Exhibit A1

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF TENNESSEE

JENNIFER SYLVESTER, JASON PEFFLEY, and JAMES FORSYTHE individually and on behalf of all others similarly situated, Plaintiffs, v. UNITED SEATING AND MOBILITY, LLC d/b/a NUMOTION, Defendant.	Case No. 3:25-cv-00469 Judge Aleta A. Trauger Jury Demand

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Jennifer Sylvester, Jason Peffley, and James Forsythe ("Plaintiffs"), on behalf of themselves and all others similarly situated ("Class Members"), allege the following against Defendant United Seating and Mobility, LLC d/b/a Numotion ("Defendant"), upon personal knowledge as to Plaintiffs and their own actions, and upon information and belief, including the investigation of counsel as follows:

I. INTRODUCTION

1. This action arises from Defendant's failure to safeguard the Personally Identifiable Information[1] ("PII") and Protected Health Information ("PHI") (collectively, "Private Information") of Plaintiffs and the proposed Class Members, who are approximately 494,326 of Defendant's current and former customers. Specifically, between September 2, 2024, and

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

November 18, 2024, an unknown, unauthorized criminal hacker accessed Defendant's network systems and exfiltrated Plaintiffs' and Class Members' Private Information stored therein, including their names, dates of birth, driver's license Social Security numbers, product information payment and financial account information health insurance information and medical information (the "Data Breach"), causing widespread injury and damages to Plaintiffs and Class Members.

2. According to its website, Defendant "is the nation's largest and leading provider of products and services to help individuals with mobility limitations," selling complex rehabilitation technology products and services, including catheters, wheelchair accessible vehicles, repair services, and other products and services for individuals with mobility challenges.[2]

3. Plaintiffs are former customers of Defendant. As a condition of receiving medical equipment products from Defendant, Plaintiffs and Class Members were required to entrust Defendant with their sensitive names, dates of birth, driver's license Social Security numbers, product information payment and financial account information health insurance information and medical information

4. As the custodian of Plaintiffs' and Class Members' Private Information it collected and maintained, Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to unauthorized third parties, and to keep the Private Information safe and confidential. Defendant had obligations under the Federal Trade Commission ("FTC") Act, 15 U.S.C. § 45 ("FTC Act"), HIPAA, contract, statutory and common law, industry standards, and representations made to Plaintiffs and Class Members, to keep their Private Information secure and to protect it from unauthorized access and disclosure.

[2] https://www.numotion.com/about-us (last accessed Mar. 21, 2025).

5. Defendant breached these duties owed to Plaintiffs and Class Members by failing to safeguard the Private Information it collected and maintained, including by failing to implement industry standards for data security to protect against cyberattacks, resulting in the Data Breach.

6. According to Defendant's March 11, 2025 letter notifying Plaintiffs and other affected individuals of the Data Breach ("Notice Letter"), between approximately September 2, 2024 and November 18, 2024, an unauthorized cybercriminal gained access to an employe email account and acquired files containing Plaintiffs' and Class Members' Personal Information.[3]

7. Although the Data Breach occurred between September 2, 2024 and November 18, 2024, Defendant failed to notify and warn Plaintiffs and Class Members of the unauthorized disclosure of their Private Information until March 11, 2025, over ***three months*** later.

8. As a direct result of the Data Breach, which Defendant failed to prevent, the Private Information of Defendant's customers and employees, including Plaintiffs and Class Members, was stolen to the hands of an unknown criminal hacker.

9. Plaintiffs and Class Members now face a lifetime risk of identity theft due to the nature of the Private Information lost, which they cannot change, and which cannot be made private again.

10. Defendant's harmful conduct has injured Plaintiffs and Class Members in multiple ways, including, inter alia (i) the lost or diminished value of their Private Information; (ii) costs associated with the prevention, detection, and recovery from identity theft, tax fraud, and other unauthorized use of their data; (iii) lost opportunity costs to mitigate the Data Breach's consequences, including lost time; and (iv) emotional distress associated with the loss of control over their highly sensitive Private Information.

[3] *See* Notice of Security Incident Sent to Plaintiffs, attached hereto as **Exhibit A**.

11. Defendant's failure to protect Plaintiffs' and Class Members' Private Information has harmed and will continue to harm thousands of Defendant's customers, causing Plaintiffs to seek relief on a class-wide basis.

12. Plaintiffs bring this action on behalf of herself and all others similarly situated, the proposed Class of persons whose Private Information was compromised in the Data Breach, asserting causes of action for (i) negligence; (ii) negligence per se; (iii) breach of implied contract; (iv) breach of confidence; (v) unjust enrichment; and (vi) invasion of privacy; seeking an award of monetary damages and injunctive and declaratory relief, resulting from Defendant's failure to adequately protect their Private Information.

II. PARTIES

13. Plaintiff Jennifer Sylvester is a natural person, resident, and citizen of Wisconsin.

14. Plaintiff Jason Peffley is a natural person, resident, and citizen of California.

15. Plaintiff James Forsythe is a natural person, resident, and citizen of Pennsylvania.

16. Like Plaintiffs, other potential Class Members received similar notices informing them that their PII and PHI was exposed in the Data Breach on or about March 7, 2025.

17. Defendant is a limited liability company formed under the laws of Missouri, with its headquarters and principal place of business located at 155 Franklin Road, Suite 300, Brentwood, Tennessee, 37027.

III. JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant. Indeed,

Defendant and the named Plaintiffs here are diverse.

19. The Court has personal jurisdiction over Defendant because it is at home in this State.

20. Venue is proper in this District because Defendant's principal place of business is located in this District.

IV. BACKGROUND FACTUAL ALLEGATIONS

Defendant's Business

21. According to Defendant's website,

> Numotion is the nation's largest and leading provider of products and services to help individuals with mobility limitations maximize their health, personal independence, and actively participate in everyday life.[4]

22. Defendant has over 150 locations throughout the country, serves over 300,000 individual customers, and has more than 3,100 employees.5

23. As a condition of receiving products and services from Defendant, Plaintiffs and Class Members were required to entrust Defendant with their sensitive Private Information including names, dates of birth, Social Security numbers, medical equipment information, medical treatment and diagnosis information, and health insurance information, and did in fact turn over such Private Information to Defendant.

