

**UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS
EASTERN DIVISION**

Ileana May, on behalf of herself and all others similarly situated, Plaintiff, v. DentaQuest Group, Inc., Defendant.	CASE NO. _____ JURY DEMAND
---	---

CLASS ACTION COMPLAINT

Plaintiff Ileana May (“Plaintiff”) brings this Class Action Complaint (“Complaint”) against Defendant DentaQuest Group, Inc., (“DentaQuest” or “Defendant”) individually, on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels’ investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This Class Action arises from a recent cyberattack resulting in a data breach of sensitive information in the possession and custody and/or control of Defendant (the “Data Breach”).
2. DentaQuest’s breach differs from typical data breaches because it affects consumers who had no relationship with DentaQuest, never sought one, and never consented to it collecting and storing their information.
3. DentaQuest sourced their information from third parties, stored it on DentaQuest’s systems, and assumed a duty to protect it. But DentaQuest never implemented the security safeguards needed despite understanding the importance of doing so.

4. The Data Breach resulted in unauthorized disclosure, exfiltration, and theft of current and former consumers' highly personal information, which include, on information and belief, at least their name, Social Security number, health insurance information, and dates of birth ("personally identifying information" or "Sensitive Information.")

5. The notorious cybercriminal gang, ShinyHunter, took credit for this breach on or around May 22, 2026, when it identified Defendant on its dark web leak page, stating it would be releasing all stolen information on or around May 27, 2026, if Defendant did not pay its demanded ransom.

6. Defendant continues to delay informing Class Members of the Breach even though Plaintiff and thousands of Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

7. DentaQuest's continues to obfuscate the details of the breach, including nature of the breach and the threat it posted—refusing to tell consumers how many people were impacted, how the breach happened, and why Defendant continues delaying notifying victims that hackers had gained access to highly private Sensitive Information despite the notorious cyberhacker ShinyHunter taking credit for the Breach on or around May 22, 2026.

8. Defendant's failure to timely detect and report the Data Breach made its consumers vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Sensitive Information.

9. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of Sensitive Information misuse.

10. In failing to adequately protect Plaintiff's and the Class's Sensitive Information, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendant violated state and federal law and harmed thousands of its current and former consumers.

11. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their Sensitive Information. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

12. On information and belief, Plaintiff is a Data Breach victim.

13. Accordingly, Plaintiff, on behalf of herself and a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

PARTIES

14. Plaintiff Ileana May is a natural person and citizen and resident of La Pine, Oregon, where she intends to remain.

15. Defendant is a Delaware corporation with its principal place of business located at 96 Worcester Street, Wellesley Hills, Massachusetts 02481.

JURISDICTION AND VENUE

16. 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; Plaintiff and Defendant are citizens of different states; and there are over 100 putative Class members.

17. This Court has personal jurisdiction over Defendant because it is headquartered in Massachusetts, regularly conducts business in Massachusetts and has sufficient minimum contacts in Massachusetts.

18. Venue is proper in this Court because Defendant's principal offices are in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

STATEMENT OF FACTS

DentaQuest

19. DentaQuest touts that “[w]e are one of the largest dental benefits providers in the U.S. by membership.” It further boasts that “We manage dental and vision benefits for approximately 32 million Americans.”¹

20. As part of its business, Defendant receives and maintains the Sensitive Information of thousands of consumers. In collecting and maintaining Sensitive Information, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class members themselves took reasonable steps to secure their Sensitive Information.

¹ About us, <https://www.dentaquest.com/en/about-us> (last visited May 29, 2026).

21. DentaQuest understood the need to protect its current and former consumers' Sensitive Information and prioritize its data security.

