strongest methods of encryption commercially available today. All online activity involving personal or sensitive information is encrypted from the point it leaves your computer until it enters our systems."[17]

31. Defendant BCBS MA also claims that PHI provided to it will be subjected to its "Commitment to Confidentiality."[18]

---

[14]Emily Hill, *Health Data of BCBS Massachusetts Members Exposed in Cierant Cyberattack*, THE NATIONAL CIO REV. (July 11, 2025), https://nationalcioreview.com/articles-insights/extra-bytes/health-data-of-bcbs-massachusetts-members-exposed-in-cierant-cyberattack/ (last accessed Aug. 13, 2025).

[15]*See* Exhibit A.

[16]*Privacy Policy*, *available at* https://www.cierant.com/privacy-policy/ (last accessed Aug. 13, 2025).

[17]*Allowing Access to Your Private Health Information,* BLUE CROSS BLUE SHIELD OF MASSACHUSETTS, https://www.bluecrossma.org/disclaimer/allowing-access-to-your-private-health-information (last accessed Aug. 13, 2025).

[18]*Well Connection Privacy Policy*, BLUE CROSS BLUE SHIELD OF MASSACHUSETTS, https://www.bluecrossma.org/disclaimer/privacy-and-security/well-connection-privacy-policy (last accessed Aug. 13, 2025).

32. Defendant BCBS MA demonstrates its "commit[ment] to maintaining your trust" and claims that it "use[s] reasonable measures to help protect information from loss, theft, misuse and unauthorized access, disclosure, alteration, and destruction."[19]

33. Defendant BCBS MA claims that subscribers' "information is stored in a secure server environment and is protected behind a firewall. The information that is transmitted back and forth is scrambled with the aid of encryption technology."[20]

34. Defendant BCBS MA also claims to "maintain reasonable and appropriate measures designed to maintain information we collect in a secure manner. We have taken certain physical, electronic, and administrative steps to safeguard and secure the information we collect from visitors to the Sites."[21]

35. Defendant BCBS MA also cautions its subscribers from sharing their data with unauthorized third parties because "the third party may choose how to use your information[,]"[22] "release of your private health information is final[,]"[23] and "Blue Cross cannot guarantee that third parties will abide by"[24] their written privacy policies but did not heed its own advice when providing its subscribers' data to Defendant Cierant.

36. Plaintiff and Class Members provided their Private Information to Defendants with the reasonable expectation and on the mutual understanding that Defendants would comply

[19] *Id.*

[20] *Privacy*, BLUE CROSS BLUE SHIELD OF MASSACHUSETTS, https://www.bluecrossma.org/disclaimer/privacy-and-security (last accessed Aug. 13, 2025).

[21] *Id.*

[22] *See supra* note 17.

[23] *Id.*

[24] *Id.*

with their obligations to keep such information confidential and secure from unauthorized access.

37. As a result of collecting and storing the Private Information of Plaintiff and Class Members for their own financial benefit, Defendants had a continuous duty to adopt and employ reasonable measures to protect Plaintiff's and Class Members' Private Information from disclosure to third parties.

II. The Data Breach

38. Defendant Cierant Corporation detected a vulnerability in the Cleo VL Trader managed file transfer solution on December 10, 2024.[25] After further investigation, Cierant learned that the "vulnerability had been exploited by a threat actor, resulting in unauthorized access to Cierant's systems."[26] Cierant's Data Breach Notice states that the Data Breach "may have compromised personal or health data. . . .processed by Cierant on behalf of third-party health plans."[27]

39. Defendant Cierant then "notified and then worked with these health plans to identify and notify potentially affected individuals."[28] Defendant Cierant has not publicly disclosed which health plans were impacted.

40. It is believed that the Cierant Data Breach might be linked to two vulnerabilities affecting Cleo products that were disclosed in December 2024: CVE-2024-50623, and CVE-

[25]Steve Alder, *Cierant Corporation Announced 232,500-Record Data Breach*, THE HIPAA JOURNAL (July 22, 2025), https://www.hipaajournal.com/cierant-corporation-data-breach/ (last accessed Aug. 13, 2025).