24. In exchange for receiving Plaintiffs' and Class Members' Private Information, Defendant promised to safeguard the sensitive, confidential data and to only it for authorized and legitimate purposes.

25. Thus, the data held by Defendant and accessed in the Data Breach included the

[4] https://www.numotion.com/about-us **(**last accessed Mar. 21, 2025).
[5] *Id.*

unencrypted Private Information of Plaintiffs and Class Members.

26. Defendant made promises to Plaintiffs and Class Members to adequately maintain and protect their Private Information, demonstrating its understanding of the importance of securing Private Information.

27. Defendant made promises and representations to its customers, including Plaintiffs and Class Members, that the Private Information it collected would be kept safe and confidential, the privacy of that information would be maintained, and Defendant would delete any sensitive information after it was no longer required to maintain it.

28. Indeed, Defendant's "Privacy Principles" published on its website promises as follows:

> **We are open and honest in how we use customer data.**
> We use data to offer and provide our customers products that enhance mobility and independence. Nothing more. Nothing less.
>
> **We collect only the data we need.**
> Our customers trust us with their most sensitive data at incredibly vulnerable moments in life. We are grateful for that trust and we will not abuse it.
>
> **We respect and protect our customers' data.**
> We understand that each of us alone gets to choose whom we share our data with. We take steps to protect customer data from unauthorized access or disclosure.[6]

29. Defendant's Notice of Privacy Practices published on its website further promises and warrants to its customer patients as follows, in part:

> We will share your health information within Numotion to carry out our treatment, payment, and health care operations. The law requires us to maintain the privacy of certain health information called "Protected Health Information" ("PHI"). PHI is the information that you provide us or that we create or receive about your health care. When we use or disclose (share) your PHI, we are required to follow the terms of this Notice or other notices in effect at the time we use

[6] https://www.numotion.com/about-us/privacy-principles (last accessed Mar. 21, 2025).

> or share the PHI. Finally, the law provides you with certain rights described in this Notice. Furthermore, we are required to notify you following a breach of unsecured PHI.
> . . .
> The information you provide us will/may be shared with other organizations directly related to providing the equipment you need, like hospitals and clinics.
> . . .
> For any purpose other than the ones described above, we may only use or share your PHI when you grant us your written permission (authorization).

30. None of the above permitted purposes for Defendant's disclosure of Private Information as set forth in the Notice of Privacy Practices include the disclosure to unknown and unauthorized cybercriminals as in the Data Breach.

31. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of its promises to safeguard that information, including in the manners set forth in Defendant's Privacy Principles web page and Notice of Privacy Practices.

32. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform the services it provides.

33. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties to Plaintiffs and Class Members, and knew or should have known that it was responsible for protecting their Private Information from unauthorized disclosure.

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

35. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiffs and Class Members relied on the

sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

Defendant Failed to Adequately Safeguard Plaintiffs' and Class Members' Private Information, resulting in the Data Breach.

36. Defendant collected and maintained its customers' and employees' Private Information in its computer information technology systems and networks.

37. The information held by Defendant at the time of the Data Breach included the unencrypted Private Information of Plaintiffs and Class Members.

38. On or about March 11, 2025, Defendant began sending Notice Letters notifying Plaintiffs and Class Members of the Data Breach.[7]

39. In the Notice Letters Defendant informed as follows:

> **What Happened?** Numotion recently learned that someone accessed certain employee email account without authorization on several occasions between September 2, 2024, and November 18, 2024. Numotion has no reasons to believe that anyone was trying to access personal information in the accounts, and there is no indication that any information has been used for fraud or identity theft. Nevertheless, out of an abundance of caution, Numotion undertook an extensive review of the emails that may have been accessed.[8]

40. Defendant's Notice Letter further acknowledges that its customers' sensitive Private Information was accessed in the Data Breach, including names and information of Plaintiffs and Class Members.[9]

41. Defendant did not use reasonable security procedures and practices appropriate to the sensitive and confidential nature of Plaintiffs' and Class Members' Private Information it

[7] *See* Ex. A.
[8] *Id.*
[9] *Id.*

collected and maintained, such as encrypting the information or deleting it when it is no longer needed, causing the theft of that Private Information in the Data Breach.

42. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiffs and Class Members.

43. As a result of Defendant's failures, Plaintiffs' and Class Members' Private Information was stolen in the Data Breach when criminal hackers accessed and acquired files in Defendant's computer systems containing that sensitive information in unencrypted form.

44. Defendant's tortious conduct and breach of contractual obligations, as detailed herein, are evidenced by its failure to recognize the Data Breach until cybercriminals had already accessed Plaintiffs' and Class Members' Private Information, meaning Defendant had no effective means in place to detect and prevent attempted cyberattacks.

45. Moreover, despite the Data Breach occurring on September 2, 2024, and November 18, 2024, and its investigation conducted on January 22, 2025, Defendant waited until March 7, 2025, to report the Data Breach to the U.S. Department of Health and Human Services Office for Civil Rights and other consumer agencies as required, stating that the Data Breach involved an hacking/IT incident affecting 494,326 persons and occurring between September 2, 2024, and November 18, 2024.[10]

Defendant Was on Notice of the Risk Cyber Attack because Defendant has Suffered a Previous Data Breach.

46. Defendant's negligence in failing to safeguard Plaintiffs' and Class Members' Private Information is exacerbated by its history of Data Breaches.

[10] *See* United Seating and Mobility's Data Breach Notification to the U.S. Dep't of Health & Human Servs., https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited May 22, 2025.

47. Defendant was on Notice because Defendant suffered a previous data breach between February 29, 2024, and March 2, 2024. At that time, an unknown, unauthorized criminal hacker accessed Defendant's network systems and exfiltrated customers and current and former employees of Defendant's Private Information stored therein, including their names, dates of birth, Social Security numbers, employment information medical equipment order details, supporting medical documentation, and health insurance information causing widespread injury and damages to affected individuals.

48. Although Defendant discovered their previous Data Breach on or about March 2, 2024, it failed to notify and warn affected individuals of the unauthorized disclosure of their Private Information until April 15, 2024, over six weeks later.