22. Indeed, DentaQuest's Internet Privacy Policy promises that it "respects your interest in privacy when visiting our website. We are responsible for protecting the security of the personal information we collect from you." Defendant also states that "We are committed to maintaining the confidentiality of all information we receive from this website's users."²

23. DentaQuest similarly states in its Notice of Privacy Practices that it "takes your privacy seriously. We want to tell you about our privacy practices to protect your personal health information." Defendant further assures that it is "required by law to: Maintain the privacy of your health information."³

24. Despite recognizing its duty to do so, on information and belief, DentaQuest has not implemented reasonably cybersecurity safeguards or policies to protect its consumers' Sensitive Information or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to consumers' Sensitive Information.

The Data Breach

25. On information and belief, Plaintiff is a data breach victim. She is unsure how DentaQuest got her information but assumes that DentaQuest obtained her information through Advantage Dental, where she is a current patient. On information and belief, the information DentaQuest obtained includes at least her name, health insurance information, dates of birth, and Social Security Number.

² Internet Privacy Policy, <https://www.dentaquest.com/en/policies/notice-of-privacy-practices> (last visited May 29, 2026).

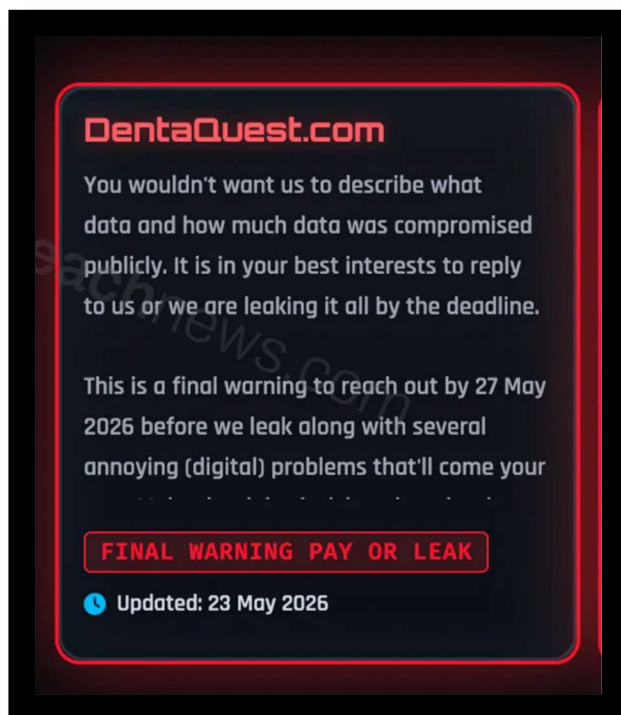
³ Notice of Privacy Policy, <https://www.dentaquest.com/en/policies/hipaa-privacy-policy> (last visited May 29, 2026).

26. On information and belief, Defendant collects and maintains consumers' Sensitive Information in its computer systems.

27. In collecting and maintaining Sensitive Information, Defendant implicitly agrees that it will safeguard the data using reasonable means according to state and federal law.

28. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class's Sensitive Information for theft and sale on the dark web.

29. On information and belief, the cybercriminals that obtained Plaintiff's and Class Members' Sensitive Information appear to be a sophisticated cybercriminal gang, Shiny Hunters. In its post, Shiny Hunters issued a 'final warning' to Defendant, stating that Defendant had until May 27, 2026, to pay its ransom or it would leak all stolen information, for any and all unauthorized individuals to further download and distribution on the dark web.



30. ShinyHunters is one of the most active ransomware actors, and Defendant, self-proclaimed leader in its industry, knew or should have known of the tactics that groups like ShinyHunters employ.⁴

31. Ransomware groups can monetize stolen Sensitive Information and sell it on the dark web as part of a full identity profile.⁵ Buyers can then use that information to conduct different types of identity theft or fraud, such as filing a fake tax return, applying for a fraudulent mortgage or opening a bank account while impersonating the victim.⁶

32. Defendant continues to delay notifying its victims of the Data Breach despite ShinyHunters taking credit of the Breach and, on information and belief, posting all stolen information, including Plaintiff's Sensitive Information, on the dark web.

33. Defendant did not in fact follow industry standard practices in securing consumers' Sensitive Information, as evidenced by the Data Breach.