[26]*Id.*

[27]*Data Incident*, CIERANT CORPORATION, https://www.cierant.com/notice-of-data-incident/ (last accessed Aug. 13, 2025).

[28]*Id.*

2024-55956.[29] The first vulnerability allowed malicious files to be uploaded, and the second allowed Bash and PowerShell commands to be run on the host system.[30]

41. Through the Data Breach, the cybercriminal gained unauthorized access to highly sensitive Private Information, including "name, address, date of birth, treatment-related dates, a generic description of services received, provider name, medical record number, health plan beneficiary number, claims number, and/or plan member account number, premium information."[31]

42. Defendant Cierant reported to the United States Department of Health and Human Services Office of Civil Rights that 232,506 individuals were impacted by the Data Breach.[32]

43. The Data Breach Notices do not provide details about the root cause of the Data Breach, the vulnerabilities exploited, the criminals responsible for the breach, and the remedial measures undertaken to ensure such a breach does not occur again. To date, Defendants have not explained or disclosed these facts to Plaintiff and Class Members.

44. Without these details, Plaintiff's and Class Members' ability to mitigate harms resulting from the Data Breach is severely diminished.

45. Defendant Cierant's Data Breach notice offers no substantive steps to help victims like Plaintiff and Class Members to protect themselves other than providing credit monitoring and identity protection, which is woefully inadequate considering the lifelong

[29]Alder, *supra* note 25.

[30]*Id.*

[31]*Data Incident*, CIERANT CORPORATION, https://www.cierant.com/notice-of-data-incident/ (last accessed Aug. 13, 2025).

[32]*Cases Currently Under Investigation*, UNITED STATES DEP'T OF HEALTH AND HUMAN SVS. OFFICE FOR CIVIL RIGHTS, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Aug. 13, 2025).

increased risk of fraud and identity theft that Plaintiff and Class Members now face as a result of the Data Breach.

46. Defendant Cierant has offered affected individuals 12 months of credit monitoring services through Epiq.[33] These limitations are inadequate when the victims will likely face many years of identity theft.

47. Moreover, Defendant Cierant's credit monitoring offer and advice to Plaintiff and Class Members squarely place the burden on Plaintiff and Class Members, rather than on Defendants, to monitor and report suspicious activities to law enforcement. In other words, Defendants expect Plaintiff and Class Members to protect themselves from its tortious acts resulting from the Data Breach. Rather than automatically enrolling Plaintiff and Class Members in credit monitoring services upon discovery of the Data Breach, Defendant Cierant merely sent instructions to Plaintiff and Class Members about actions they could affirmatively take to protect themselves.

III. The Data Breach was Preventable

48. At all relevant times, Defendants knew, or should have known, that the PII and PHI they were entrusted with was a prime target for malicious actors. Defendants knew this given the unique type and the significant volume of data on their networks, servers, and systems, comprising individuals' detailed and confidential personal information and, thus, the significant number of individuals for whom the exposure of the unencrypted data would harm.

49. As custodians of Plaintiff's and Class Members' PII and PHI, Defendants knew or should have known the importance of protecting their PII and PHI, and of the foreseeable consequences and harms to such persons if any data breach occurred. Defendants' security

[33] *See* Exhibit A.

obligations were also especially important due to the substantial increase of cyberattacks and data breaches in recent years, particularly those targeting businesses and other organizations like Defendant, which store and maintain large volumes of PII and PHI.

50. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[34] The 330 reported breaches in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.

51. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's Private Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

52. On information and belief, Defendants failed to adequately train and supervise their IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing them to lose control over the PII and PHI in their possession. Defendants' negligence is evidenced by their failure to prevent the Data Breach and stop cybercriminals from accessing the Private Information.

IV. Defendants Failed to Comply with FTC Guidelines

53. At all times relevant to this Complaint, Defendants knew or should have known the significance and necessity of safeguarding the Private Information in their possession, and the foreseeable consequences of a data breach. Defendants knew or should have known that

[34] 2021 Data Breach Annual Report, ITRC, https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last accessed April 3, 2025).

because they collected and maintained the PII and PHI for a significant number of individuals, a significant number of individuals would be harmed by a breach of their systems. Defendants further knew that the data they were entrusted with was highly valuable and contained private and sensitive information including medical information.