49. As such, Defendant is on Notice of the risk of cyber-attacks, its inadequate security system, and its requirement to timely notify affected individuals.

Defendant Knew or Should Have Known of the Risk of a Cyber Attack Because Healthcare Entities in Possession of Private Information Are Particularly Suspectable.

50. Defendant's negligence in failing to safeguard Plaintiffs' and Class Members' Private Information is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

51. Private Information of the kind accessed in the Data Breach is of great value to hackers and cybercriminals as it can be used for a variety of unlawful and nefarious purposes, including ransomware, fraudulent misuse, and sale on the Dark Web.

52. Private Information can also be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and financial records. This may be accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as his or her birthdate, birthplace, and mother's maiden

name.

53. Data thieves regularly target entities in the healthcare industry like Defendant due to the highly sensitive information that they maintain. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

54. Cyber-attacks against institutions such as Defendant are targeted and frequent. According to Contrast Security's 2023 report, "Cyber Bank Heists: Threats to the financial sector," "[o]ver the past year, attacks have included banking trojans, ransomware, account takeover, theft of client data and cybercrime cartels deploying 'trojanized' finance apps to deliver malware in spear-phishing campaigns."[11] In fact, "40% [of financial institutions] have been victimized by a ransomware attack."[12]

55. In light of recent high profile data breaches at other industry-leading companies, including, *e.g.*, 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), Defendant knew or, if acting as a reasonable healthcare provider and employer, should have known that the Private Information it collected and maintained would be targeted by cybercriminals.

56. According to the Identity Theft Resource Center's January 24, 2022 report for the year 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high

[11] Contrast Security, *Cyber Bank Heists: Threats to the financial sector*, pg. 5, https://www.contrastsecurity.com/hubfs/Cyber%20Bank%20Heists%20Report%202023.pdf (last accessed May 22, 2025).
[12] *Id.* at 15.

(1,506) set in 2017. The number of data events that involved sensitive information (Ex: Social Security numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)."[13]

57. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant itself. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[14]

58. Defendant's data security obligations were particularly important given the substantial increase, preceding the date of the subject Data Breach, in cyberattacks and/or data breaches targeting healthcare entities like Defendant that collect and store PHI and other sensitive information.

59. For example, of the 1,862 recorded data breaches in 2021, 330 of them, or 17.7%, were in the medical or healthcare industry.[15]

60. The 330 breaches reported 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.[16]

61. Entities in custody of PHI, like Defendant, reported the largest number of data breaches among all measured sectors in 2022, with the highest rate of exposure per breach.[17] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found the "average total cost to resolve

---

[13] *See* Identity Theft Res. Ctr., *2021 Annual Data Breach Report Sets New Record for Number of Compromises* (Jan. 24, 2022), https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises.

[14] IBM, *Cost of a data breach 2022: A million-dollar Race to Detect and Respond*, https://www.ibm.com/reports/data-breach (last accessed May 22, 2025).

[15] 2021 Data Breach Annual Report (Jan. 2022), https://notified.idtheftcenter.org/s/, at 6.

[16] *Id.*

[17] *See* Identity Theft Res. Ctr., *2022 Annual Data Breach Report*, https://www.idtheftcenter.org/publication/2022-data-breach-report/ (last accessed Mar. 21, 2024).

an identity theft-related incident . . . came to about $20,000," and that victims were often forced to pay out of pocket costs for healthcare they did not receive in order to restore coverage.[18] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. 40 percent of the patients were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impact the economy as a whole.[19]

62. Thus, the healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[20]

63. As indicated by Jim Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[21] A complete identity theft kit with health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[22]

64. As a healthcare entity in possession of its patient customers' Private Information,

---

[18] *See* Elinor Mills, *Study: Medical Identity Theft is Costly for Victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed Mar. 21, 2024).
[19] *Id.*
[20] SwivelSecure, *9 Reasons Why Healthcare is the Biggest Target for Cyberattacks*, https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks.
[21] IDExperts, *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows* (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.
[22] PriceWaterhouseCoopers, *Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security® Survey 2015*, https://docslib.org/doc/11817743/managing-cyber-risks-in-an-interconnected-world-key-findings-from-the-global-state-of-information-security%C2%AE-survey-2015.

Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class Members and of the foreseeable consequences if its data security systems were breached. Such consequences include the significant costs imposed on Plaintiffs and Class Members because of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

65. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being compromised.

66. Given the nature of the Data Breach, it was foreseeable that Plaintiffs' and Class Members' Private Information compromised therein would be targeted by hackers and cybercriminals for use in variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiffs' and Class Members' PII can easily obtain their tax returns or open fraudulent credit card accounts in Plaintiffs' and Class Members' names.

67. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to thousands of individuals' detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

68. Plaintiffs and Class Members were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing Private Information and the critical importance of providing adequate security for that information.

69. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiffs and Class Members especially vulnerable to

identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

Defendant Was Required but Failed to Comply with FTC Guidelines.

70. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

71. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses like Defendant. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[23]

72. The FTC's guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[24]

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

74. The FTC has brought enforcement actions against businesses for failing to

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

adequately and reasonably protect third parties' confidential 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 FTC Act. Orders resulting from these actions further clarify the measures business like Defendant must undertake to meet their data security obligations.

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

76. 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 businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

77. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[25]

78. Defendant failed to properly implement basic data security practices, in violation of its duties under the FTC Act.

[25] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf.

79. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

Defendant was Required but Failed to Comply with HIPAA Guidelines.

80. Defendant is covered businesses under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

81. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").13 See 42 U.S.C. §17921, 45 C.F.R. § 160.103.

82. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting PHI that is kept or transferred in electronic form.

83. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302. "Electronic protected health information" is "individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

84. HIPAA's Security Rule required and requires that Defendant do the following:

a. Ensure the confidentiality, integrity, and availability of all

electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

85. HIPAA also requires Defendant to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. §164.312(a)(1).

86. HIPAA and HITECH also obligate Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic PHI that are reasonably anticipated but not permitted by the privacy rules. See 45 C.F.R. §§ 164.306(a)(1), (a)(3); see also 42 U.S.C. §17902.