34. Upon information and belief, the cybercriminals in question are particularly sophisticated. After all, the cybercriminals: (1) defeated the relevant data security systems, (2) gained actual access to sensitive data, and (3) successfully accessed data.

35. And as the Harvard Business Review notes, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."⁷

⁴ <https://www.bleepingcomputer.com/news/security/wynn-resorts-confirms-employee-data-breach-after-extortion-threat/> (last visited February 27, 2026).

⁵ Anthony M. Freed, *Which Data Do Ransomware Attackers Target for Double Extortion?*, MALICIOUSLIFE BY CYBEREASON, <https://www.cybereason.com/blog/which-data-do-ransomware-attackers-target-for-double-extortion> (listed visited Mar. 6, 2025).

⁶ *Id.*

⁷ Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) <https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back>.

36. 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 Sensitive 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.

37. On information and belief, Defendant plans to offer several months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers.

38. The risk of identity theft and unauthorized use of Plaintiff's and Class Members' Sensitive Information is substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

39. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its consumers' Sensitive Information. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the Sensitive Information.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice.

40. It is well known that Sensitive Information, including Social Security numbers, is an invaluable commodity and a frequent target of hackers.

41. 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 2017.⁸

42. In light of recent high profile data breaches, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendants knew or should have known that their electronic records would be targeted by cybercriminals.

43. Indeed, 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 take appropriate measures to prepare for and are able to thwart such an attack.

44. 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 Sensitive Information private and secure, Defendant failed to take appropriate steps to protect the Sensitive Information of Plaintiff and Class Members from being compromised.

45. In the years immediately preceding the Data Breach, Defendant knew or should have known that Defendant's computer systems were a target for cybersecurity attacks, including ransomware attacks involving data theft, because warnings were readily available and accessible via the internet.

46. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that,

⁸ Data breaches break record in 2021, CNET (Jan. 24, 2022), <https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/> (last accessed September 4, 2023).

among other things, warned that “[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector.”⁹

47. In April 2020, ZDNet reported, in an article titled “Ransomware mentioned in 1,000+ SEC filings over the past year,” that “[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay.”¹⁰

48. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a “Ransomware Guide” advising that “[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion.”¹¹

49. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) ransomware actors were targeting entities such as Defendant, (ii) ransomware gangs were ferociously aggressive in their pursuit of entities such as Defendant, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included threatening to release stolen data.

⁹ High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations, FBI, available at <https://www.ic3.gov/Media/Y2019/PSA191002> (last accessed September 4, 2023).

¹⁰ Ransomware mentioned in 1,000+ SEC filings over the past year, ZDNet, <https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/> (last accessed September 4, 2023).

¹¹ Ransomware Guide, U.S. CISA, <https://www.cisa.gov/stopransomware/ransomware-guide> (last accessed September 4, 2023).

50. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted Sensitive Information of thousands of its current and former employees in an Internet-accessible environment, had reason to be on guard for the exfiltration of the Sensitive Information and Defendant's type of business had cause to be particularly on guard against such an attack.

51. Before the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' Sensitive Information could be accessed, exfiltrated, and published as the result of a cyberattack. Notably, data breaches are prevalent in today's society therefore making the risk of experiencing a data breach entirely foreseeable to Defendants.

52. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted their consumers' sensitive data elements within the Sensitive Information to protect against their publication and misuse in the event of a cyberattack.

Plaintiff's Experience

53. On information and belief, Plaintiff is a data breach victim. She is unsure how DentaQuest got her information but assumes that DentaQuest obtained her information through Advantage Dental, where she is a current patient. On information and belief, the information DentaQuest obtained includes at least her name, health insurance information, dates of birth, and Social Security Number.

54. Defendant deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to promptly notify her and continuing to delay notification.

55. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's Sensitive Information for theft by cybercriminals and sale on the dark web.

56. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

57. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff fears for her personal financial security and uncertainty over what Sensitive Information was exposed in the Data Breach.