54. Because PII is so sensitive and cyberattacks have become a rising threat, the FTC has issued numerous guides for businesses holding sensitive PII and emphasized the importance of adequate data security practices. The FTC also stresses that appropriately safeguarding PII held by businesses should be factored into all business-related decision making.

55. An FTC Publication titled "Protecting Personal Information: A Guide for Business" lays out fundamental data security principles and standard practices that businesses should implement to protect PII.[35] The guidelines highlight that businesses should (a) protect the personal customer information they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems.

56. The FTC also recommends businesses use an intrusion detection system, monitor all incoming traffic to the networks for unusual activity, monitor for large amounts of data being transmitted from their systems, and have a response plan prepared in the event of a breach.

57. The FTC also recommends that businesses limit access to sensitive PII, require complex passwords to be used on the networks, use industry-tested methods for security, monitor

[35] *See Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed June 30, 2025).

for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.

58. Businesses that do not comply with the basic protection of sensitive PII are facing enforcement actions brought by the FTC. Failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data is an unfair act or practice prohibited pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45.

59. Many states' unfair and deceptive trade practices statutes are similar to the FTC Act, and many states adopt the FTC's interpretations of what constitutes an unfair or deceptive trade practice.

60. Defendants knew or should have known of their obligation to implement appropriate measures to protect Plaintiff's and Class Members' Private Information but failed to comply with the FTC's basic guidelines.

61. Defendants' failure to employ reasonable measures to adequately safeguard against unauthorized access to PII constitutes an unfair act or practice as prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, as well as by state statutory analogs.

62. Once Defendants became aware of the breach, they could have acted far faster and more aggressively in responding to the breach and in assisting victims in redressing harms, including taking *any* steps whatsoever to attempt to mitigate the harm caused by the breach.

63. Identity thieves use such PII to, among other things, gain access to bank accounts, social media accounts, and credit cards. Identity thieves can also use this PII to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government identification cards, or create "synthetic identities." Additionally, identity thieves often wait

significant amounts of time—months or even years—to use the PII obtained in data breaches because victims often become less vigilant in monitoring their accounts as time passes, therefore making the PII easier to use without detection. These identity thieves will also re-use stolen PII and PHI, resulting in victims of one data breach suffering the effects of several cybercrimes from one instance of unauthorized access to their PII and PHI.

64. Data breaches and disclosures involving medical records are not only incredibly costly, they can "also [be] more difficult to detect, taking almost twice as long as normal identity theft."[36] The FTC warns that a thief may use private medical information to, among other things, "see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care"[37] and that this may have far reaching consequences for a victim's ability to access medical care and use insurance benefits.

V. Defendants Failed to Comply with Industry Standards

65. Security standards for businesses storing PII and PHI commonly include, but are not limited to:

a) Maintaining a secure firewall

b) Monitoring for suspicious or unusual traffic on the website

c) Looking for trends in user activity including for unknown or suspicious users

d) Looking at server requests for PII

e) Looking for server requests from VPNs and Tor exit nodes

[36] *See What to Know About Medical Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Nov. 22, 2023).

[37] *Id.*

f) Requiring Multi-factor authentication before permitting new IP addresses to access user accounts and PII

g) Structuring a system including design and control to limit user access as necessary, including a user's access to the account data and PII of other users.

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

67. Defendants failed to meet minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR- DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM- 06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIC CSC), which are all established standards in reasonable cybersecurity readiness.

68. These frameworks are existing and applicable industry standards which Defendants failed to comply with.

VI. Defendants Failed to Comply with HIPAA Guidelines

69. HIPAA requires business associates such as Defendant Cierant and covered entities such as Defendant BCBS MA to protect against reasonably foreseeable threats to the security of sensitive patient health information.

70. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

71. Title II of HIPAA contains the Administrative Simplification provisions, which require that the Department of Health and Human Services ("HHS") create rules to streamline standards for handling PII like the data that was not adequately safeguarded by Defendants.

72. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII/PHI is properly maintained.[38]

73. The Data Breach itself resulted from a combination of inadequacies showing Defendants failed to comply with safeguards mandated by HIPAA. Defendants' safety failures include, but are not limited to:

a) Failing to ensure the confidentiality and integrity of electronic PHI that they create, receive, maintain, and transmit in violation of 45 C.F.R. § 164.306(a)(1);

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

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

d) Failing to ensure compliance with HIPAA security standards by Defendants' workforce in violation of 45 C.F.R. § 164.306(a)(4);

[38] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

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

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

g) Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents known to Defendants in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

h) Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

VII. Plaintiff's and Class Members' Experiences.

74. Plaintiff received notice of the Data Breach on or around July 3, 2025, informing him that his sensitive information was part of Defendant Cierant's Data Breach. The Data Breach Notice lists Defendant BCBS MA as the customer through which Defendant Cierant originally obtained Plaintiff's Private Information.[39]

75. Plaintiff has had a Blue Cross Blue Shield of Massachusetts health insurance plan for the last two years.

76. Prior to the Data Breach, Plaintiff has always taken reasonable precautions to protect his data.

[39] *See* Exhibit A.

77. Plaintiff provided Defendant with his most sensitive medical and personal information and cannot be sure how much of it was exfiltrated.

78. Plaintiff suffered an actual injury in the form of damages and diminution in the value of his Private Information—a form of tangible property that Plaintiff entrusted to Defendants, which was compromised in and because of the Data Breach. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

79. Plaintiff has suffered imminent and impending injury arising from the heightened risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

80. Plaintiff has a continuing interest in ensuring that his Private Information, which upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

VIII. Defendants Breached Their Obligations to Plaintiff and the Class

81. Defendants fail to offer any compensation to victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and they entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' Private Information, out-of-pocket costs, and the time taken by Plaintiff and Class Members to mitigate their injuries.

82. Plaintiff and Class Members have been damaged by the compromise and exfiltration by cybercriminals 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 the Data Breach.

83. Plaintiff and Class Members were damaged since their Private Information is being sold or potentially for sale by cybercriminals in the years to come.

84. As a direct and proximate consequence of Defendants' conduct, Plaintiff and Class Members have been placed at an imminent, actual, and substantial risk of harm from fraud and identity theft, especially considering the actual fraudulent misuse of the Private Information that has already taken place.

85. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

86. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Plaintiff 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. Plaintiff 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.

87. Plaintiff 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 Plaintiff and Class Members.

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

89. Cybercriminals sell health information at a far higher premium than stand-alone PII. This is because health information enables thieves to go beyond traditional identity theft and obtain medical treatments, purchase prescription drugs, submit false bills to insurance

companies, or even undergo surgery under a false identity.[40] The shelf life for this information is also much longer—while individuals can update their credit card numbers, they are less likely to change their health insurance information. When medical identity theft occurs, the associated costs to victims can be exorbitant. According to a 2015 study, at least 65% of medical identity theft victims had to "pay an average of $13,500 to resolve the crime."[41]

90. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

91. Many Class Members 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) Cancelling 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;

[40]Medical Identity Theft: FAQs for Health Care Providers and Health Plans, FEDERAL TRADE COMMISSION, *available at* https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf (last accessed Jan. 8, 2024).

[41]Justin Klawans, *What is medical identity theft and how can you avoid it?*, THE WEEK (Aug. 2, 2023), https://theweek.com/feature/briefing/1025328/medical-identity-theft-how-to-avoid.

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.

92. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendants, 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.

CLASS ACTION ALLEGATIONS

93. Plaintiff brings this class action on behalf of himself and all other similarly situated individuals under Federal Rules of Civil Procedure 23(a), 23(b)(2), and 23(b)(3), on behalf of the following class (the "Class"):

> All individuals within the United States whose PII and/or PHI were identified as compromised in the Data Breach.