87. HIPAA further requires a covered entity like Defendant to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. See 45 C.F.R. § 164.530(e).

88. HIPAA further requires a covered entity like Defendant to mitigate, to the extent

practicable, any harmful effect that is known to the covered entity of a use or disclosure of PHI in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. See 45 C.F.R. § 164.530(f).

89. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. See 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.26 The list of resources includes a link to guidelines set by the National Institute of Standards and Technology ("NIST"), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.27

90. As alleged in this Complaint, Defendant failed to comply with HIPAA and HITECH. It failed to maintain adequate security practices, systems, and protocols to prevent data loss, failed to mitigate the risks of a data breach, and failed to ensure the confidentiality and protection of Plaintiffs' and Class Members' Private Information, including PHI.

Defendant Failed to Comply with Industry Standards.

91. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards.

---

[26] U.S. Dep't of Health & Human Servs., *Security Rule Guidance Material*, https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last accessed May 31, 2024).

[27] *Id.*

92. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including 18 Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[28]

93. In addition, the NIST recommends certain practices to safeguard systems,[29] *infra,* such as the following:

a. Control who logs on to your network and uses your computers and other devices;

b. Use security software to protect data;

c. Encrypt sensitive data, at rest and in transit;

d. Conduct regular backups of data;

e. Update security software regularly, automating those updates if possible;

f. Have formal policies for safely disposing of electronic files and old devices; and

[28] *See* Rapid7, *CIS Top 18 Critical Security Controls Solutions*, https://www.rapid7.com/solutions/compliance/critical-controls/ (last accessed May 31, 2024).
[29] Fed. Trade Comm'n, *Understanding the NIST Cybersecurity Framework*, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework (last accessed May 31, 2024).

g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

94. Further still, the Cybersecurity & Infrastructure Security Agency makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[30]

95. Defendant failed to meet the 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 (CIS

[30] Cybersecurity & Infrastructure Security Agency, *Shields Up: Guidance for Organizations*, https://www.cisa.gov/shields-guidance-organizations (last accessed Mar. 21, 2024).

CSC), which are all established standards in reasonable cybersecurity readiness.

Defendant Owed Plaintiffs and Class Members a Common Law Duty to Safeguard their Private Information.

96. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant's duty owed to Plaintiffs and Class Members obligated it to provide reasonable data security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected Plaintiffs' and Class Members' Private Information.

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

98. Defendant owed a duty to Plaintiffs and Class Members to implement processes that would detect a compromise of Private Information in a timely manner.

99. Defendant owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

100. Defendant owed a duty to Plaintiffs and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

101. Defendant owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

102. Defendant tortiously failed to take the necessary precautions required to safeguard and protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

Defendant's actions and omissions represent a flagrant disregard of Plaintiffs' and Class Members' rights.

Plaintiffs and Class Members Suffered Damages.

103. Defendant's failure to implement or maintain adequate data security measures for Plaintiffs and Class Members' Private Information directly and proximately caused injuries to Plaintiffs and Class Members by the resulting disclosure of their Private Information in the Data Breach.

104. Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiffs and Class Members significant injuries and harm in several ways. Plaintiffs and Class Members must immediately devote time, energy, and money to (a) closely monitor their medical statements, bills, records, and credit and financial accounts; (b) change login and password information on any sensitive account even more frequently than they already do; (c) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and (d) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

105. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen fraudulent use of that information and damage to victims may continue for years.

106. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendant's conduct which caused the Data Breach. Further, the value of Plaintiffs' and Class Members' Private Information has been diminished by

its exposure in the Data Breach.

107. As a result of Defendant's failures, Plaintiffs and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of Private Information.

108. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud–a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[31]

109. With respect to healthcare breaches, another study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[32]

110. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[33]

111. The reality is that cybercriminals seek nefarious outcomes from a data breach" and "stolen health data can be used to carry out a variety of crimes."[34]

112. Health information in particular is likely to be used in detrimental ways, including by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and

---

[31] Stu Sjourwerman, *28 Percent of Data Breaches Lead to Fraud*, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud.
[32] Heather Landi, *More than 70% of Hospital Data Breaches Compromise Information that Puts Patients at Risk of Identity Theft* (Sept. 23, 2019), https://www.fiercehealthcare.com/tech/more-than-70-hospital-data-breaches-expose-sensitive-information-putting-patients-at-risk.
[33] *Id.*
[34] Andrew Steger, *What Happens to Stolen Healthcare Data* (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

serious and long-term identity theft.[35]

113. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[36]

114. Plaintiffs and Class Members are also at a continued risk because their Private remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its patients' Private Information.

V. PLAINTIFFS' EXPERIENCES

Plaintiff Jennifer Sylvester

115. Plaintiff Sylvester is a former customer of Defendant. To obtain the medical device products sold by Defendant, she was required to provide Defendant with her Private Information.

116. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff's Private Information in its system.

117. Plaintiff Sylvester is very careful about sharing her sensitive Private Information. She stores any documents containing her Private Information in a safe and secure location and has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

118. Plaintiff Sylvester learned of the Data Breach after reviewing the Notice Letter from Defendant. According to the Notice Letter, Plaintiff's Private Information was improperly

[35] *Id.*
[36] Experian, *Experian® Data Breach Response Guide*, https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

accessed and obtained by unauthorized third parties in the Data Breach. The stolen Private Information comprised Plaintiff's personal information including name and medical information.

119. As a result of the Data Breach, Plaintiff Sylvester experienced two unauthorized attempts to take out a credit card in her name. As a result, Plaintiff Sylvester had to call each Bank that authorized the card to be issued and cancel them. Further, as a result of the Data Breach Plaintiff Sylvester obtained a credit freeze.

120. As a result of the Data Breach, Plaintiff Sylvester made reasonable efforts to mitigate the impact of the Data Breach, including expending time to check her bills and accounts to make sure they were correct, which time she would not have been required to spend on such tasks but for the Data Breach. Plaintiff has spent significant time dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

121. As a result of the Data Breach, Plaintiff Sylvester fears for her personal financial security and uncertainty over what medical information was revealed in the Data Breach. She is experiencing feelings of anxiety, sleep disruption, stress, and fear 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 is contemplated and addressed by law.