58. Plaintiff has and is experiencing feelings of anxiety, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

59. Plaintiff have suffered actual injury in the form of damages to and diminution in the value of her Sensitive Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

60. Plaintiff suffered actual injury from the exposure of her Sensitive Information—which violates her rights to privacy.

61. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Sensitive Information being placed in the hands of unauthorized third parties and possibly criminals.

62. Further and also following the Data Breach, Plaintiff began receiving spam texts and calls, on the same phone number that, on information and belief, MedQuest obtained to provide its services to Plaintiff. Further, the information exposed by Defendant's data breach

was more than enough for cybercriminals to use and gather additional information to send her scam texts and calls.

63. These spam texts and calls are further evidence that her Sensitive Information is now in the hands of cybercriminals.

64. Once an individual's Sensitive Information has been stolen by cybercriminals and is for sale and access on the dark web, as Plaintiff's Sensitive Information is here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.¹² On information and belief, the spam calls and texts that Plaintiff is experiencing is a result of the Data Breach.

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

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

66. Plaintiff and members of the proposed Class have suffered injury from the misuse of their Sensitive Information that can be directly traced to Defendant.

67. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

- a. The loss of the opportunity to control how their Sensitive Information is used;
- b. The diminution in value of their Sensitive Information;

¹² What do Hackers do with Stolen Information, Aura, <https://www.aura.com/learn/what-do-hackers-do-with-stolen-information> (last visited January 9, 2024).

- c. The compromise and continuing publication of their Sensitive Information;
- d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
- e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;
- f. Delay in receipt of tax refund monies;
- g. Unauthorized use of stolen Sensitive Information; and
- h. The continued risk to their Sensitive Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Sensitive Information in its possession.

68. Stolen Sensitive Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII alone can be worth up to \$1,000.00 depending on the type of information obtained.

69. The value of Plaintiff's and the Class's Sensitive Information on the black market is considerable. Stolen Sensitive Information trades on the black market for years, and criminals frequently post stolen Sensitive Information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

70. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

71. One such example of criminals using Sensitive Information for profit is the development of “Fullz” packages.

72. Cyber-criminals can cross-reference two sources of Sensitive Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as “Fullz” packages.

73. The development of “Fullz” packages means that stolen Sensitive Information from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class’ phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Sensitive Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff’s and the Class’s stolen Sensitive Information is being misused, and that such misuse is fairly traceable to the Data Breach.

74. Defendant disclosed the Sensitive Information of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the Sensitive Information of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking,

unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Sensitive Information.

75. Defendant’s failure to properly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff’s and the Class’s injury by depriving them of the earliest ability to take appropriate measures to protect their Sensitive Information and take other necessary steps to mitigate the harm caused by the Data Breach.

Consumers Prioritize Data Security

76. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year “Consumer Privacy Survey.”¹³ Therein, Cisco reported the following:

- a. “For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a customer requirement with more than 75% of consumer respondents saying they won’t purchase from an organization they don’t trust with their data.”¹⁴
- b. “Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly.”¹⁵
- c. 89% of consumers stated that “I care about data privacy.”¹⁶
- d. 83% of consumers declared that “I am willing to spend time and money to protect data” and that “I expect to pay more” for privacy.¹⁷

¹³ *Privacy Awareness: Consumers Taking Charge to Protect Personal*, CISCO, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited March 19, 2025).

¹⁴ *Id.* at 3.

¹⁵ *Id.*

¹⁶ *Id.* at 9.

¹⁷ *Id.*

- e. 51% of consumers revealed that “I have switched companies or providers over their data policies or data-sharing practices.”¹⁸
- f. 75% of consumers stated that “I will not purchase from organizations I don’t trust with my data.”¹⁹

77. Defendant knew or should have known that adequate implementation of cybersecurity and protection of Sensitive Information, including Plaintiff and the Class’s Sensitive Information, was important to its consumers.

Defendant failed to adhere to FTC guidelines.

78. According to the Federal Trade Commission (“FTC”), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of Sensitive Information.

79. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

- a. protect the sensitive consumer information that it keeps;
- b. properly dispose of Sensitive Information that is no longer needed;
- c. encrypt information stored on computer networks;
- d. understand their network’s vulnerabilities; and
- e. implement policies to correct security problems.

¹⁸ *Id.*

¹⁹ *Id.* at 11.

80. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

81. The FTC recommends that companies not maintain 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.

82. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer 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 to meet their data security obligations.

83. Defendant’s failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers’ Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Fails to Comply with Industry Standards

84. As noted above, experts studying cyber security routinely identify entities in possession of Sensitive Information as being particularly vulnerable to cyberattacks because of the value of the Sensitive Information which they collect and maintain.

85. Several best practices have been identified that a minimum should be implemented by employers in possession of Sensitive Information, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including

firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

86. Other best cybersecurity practices that are standard for employers 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. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

87. Upon information and belief, Defendants failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both 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).

88. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its consumers. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

89. Plaintiff brings this class action individually and on behalf of all members of the following class:

All individuals residing in the United States whose Sensitive Information was compromised in the Data Breach, including all those who received notice of the breach.

90. Excluded from the Class is Defendant, their agents, affiliates, parents, subsidiaries, any entity in which Defendant have a controlling interest, any of Defendant's officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

91. Plaintiff reserves the right to amend the class definition.

92. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of their claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

- a. **Numerosity.** Plaintiff is representative of the Class, consisting of several thousand members, far too many to join in a single action;
- b. **Ascertainability.** Members of the Class are readily identifiable from information in Defendant's possession, custody, and control;
- c. **Typicality.** Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.
- d. **Adequacy.** Plaintiff will fairly and adequately protect the proposed Class's interests. Her interests do not conflict with the Class's interests, and she has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

- e. **Commonality.** Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class.

Indeed, it will be necessary to answer the following questions:

- i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's Sensitive Information;
- ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- iii. Whether Defendant were negligent in maintaining, protecting, and securing Sensitive Information;
- iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's Sensitive Information;
- v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;
- vi. Whether the Data Breach caused Plaintiff's and the Class's injuries;
- vii. What the proper damages measure is; and
- viii. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

93. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

94. Plaintiff realleges all previous paragraphs as if fully set forth below.

95. Plaintiff and members of the Class entrusted their Sensitive Information to Defendant. Defendant owed to Plaintiff and the Class a duty to exercise reasonable care in handling and using the Sensitive Information in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

96. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their Sensitive Information in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that Sensitive Information —just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and the Class's Sensitive Information by disclosing and providing access to this information to unauthorized third parties and by failing to properly supervise both the way the Sensitive Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

97. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their Sensitive Information. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and the Class to take appropriate measures to protect their Sensitive Information,

to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

98. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and the Class's Sensitive Information.

99. The risk that unauthorized persons would attempt to gain access to the Sensitive Information and misuse it was foreseeable. Given that Defendant holds vast amounts of Sensitive Information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Sensitive Information —whether by malware or otherwise.

100. Sensitive Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Sensitive Information of Plaintiff and the Class and the importance of exercising reasonable care in handling it.

101. Defendant breached its duties by failing to exercise reasonable care in supervising its employees, agents, contractors, vendors, and suppliers, and in handling and securing the Sensitive Information of Plaintiff and the Class which actually and proximately caused the Data Breach and Plaintiff's and the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and the Class

have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

102. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Class's Sensitive Information.

103. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, patients' Sensitive Information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the members of the Class's Sensitive Information.

104. Defendant breached its duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Sensitive Information.

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

106. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's Sensitive Information and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendant collected and stored and the foreseeable consequences of a data breach, including,

specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

107. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

108. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect their PHI and by not complying with applicable regulations detailed *supra*. Here too, Defendant's conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

109. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

110. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their Sensitive Information.

111. Had Plaintiff and the Class known that Defendant did not adequately protect their Sensitive Information, Plaintiff and members of the Class would not have entrusted Defendant with their Sensitive Information.