94. Excluded from the Class are governmental entities, Defendants, any entity in which Defendants have a controlling interest, and Defendants' officers, directors, affiliates, legal representatives, employees, coconspirators, successors, subsidiaries, and assigns. Also excluded

from the Class are any judges, justices, or judicial officers presiding over this matter and the members of their immediate families and judicial staff.

95. This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements therein.

96. **Numerosity.** The Class is so numerous that the individual joinder of all members is impracticable. Defendant Cierant has reported to the United States Department of Health and Human Services Office for Civil Rights that 232,506 individuals were impacted by the breach. The Class is sufficiently numerous to warrant certification.

97. **Commonality.** Common legal and factual questions exist that predominate over any questions affecting only individual Class Members. These common questions, which do not vary among Class Members and which may be determined without reference to any Class Member's individual circumstances, include, but are not limited to:

a) Whether Defendants failed to take adequate and reasonable measures to ensure their website and data systems were protected;

b) Whether Defendants failed to take available steps to prevent and stop the breach from happening or mitigating the risk of a long-term breach;

c) Whether Defendants unreasonably delayed in notifying Plaintiff and Class Members of the harm they suffered once the suspicious activity was detected;

d) Whether Defendants owed a legal duty to Plaintiff and Class Members to protect their PII and PHI;

e) Whether Defendants breached any duty to protect the personal information of Plaintiff and Class Members by failing to exercise due care in protecting their PII and PHI;

f) Whether Defendants took sufficient steps to secure Class Members' Private Information;

g) Whether Defendants were unjustly enriched;

h) Whether Plaintiff and Class Members are entitled to actual, statutory, or other forms of damages and other monetary relief; and,

i) Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief or restitution.

98. **Typicality.** Plaintiff's claims are typical of other Class Members' claims because Plaintiff and Class Members were subjected to the same allegedly unlawful conduct and damaged in the same way.

99. **Adequacy of Representation.** Plaintiff is an adequate class representative because he is a Class Member, and his interests do not conflict with the Class's interests. Plaintiff retained counsel who are competent and experienced in class action and data breach litigation. Plaintiff and his counsel intend to prosecute this action vigorously for the Class's benefit and will fairly and adequately protect his interests.

100. **Predominance and Superiority.** The Class can be properly maintained because the above common questions of law and fact predominate over any questions affecting individual Class Members. A class action is also superior to other available methods for the fair and efficient adjudication of this litigation because individual litigation of each Class Member's claim is impracticable. Even if each Class Member could afford individual litigation, the court system could not. It would be unduly burdensome if thousands of individual cases proceed. Individual litigation also presents the potential for inconsistent or contradictory judgments, the prospect of a race to the courthouse, and the risk of an inequitable allocation of recovery among

those with equally meritorious claims. Individual litigation would increase the expense and delay to all parties and the courts because it requires individual resolution of common legal and factual questions. By contrast, the class-action device presents far fewer management difficulties and provides the benefit of a single adjudication, economies of scale, and comprehensive supervision by a single court.

101. **Declaratory and Injunctive Relief.** The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members that would establish incompatible standards of conduct for Defendants. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class Members and impair their interests. Defendants have acted and/or refused to act on grounds generally applicable to the Class, making final injunctive relief or corresponding declaratory relief appropriate.

CLAIMS FOR RELIEF

Count 1
Negligence
On behalf of Plaintiff and the Class

102. Plaintiff, individually and on behalf of the Class, incorporates by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

103. Plaintiff and Class Members entrusted their PII and PHI to Defendants with the understanding that they would safeguard their PII and PHI.

104. Defendants had full knowledge of the sensitivity of the PII and PHI that they stored and the types of harm that Plaintiff and Class Members could and would suffer if that PII and PHI were wrongfully disclosed.

105. Defendants violated their duty to implement and maintain reasonable security procedures and practices. That duty includes, among other things, designing, maintaining, and testing Defendants' information security controls sufficiently rigorously to ensure that PII and PHI in their possession was adequately secured by, for example, encrypting sensitive personal information, installing effective intrusion detection systems and monitoring mechanisms, using access controls to limit access to sensitive data, regularly testing for security weaknesses and failures, failing to notify victims of the specific breached data in a timely manner, and failing to remedy the continuing harm by unreasonably delaying notifying specific victims who were harmed.