122. As a result of the Data Breach, Plaintiff Sylvester anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

123. As a result of Defendant's inadequate data security practices and the resulting Data Breach, Plaintiff Sylvester faces a present and continuing risk of identity theft for her lifetime.

124. Plaintiff Sylvester has a continuing interest in ensuring that her Private Information,

which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future cyberattacks.

Plaintiff Jason Peffley

125. Plaintiff Peffley is and was Defendant's patient at all times relevant to this Complaint. Plaintiff Peffley received a Notice of Data Breach Letter, related to Defendant's Data Breach, dated March 7, 2025. See Exhibit A.

126. The Notice Letter that Plaintiff received does not explain exactly which parts of his PII and PHI were accessed and taken but instead generically states that the files contained his name, "date of birth, dates of service, medical record number, patient account number, medical treatment/diagnosis information, and health insurance policy number."

127. Plaintiff Peffley is especially alarmed by the vagueness in the Notice Letter regarding his stolen extremely private medical information, including his PII/PHI, as among the breached data on Defendant's computer system.

128. Since the Data Breach, Plaintiff Peffley has tried to mitigate the damage by changing his passwords, contacting the credit bureaus as Defendant instructed, and monitoring his financial accounts for about 2 and a half hours per week. This is more time than she spent prior to learning of the Defendant's Data Breach. Having to do this every week not only wastes his time as a result of Defendant's negligence, but it also causes him great anxiety.

129. Soon after the Data Breach, Plaintiff Peffley began receiving an excessive number of spam calls on the same cell phone number provided to Defendant on his records. These calls are a distraction, must be deleted, and waste time each day. Given the timing of the Data Breach, she believes that the calls are related to his stolen PII/PHI.

130. Plaintiff Peffley is aware that cybercriminals often sell Private Information, and

once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

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

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

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

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

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

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

Plaintiff James Forsythe

137. Plaintiff Forsythe is a former customer of Defendant. To obtain the medical device products sold by Defendant, she was required to provide Defendant with his Private Information.

138. Upon information and belief, at the time of the Data Breach, Defendant retained

Plaintiff's Private Information in its system.

139. Plaintiff Forsythe is very careful about sharing his sensitive Private Information. He stores any documents containing his Private Information in a safe and secure location and has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

140. Plaintiff Forsythe learned of the Data Breach after reviewing the Notice Letter from Defendant. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties in the Data Breach. The stolen Private Information comprised Plaintiff's personal information including name and medical information.

141. As a result of the Data Breach, Plaintiff Forsythe made reasonable efforts to mitigate the impact of the Data Breach, including expending time to check his bills and accounts to make sure they were correct, which time she would not have been required to spend on such tasks but for the Data Breach. Plaintiff has spent significant time dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

142. As a result of the Data Breach, Plaintiff Forsythe fears for his personal financial security and uncertainty over what medical information was revealed in the Data Breach. He is experiencing feelings of anxiety, sleep disruption, stress, and fear 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 is contemplated and addressed by law.

143. As a result of the Data Breach, Plaintiff Forsythe anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

144. As a result of Defendant's inadequate data security practices and the resulting Data Breach, Plaintiff Forsythe faces a present and continuing risk of identity theft for his lifetime.

145. Plaintiff Forsythe has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future cyberattacks.

VI. COMMON INJURIES AND DAMAGES

146. As the direct and proximate result of Defendant's ineffective and inadequate data security practices and the resulting Data Breach, Plaintiffs and Class Members now face a present and ongoing risk of fraud and identity theft.

147. Due to the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including but not limited to: (a) invasion of privacy; (b) out of pocket costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) out of pocket costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) diminution of value of their Private Information; and (i) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

The Risk of Identity Theft to Plaintiffs and Class Members is Present and Ongoing

148. The link between a data breach and the risk of identity theft is simple and well

established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

149. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or to track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

150. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

151. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[37] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[38] This prevents dark web

[37] Experian, *What Is the Dark Web?*, https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[38] *Id.*

marketplaces from being easily monitored by authorities or accessed by those not in the know.

152. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the Private Information at issue here.[39] The digital character of Private Information stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[40] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[41]

153. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity

[39] Experian, *What is the Dark Web?* – Microsoft 365, https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.
[40] *Id.*; Experian, *What Is the Dark Web?*, https://www.experian.com/blogs/ask-experian/what-is-the-dark-web.
[41] Experian, *What is the Dark Web?* – Microsoft 365, https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

can cause a lot of problems.[42]

154. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

155. Even then, new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[43]

156. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[44]

157. Theft of PHI, in particular, is gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider,

---

[42] Social Sec. Admin., *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf.

[43] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[44] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf.

or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[45]

158. One such example of criminals using Private Information for profit is the development of "Fullz" packages. Cyber-criminals can cross-reference two sources of Private 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.

159. The development of "Fullz" packages means that stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' 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 Private 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 Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and Class Members' stolen Private Information is being misused, and that such misuse is traceable to the Data Breach.

160. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[46]

161. Further, according to the same report, "rapid reporting can help law enforcement

[45] *See* Fed. Trade Comm'n, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.
[46] *See* Fed. Bureau of Investigations, *2019 Internet Crime Report Released* (Feb. 11, 2020), https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.

stop fraudulent transactions before a victim loses the money for good."[47] Defendant did not rapidly report to Plaintiffs and the Class that their Private Information had been stolen.

162. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

163. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their Private Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

164. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Private Information. To protect themselves, Plaintiffs and Class Members will need to remain vigilant against unauthorized data use for years or even decades to come.

Loss of Time to Mitigate the Risk of Identify Theft and Fraud

165. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm–yet the asset of time has been lost.

[47] *Id.*

166. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

167. In the event that Plaintiffs and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[48] Indeed, the FTC recommends that identity theft victims take several steps and spend time to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[49]

Diminution of Value of the Private Information

168. Private Information is a valuable property right.[50] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

---

[48] *See* U.S. Gov't Accountability Off., *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, p. 2 (June 2007), https://www.gao.gov/new.items/d07737.pdf ("GAO Report").

[49] *See* Fed. Trade Comm'n, *Steps*, https://www.identitytheft.gov/Steps.