112. Defendant's various violations and its failure to comply with applicable laws and regulations constitute negligence *per se*.

113. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Sensitive Information by criminals, improper disclosure of their Sensitive Information, lost benefit of their bargain, lost value of their Sensitive Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Breach of Third-Party Contract
(On Behalf of Plaintiff and the Class)

114. Plaintiff realleges all previous paragraphs as if fully set forth below.

115. Defendant entered into various contracts with its clients to provide insurance services to its clients' customer's; Defendant's consumer.

116. These contracts are virtually identical to each other and were made expressly for the benefit of Plaintiff and the Class, as it was their confidential Sensitive Information that Defendant agreed to collect and protect through its services. Thus, the benefit of collection and protection of the Sensitive Information belonging to Plaintiff and the Class were the direct and primary objective of the contracting parties.

117. Defendant knew that if it were to breach these contracts with its clients, the clients' consumers, including Plaintiff and the Class, would be harmed by, among other things, fraudulent misuse of their Sensitive Information.

118. Defendant breached its contracts with its clients when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiff's and Class Members' Sensitive Information.

119. As reasonably foreseeable result of the breach, Plaintiff and the Class were harmed by Defendant's failure to use reasonable data security measures to store their Sensitive Information, including but not limited to, the actual harm through the loss of their Sensitive Information to cybercriminals.

120. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

121. Plaintiff realleges all previous paragraphs as if fully set forth below.

122. This claim is pleaded in the alternative to the breach of contractual duty claim.

123. Plaintiff and members of the Class conferred a benefit upon Defendant in providing Sensitive Information to Defendant.

124. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and the Class. Defendant also benefited from the receipt of Plaintiff's and the Class's Sensitive Information, as this was used to facilitate the treatment, services, and goods it sold to Plaintiff and the Class.

125. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the Class's Sensitive Information because Defendant failed to adequately protect their Sensitive Information. Plaintiff and the proposed

Class would not have provided their Sensitive Information to Defendant had they known Defendant would not adequately protect their Sensitive Information.

126. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT IV
Invasion of Privacy—Intrusion Upon Seclusion
(On Behalf of Plaintiff and the Class)

127. Plaintiff realleges all previous paragraphs as if fully set forth below.

128. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential Sensitive Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

129. Defendant owed a duty to its consumers, including Plaintiff and the Class, to keep this information confidential.

130. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff's and Class Members' Sensitive Information is highly offensive to a reasonable person.

131. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant as part of their employment, but they did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

132. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

133. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

134. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

135. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

136. As a proximate result of Defendant's acts and omissions, the Sensitive Information of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

137. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class because their Sensitive Information are still maintained by Defendant with its inadequate cybersecurity system and policies.

138. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the Sensitive Information of Plaintiff and the Class.

139. In addition to injunctive relief, Plaintiff, on behalf of herself and the other members of the Class, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

PRAYER FOR RELIEF

Plaintiff and the Class demand a jury trial on all claims so triable and request that the Court enter an order:

- A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing their counsel to represent the Class;
- B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;
- C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;
- D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen Sensitive Information;
- E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;
- F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;
- G. Awarding attorneys' fees and costs, as allowed by law;
- H. Awarding prejudgment and post-judgment interest, as provided by law;

- I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and
- J. Granting such other or further relief as may be appropriate under the circumstances.

Dated: May 29, 2026,

Respectfully submitted,

By: /s/ Casondra Turner
Casondra Turner (MA BBO 687682)
MILBERG, PLLC
260 Peachtree Street NW, Suite 2200
Atlanta, GA 30303
Telephone: 771-772-3086
cturner@milberg.com

Samuel J. Strauss (*Pro Hac Vice* forthcoming)
Raina Borelli (*Pro Hac Vice* forthcoming)
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
(872) 263-1100
(872) 263-1109 (facsimile)
sam@straussborrelli.com
raina@straussborrelli.com

Attorneys for Plaintiff and Proposed Class