106. Defendants' duty of care arose from, among other things,

a) The special relationship between Defendants, Plaintiff, and Class Members resulting from Plaintiff and Class Members entrusting Defendants with confidential PII/PHI;

b) Defendants' exclusive ability (and Class Members' inability) to ensure that their systems, website, and vendor services were sufficient to protect against the foreseeable risk that a data breach could occur;

c) HIPAA, which requires covered entities such as Defendant BCBS MA to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

d) Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, failing to adopt reasonable data security measures; and

e) Defendants' common law duties to adopt reasonable data security measures to protect PII and PHI under their possession and to act under the same or similar circumstances as a reasonable and prudent person would act.

107. Plaintiff and Class Members were the foreseeable victims of Defendants' inadequate data security. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches. Defendants knew that a breach of their systems could and would cause harm to Plaintiff and Class Members.

108. Defendants' conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendants' conduct included their failure to adequately mitigate harm through negligently failing to inform victims of the breach of the specific information breached.

109. Defendants knew or should have known of the inherent risks in collecting and storing massive amounts of PII and PHI and the importance of limiting disclosure of that PII and PHI.

110. Defendants, through their actions and inactions, breached their duty owed to Plaintiff and Class Members by failing to exercise reasonable care in safeguarding their PII and PHI while it was in their possession and control. Defendants breached their duty by, among other things, their failure to adopt reasonable data security practices and their failure to adopt reasonable security and notification practices, failure to monitor the security of their networks and systems, and allowing unauthorized access to Plaintiff's and Class Members' Private Information.

111. Defendants inadequately safeguarded PII and PHI in breach of standard industry rules, regulations, and best practices at the time of the Data Breach.

112. But for Defendants' breach of their duty to adequately protect Class Members' PII and PHI, Class Members' PII and PHI would not have been stolen.

113. There is a temporal and close causal connection between Defendants' failure to implement adequate data security measures and notification practices, the Data Breach/unauthorized disclosure, and the harms suffered by Plaintiff and Class Members.

114. As a result of Defendants' failure to timely notify Plaintiff and Class Members that their Private Information had been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

115. As a direct and traceable result of Defendants' negligence, Plaintiff and Class Members suffered and will continue to suffer damages, including monetary damages, increased risk of future harm, loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach, overpayment for the services and products that were received without adequate data security; and embarrassment, humiliation, and emotional distress.

116. Plaintiff and Class Members are entitled to all forms of monetary compensation set forth herein, including monetary payments to provide adequate identity protection services. Plaintiff and Class Members are also entitled to the injunctive relief sought herein.

117. Plaintiff also seeks such other relief as the Court may deem just and proper.

Count 2
Negligence *Per Se*
On behalf of Plaintiff and the Class

118. Plaintiff, individually and on behalf of the Class, incorporates by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

119. Section 5 of the FTC Act, 15 U.S.C. § 45 prohibits, "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information.

120. Defendants violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information and by failing to comply with industry standards.

121. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendants' systems. Plaintiff was required to provide PII and PHI to Defendants. Plaintiff and Class Members entrusted their PII and PHI to Defendants with the understanding that Defendants would safeguard their PII and PHI.

122. Class Members are within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

123. Pursuant to HIPAA, 42 U.S.C. § 1302d *et seq*., Defendants had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

124. Pursuant to HIPAA, Defendants had a duty to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in

which there is a low probability of assigning meaning without use of a confidential process or key." *See* 45 C.F.R. § 164.304 (defining "encryption").

125. Defendants' failure to comply with applicable laws and regulations constitutes negligence *per se*.

126. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

127. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they failed to meet their duties, and that Defendants' breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

128. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

Count 3
Breach of Implied Contract
On behalf of Plaintiff and the Class

129. Plaintiff, individually and on behalf of the Class, incorporates by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

130. Plaintiff and Class Members were the third-party beneficiaries of contracts with Defendant Cierant.

131. Plaintiff and Class Members provided and entrusted their Private Information to Defendants as part of Defendants' regular business practices.