[50] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

169. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase Private Information on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

170. Private Information can sell for as much as $363 per record according to the Infosec Institute.[51]

171. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, medical data was selling on the dark web for $50 and up.[52]

172. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[53] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[54, 55] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[56]

173. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and

---

[51] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market.
[52] *Ransomware Attacks Paralyze and Sometimes Crush Hospitals* (Oct. 3, 2019), https://news.sophos.com/en-us/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals.
[53] David Lazarus, *Shadowy Data Brokers Make the Most of Their Invisibility Cloak*, L.A. TIMES (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.
[54] https://datacoup.com/.
[55] https://digi.me/what-is-digime/.
[56] Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

diminished in its value by its unauthorized and potential release onto the Dark Web, where it may soon be available and holds significant value for the threat actors.

Future Cost of Credit and Identify Theft Monitoring is Reasonable and Necessary

174. To date, Defendant has done little to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the Data Breach.

175. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes–e.g., opening bank accounts in the victims' names to make purchases or to launder money; filing false tax returns; taking out loans or lines of credit; or filing false unemployment claims.

176. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that her or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

177. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[57] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change

[57] *See* Jesse Damiani, *Your Social Security Number Costs $4 On the Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

(such as Social Security numbers).

178. Consequently, Plaintiffs and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

179. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

Loss of Benefit of the Bargain

180. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain.

181. When agreeing to provide their Private Information, which was a condition precedent to obtain products and services from Defendant, and paying Defendant, directly or indirectly, for its services, Plaintiffs and Class Members, as consumers, understood and expected that they were, in part, paying for services and data security to protect the Private Information required to be collected by Defendant.

182. In fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains struck with Defendant.

Lack of Compensation

183. Defendant's Notice Letter fails to sufficiently compensate victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and it entirely fails to provide any compensation for their unauthorized release and disclosure of Plaintiffs' and Class Members'

Private Information, out of pocket costs, and the time they are required to spend attempting to mitigate their injuries.

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

185. As a direct and proximate result of Defendant's conduct, Plaintiffs sand Class Members have been placed at an actual, imminent, and substantial risk of harm from fraud and identity theft.

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

187. Specifically, many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

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

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

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

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

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

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

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

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

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

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

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

Injunctive Relief is Necessary to Protect Against Future Data Breaches

190. Moreover, Plaintiffs and Class Members have an interest in ensuring that Private Information, which is believed to remain in the possession of Defendant, 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 Private Information is not accessible online and that access to such data is password protected.

191. Because of Defendant's failure to prevent the Data Breach, Plaintiffs and Class Members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses and lost time. Also, they suffered or are at a materially increased risk of imminently suffering

a. loss of the opportunity to control how their Private Information is used;

b. diminution in value of their Private Information;

c. compromise and continuing publication of their Private Information;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen Private Information; and

h. continued risk to their Private Information, which remains in Defendant's possession and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect it.

VII. CLASS ALLEGATIONS

192. Plaintiffs bring this nationwide class action individually and on behalf of all other persons similarly situated (the "Class") pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3).

193. Plaintiffs' propose the following Class definition, subject to amendment based on information obtained through discovery:

> **All individuals whose Private Information was compromised in the Data Breach beginning on or about September 2, 2024, including all persons who received the Notice Letter from Defendant.**

194. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

195. Plaintiffs reserve the right to amend the definition of the Class or add a class or subclass if further information and discovery indicate that the definition of the Class should be narrowed, expanded, or otherwise modified.

196. Certification of Plaintiffs' claim for class-wide treatment is appropriate because Plaintiffs can prove the elements of Class Members' claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims for each Class Member.

197. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Tenn. R. Civ. P. 23.01(1)-(4):.

198. **Numerosity:** The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Private Information of approximately 494,326 customers of Defendant was compromised in the Data Breach. Such information is readily ascertainable from Defendant's records.

199. **Commonality:** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b. 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;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, the FTC Act and HIPAA;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether hackers obtained Plaintiffs' and Class Members' Private Information in the Data Breach;

f. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

g. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

h. Whether Defendant breached the covenant of good faith and fair dealing implied in its contracts with Plaintiffs and Class Members; and

i. Whether Plaintiffs and the Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

200. **Typicality:** The claims or defenses of Plaintiffs are typical of the claims or defenses of the proposed Class because Plaintiffs' claims are based upon the same legal theories and same violations of law. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

201. This lawsuit presents no difficulties that would impede its management by the

Court as a class action. The class certification issues can be easily determined because the Class includes only Defendant's employees, the legal and factual issues are narrow and easily defined, and the Class Membership is limited. The Class does not contain so many persons that would make the Class notice procedures unworkable or overly expensive. The identity of the Class Members can be identified from Defendant's records, such that direct notice to the Class Members would be appropriate.

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

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

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

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

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

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

e. Whether Defendant failed to take commercially reasonable steps to safeguard customers' and employees' Private Information; and

f. Whether adherence to FTC data security recommendations, and measures

recommended by data security experts would have reasonably prevented the Data Breach.

204. Further, this action satisfies Tenn. R. Civ. P. 23.02 because: (i) common questions of law and fact predominate over any individualized questions; (ii) prosecuting individual actions would create a risk of inconsistent or varying adjudications, risking incompatible standards of conduct for Defendant, and a risk adjudications with respect to individual members of the Class which would as a practical matter be dispositive of the interests of the other members not parties to the adjudications or would substantially impair or impede their ability to protect their interest; and (iii) the Defendant have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

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

CAUSES OF ACTION
COUNT I: NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

206. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

207. Defendant required Plaintiffs and Class Members to submit private, confidential Private Information to Defendant as a condition of receiving products and services from Defendant.

208. Plaintiffs and Class Members provided certain Private Information to Defendant including their names, Social Security numbers, dates of birth, medical equipment information, medical diagnosis and treatment information, health insurance information, and other personal

information.

209. Defendant had full knowledge of the sensitivity of the Private Information to which it was entrusted, and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information was wrongfully disclosed to unauthorized persons. Defendant had a duty to Plaintiffs and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that Private Information.

210. Plaintiffs and Class Members were the foreseeable victims of any inadequate safety and security practices by Defendant.

211. Plaintiffs and the Class Members had no ability to protect their Private Information in Defendant's possession.

212. By collecting and storing Plaintiffs' and Class Members' Private Information in its computer systems, Defendant had a duty of care to use reasonable means to secure and safeguard it, to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect if that Private Information was exposed to the internet and to give prompt notice to those affected in the case of a data breach.

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

214. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customers and/or its employees, which is recognized by laws and regulations including but not limited to the FTC Act, as well as

the common law. Defendant was able to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs and Class Members from a data breach.

215. In addition, Defendant had a duty to employ reasonable security measures under 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, the unfair practice of failing to use reasonable measures to protect confidential data.

216. Defendant's duty to use reasonable care in protecting Plaintiffs' and Class Members' confidential Private Information in its possession arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to such Private Information.

217. Defendant's duty also arose from its position as a healthcare provider. Defendant holds itself out as a trusted provider of healthcare, and thereby assumes a duty to reasonably protect its patients' information. Indeed, Defendant, as a healthcare provider, was in a unique and superior position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

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

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

219.

b. Failing to adequately train employees on proper cybersecurity protocols;

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

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

e. Allowing unauthorized access to Plaintiffs' and Class Members' Private Information;

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

220. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their Private Information would not have been compromised.

221. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiffs' and Class Members' Private Information would result in injury to Plaintiffs and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyber-attacks and data breaches in the industry.

222. The breach was foreseeable due to Defendant's history of data breaches.

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

224. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (d) loss of benefit of the bargain; and (e) the continued and certainly increased risk to their Private Information, which (i) remains unencrypted and available for unauthorized third

parties to access and abuse; and (ii) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

225. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

226. Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

227. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) continue to provide adequate credit monitoring to all Class Members.

COUNT II: NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Class)

228. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

229. 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 Plaintiffs' and Class Members' Private Information.

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

231. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI it 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.

232. Defendant breached its duties to Plaintiffs and Class Members under the FTC Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

233. The injuries to Plaintiffs and Class Members resulting from the Data Breach were directly and indirectly caused by Defendant's violation of the statutes described herein.

234. Plaintiffs and Class Members are within the class of persons the FTC Act and HIPAA were intended to protect.

235. The type of harm that resulted from the Data Breach was the type of harm the FTC Act and HIPAA were intended to guard against.

236. Defendant's failure to comply with the FTC Act and HIPAA and regulations constitutes negligence *per se.*

237. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

238. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will suffer injuries, including but not limited to (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (d) loss of benefit of the bargain; and (e) the continued and certainly increased risk to their Private Information, which (i) remains unencrypted and available for unauthorized third parties to access and abuse; and (ii) remains in Defendant's possession and is

subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

239. Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

240. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) continue to provide adequate credit monitoring to all Class Members.

COUNT III: BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

241. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

242. Defendant required Plaintiffs and Class Members to provide and entrust their Private Information as a condition of obtaining products and services from Defendant.

243. When Plaintiffs and Class Members provided their Private Information to Defendant, they entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such Private Information and to timely and accurately notify Plaintiffs and Class Members if and when their Private Information was breached and compromised.

244. Specifically, Plaintiffs and Class Members entered into valid and enforceable implied contracts with Defendant when they agreed to provide their Private Information to Defendant.

245. The valid and enforceable implied contracts that Plaintiffs and Class Members entered into with Defendant included Defendant's promise to protect Private Information it collected from Plaintiffs and Class Members, or created on its own, from unauthorized disclosures.

Plaintiffs and Class Members provided this Private Information in reliance on Defendant's promise.

246. Under the implied contracts, Defendant promised and was obligated to (a) provide products and services to Plaintiffs and Class Members; and (b) protect Plaintiffs' and Class Members' Private Information (i) provided to obtain such services and/or (ii) created in connection therewith. In exchange, Plaintiffs and Class Members agreed to provide Defendant payment and their Private Information.

247. The provision of payment and the protection of Plaintiffs' and Class Members' Private Information were material aspects of these implied contracts with Defendant.

248. Defendant's implied contracts for employment—contracts that include the contractual obligations to maintain the privacy of Plaintiffs' and Class Members' Private Information—are also acknowledged, memorialized, and embodied in multiple documents, including Defendant's Notice of Privacy Practices as described *supra*.

249. Defendant solicited and invited Plaintiffs and Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

250. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with industry standards and relevant laws and regulations, including the FTC Act.

251. Plaintiffs and Class Members who partnered or contracted with Defendant for products and services and who provided their Private Information to Defendant, reasonably believed and expected that Defendant would adequately employ adequate data security to protect that Private Information. Defendant failed to do so.

252. A meeting of the minds occurred when Plaintiffs and the Class Members agreed to, and did, provide their Private Information to Defendant and agreed Defendant would receive payment for, amongst other things, the protection of their Private Information.

253. Plaintiffs and Class Members performed their obligations under the contracts when they agreed Defendant would receive payment and provided their Private Information to Defendant.

254. Defendant materially breached its contractual obligations to protect the Private Information it required Plaintiffs and Class Members to provide and when that Private Information was unauthorizedly disclosed in the Data Breach.

255. Defendant materially breached its contractual obligations to deal fairly and in good faith with Plaintiffs and Class Members when it failed to take adequate precautions to prevent the Data Breach and failed to promptly notify them of the Data Breach.

256. Defendant materially breached the terms of its implied contracts, including, but not limited to, by failing to comply with industry standards or the standards of conduct embodied in statutes like Section 5 of the FTC Act, or by failing to otherwise protect Plaintiffs' and Class Members' Private Information, as set forth *supra*.

257. The Data Breach was a reasonably foreseeable consequence of Defendant's conduct, by acts of omission or commission, in breach of these implied contracts with Plaintiffs and Class Members.

258. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiffs and Class Members did not receive the full benefit of their bargains with Defendant, and instead received products and services of a diminished value compared to that described in the implied contracts. Plaintiffs and Class Members were therefore damaged in an

amount at least equal to the difference in the value of the services with data security protection they paid for and that which they received.

259. Had Defendant disclosed that its data security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, the Class Members, nor any reasonable person would have contracted with Defendant.