132. Plaintiff and Class Members entrusted their Private Information to Defendants. In so doing, Plaintiff and Class Members entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect Private Information, and to timely and accurately notify Plaintiff and the Class if their data has been breached and compromised or stolen.

133. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards.

134. Implicit in the agreement between Plaintiff, Class Members, and Defendants to provide Private Information, was Defendants' obligation to: (1) use such Private Information for business purposes only, (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class Members' Private Information, (3) prevent unauthorized disclosures of the Private Information, and (4) retain Private information only under conditions that kept such information secure and confidential.

135. As part of these transactions, Defendants agreed to safeguard and protect the PII of Plaintiff and Class Members and to timely and accurately notify them if their PII or PHI was breached or compromised.

136. Plaintiff and Class Members entered into the implied contracts with the reasonable expectation that Defendants' data security practices and policies were reasonable and consistent with the legal requirements, industry standards, and Defendants' own representations.

137. Implicit in the agreement between Defendants, Plaintiff, and Class Members, was the obligation that all parties would maintain information confidentially and securely.

138. These exchanges constituted an agreement and meeting of the minds between the parties.

139. When the parties entered into an agreement, mutual assent occurred. Plaintiff and Class Members would not have provided and entrusted their PII and PHI to Defendants in the absence of the implied contract or implied terms between them and Defendants. The safeguarding of the PII and PHI of Plaintiff and Class Members was critical to realize the intent of the parties.

140. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendants.

141. Defendants breached their implied contracts with Plaintiff and Class Members to protect their PII and PHI when they (1) failed to take reasonable steps to use safe and secure systems to protect that information; (2) failed to comply with industry standards; (3) failed to comply with the legal obligations necessarily incorporated into these agreements; and (4) failed to notify Plaintiff and Class Members of the specific data breached in a reasonably timely manner.

142. As a direct and proximate result of Defendants' breach of implied contract, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, medical identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent

initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of their PII and PHI; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Defendants' Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

143. As a direct and proximate result of the breach/unauthorized disclosure, Plaintiff and Class Members are entitled to relief as set forth herein.

144. Plaintiff also seeks such other relief as the Court may deem just and proper.

Count 4
Unjust Enrichment
On behalf of Plaintiff and the Class

145. Plaintiff, individually and on behalf of the Class, incorporates by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

146. This count is brought in the alternative to Plaintiff's breach of contract claim.

147. Plaintiff and Class Members conferred a benefit on Defendants when they provided their Private Information to Defendants.

148. Upon information and belief, the monies paid to Defendants in the ordinary course of business included a premium for Defendants' cybersecurity obligations and were supposed to be used by Defendants, in part, to pay for the administrative and other costs of providing reasonable data security and protection for Plaintiff's and Class Members' Private Information.

149. Defendants, however, failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide adequate data security in return for the benefit Plaintiff and Class Members provided.

150. Defendants would not be able to carry out an essential function of their regular business without the money obtained in the ordinary course of business and Private Information provided by Plaintiff and Class Members. Plaintiff and Class Members expected that Defendants or anyone in Defendants' position would use a portion of that revenue to fund adequate data security practices.

151. Defendants acquired the Private Information through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

152. Defendants knew that Plaintiff and Class Members conferred a benefit upon them, which Defendants accepted. Defendants profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes, while failing to use the payments they received for adequate data security measures that would have secured Plaintiff's and Class Members' Private Information and prevented the Data Breach.

153. If Plaintiff and Class Members knew that Defendants had not reasonably secured their Private Information, they would not have provided their Private Information to Defendants.

154. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to increase their own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and cheaper contractors and diverting those funds to their own profits. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendants decision to prioritize their own profits over the requisite security and the safety of their Private Information.

155. Under the principles of equity and good conscience, Defendants should not be permitted to retain the benefits that Plaintiff and Class Members conferred upon them.

156. Plaintiff and Class Members have no adequate remedy at law.

157. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered or will suffer injuries described herein.

158. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid to Defendants.

159. Plaintiff also seeks such other relief as the Court may deem just and proper.

Count 5
Injunctive/Declaratory Relief
On behalf of Plaintiff and the Class

160. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and state statutes described herein.

161. Defendants owe a duty of care to Plaintiff and Class Members, which required Defendants to adequately monitor and safeguard Plaintiff's and Class Members' PII and PHI.

162. Defendants and their officers, directors, affiliates, legal representatives, employees, co-conspirators, successors, subsidiaries, and assigns still possess the PII and PHI belonging to Plaintiff and Class Members.

163. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and PHI and whether Defendants are currently maintaining

data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII and PHI. Plaintiff alleges that Defendants' data security measures remain inadequate. Furthermore, Plaintiff and the Class continue to suffer injury as a result of the compromise of their PII and PHI and the risk remains that further compromises of their private information will occur in the future.

164. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a) Defendants owe a legal duty to adequately secure the PII and PHI of Plaintiff and the Class within their care, custody, and control under the common law, HIPAA, and Section 5 of FTC Act;

b) Defendants breached their duty to Plaintiff and the Class by allowing the Data Breach to occur;

c) Defendants' existing data monitoring measures do not comply with their obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect the PII and PHI of Plaintiff and the Class within Defendants' custody, care, and control; and

d) Defendants' ongoing breaches of said duties continue to cause harm to Plaintiff and the Class.

165. This Court should also issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with industry standards to protect

the PII and PHI of Plaintiff and the Class within its custody, care, and control, including the following:

a) Order Defendants to provide lifetime credit monitoring and identity theft insurance and protection services to Plaintiff and Class Members; and

b) Order that, to comply with Defendants' obligations and duties of care, Defendants must implement and maintain reasonable security and monitoring measures, including, but not limited to:

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

ii. Encrypting and anonymizing the existing PII and PHI within their servers, networks, and systems to the extent practicable, and purging all such information which is no longer reasonably necessary for Defendants to provide services to its employees or customers;

iii. Engaging third-party security auditors and internal personnel to run automated security monitoring;

iv. Auditing, testing, and training their security personnel regarding any new or modified procedures;

v. Segmenting their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems, networks, and servers;

vi. Conducting regular database scanning and security checks; and

vii. Routinely and continually conducting internal training and education to inform Defendants' internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

166. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach or cybersecurity incident. This risk is real, immediate, and substantial. If another data breach or cybersecurity incident

occurs, Plaintiff and the Class will not have an adequate remedy at law because monetary relief alone will not compensate Plaintiff and the Class for the serious risks of future harm.

167. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Plaintiff and the Class will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendants' compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

168. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach or cybersecurity incident, thus preventing future injury to Plaintiff and the Class and other persons whose PII and PHI would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class set forth herein, respectfully requests the following relief:

A. That the Court certify this action as a class action and appoint Plaintiff and his counsel to represent the Class;

B. That the Court grant permanent injunctive relief to prohibit Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein and directing Defendants to adequately safeguard the PII and PHI of Plaintiff and the Class by implementing improved security controls;

C. That the Court award compensatory, consequential, and general damages, including nominal damages as appropriate, as allowed by law in an amount to be determined at trial;

D. That the Court award statutory or punitive damages as allowed by law in an amount to be determined at trial;

E. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of Defendants' unlawful acts, omissions, and practices;

F. That the Court award to Plaintiff and Class Members the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

G. That the Court award pre- and post-judgment interest at the maximum legal rate; and

H. All such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial on all claims so triable.

Dated: August 14, 2025

Respectfully submitted,

MILLER SHAH LLP

/s/ Laurie Rubinow
Laurie Rubinow
65 Main Street
Chester, CT 06412
Telephone: (866) 540-5505
Facsimile: (866) 300-7367
Email: lrubinow@millershah.com

Amber L. Schubert* (CA Bar No. 278696)
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Ste. 200
San Francisco, CA 94123
Telephone: 415-788-4220
Facsimile: 415-788-0161
Email: aschubert@sjk.law

Counsel for Plaintiff and the Proposed Class

**pro hac vice* forthcoming