260. Plaintiffs and Class Members would not have provided and entrusted their Private Information to Defendant in the absence of the implied contracts between them and Defendant.

261. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

262. Defendant breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect their Private Information and by failing to provide timely or adequate notice that their Private Information was compromised in and as a result of the Data Breach.

263. As a direct and proximate result of Defendant's breach of its implied contracts with Plaintiffs and Class Members and the attendant Data Breach, Plaintiffs and Class Members have suffered injuries and damages as set forth herein and have been irreparably harmed, as well as suffering and the loss of the benefit of the bargain they struck with Defendant.

264. Plaintiffs and Class Members, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

265. Plaintiffs and the Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) immediately provide

adequate credit monitoring to all Class Members.

COUNT IV: BREACH OF CONFIDENCE
(On Behalf of Plaintiffs and the Class)

266. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

267. At all times during Plaintiffs' and Class Members' interactions with Defendant and/or its agents, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' Private Information it collected and maintained.

268. Defendant's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs' and Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized parties.

269. Plaintiffs and Class Members provided their Private Information to Defendant and/or its agents with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized parties.

270. Plaintiffs and Class Members also provided their Private Information to Defendant and/or its agents with the explicit and implicit understandings that Defendant would take precautions to protect such Private Information from unauthorized disclosure.

271. Defendant voluntarily received in confidence Plaintiffs' and Class Members' Private Information with the understanding that the Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

272. Due to Defendant's failure to prevent, detect, or avoid the Data Breach from occurring by, *inter alia*, following industry standard information security practices to secure Plaintiffs' and Class Members' Private Information, Plaintiffs' and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs'

and Class Members' confidence, and without their express permission.

273. But for Defendant's disclosure of Plaintiffs' and Class Members' Private Information in violation of the parties' understanding of confidence, their sensitive and confidential Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' Private Information, as well as their resulting damages.

274. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will suffer injuries, including but not limited to (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (d) loss of benefit of the bargain; and (e) the continued and certainly increased risk to their Private Information, which (i) remains unencrypted and available for unauthorized third parties to access and abuse; and (ii) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

275. The injuries and harm Plaintiffs and Class Members suffered were the reasonably foreseeable result of Defendant's breach of confidence and unauthorized disclosure of Plaintiffs' and Class Members' Private Information.

276. Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

277. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) continue to provide

adequate credit monitoring to all Class Members.

COUNT V: UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

278. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

279. This claim is pleaded in the alternative to the claim of breach of implied contract (Count III).

280. Plaintiffs and Class Members conferred direct benefits upon Defendant in the form of agreeing to provide their Private Information to Defendant, without which Defendant could not perform the services it provides or pay its employees.

281. Defendant appreciated or knew of these benefits it received from Plaintiffs and Class Members. Under principles of equity and good conscience, Defendant should not be allowed to retain the full value of these benefits—specifically, the costs it saved by failing to implement reasonable or adequate data security practices with respect to the Private Information it collected from Plaintiffs and Class Members.

282. After all, Defendant failed to adequately protect Plaintiffs' and Class Members' Private Information. And if such inadequacies were known, then Plaintiffs and Class Members would never have agreed to provide their Private Information, or payment or labor, to Defendant.

283. Defendant should be compelled to disgorge into a common fund, for the benefit of Plaintiffs and the Class, all funds that were unlawfully or inequitably gained despite Defendant's misconduct and the resulting Data Breach.

COUNT VI: INVASION OF PRIVACY/INTRUSION UPON SECLUSION
(On Behalf of Plaintiffs and the Class)

284. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

285. Plaintiffs and Class Members had a legitimate expectation of privacy to their Private Information and were entitled to Defendant's protection of this Private Information in its possession against disclosure to unauthorized third parties.

286. Defendant owed a duty to its customers and employees, including Plaintiffs and Class Members, to keep their Private Information confidential and secure.

287. Defendant failed to protect Plaintiffs' and Class Members' Private Information and instead, exposed it to unauthorized persons which is now publicly available, including on the dark web, and being fraudulently misused.

288. Defendant allowed unauthorized third parties access to and examination of the Private Information of Plaintiffs and Class Members, by way of Defendant's failure to protect the Private Information.

289. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiffs and Class Members is highly offensive to a reasonable person.

290. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and Class Members disclosed their Private Information to Defendant as a condition of receiving products and services, but privately with an intention that the Private Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

291. The Data Breach constitutes an intentional or reckless interference by Defendant with Plaintiffs' and Class Members' interests in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable

person.

292. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it had actual knowledge that its information security practices were inadequate and insufficient.

293. Defendant acted with reckless disregard for Plaintiffs' and Class Members' privacy when it allowed improper access to its systems containing Plaintiffs' and Class Members' Private Information without protecting said data from the unauthorized disclosure, or even encrypting such information.

294. Defendant was aware of the potential of a data breach and failed to adequately safeguard its systems and implement appropriate policies to prevent the unauthorized release of Plaintiffs' and Class Members' Private Information.

295. Because Defendant acted with this knowing state of mind, it had notice and knew of the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and Class Members.

296. Indeed, the definition of intent is met here under Section 8A of the Restatement (Second) of Torts because, given the ubiquity of data breaches, Defendant was substantially certain that its decision to forego investments in reasonable cybersecurity would result in a data breach.

297. As a direct and proximate result of Defendant's acts and omissions set forth above, Plaintiffs' and Class Members' Private Information was disclosed to third parties without authorization, causing Plaintiffs and Class Members to suffer injuries and damages as set forth herein, including, without limitation, (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (d) loss of benefit of the

bargain; and (e) the continued and certainly increased risk to their Private Information, which (i) remains unencrypted and available for unauthorized third parties to access and abuse; and (ii) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

298. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the Private Information maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and Class Members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, pray for judgment as follows:

A. An Order certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

B. Awarding Plaintiffs and the Class damages that include applicable compensatory, actual, exemplary, and punitive damages, as allowed by law;

C. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

D. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

E. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

F. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the transmitted Private Information;

G. Awarding attorneys' fees and costs, as allowed by law,

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Any and all such relief to which Plaintiffs and the Class are entitled.

JURY TRIAL DEMAND

Plaintiffs hereby demand a trial by jury of all issues so triable.

Dated: June 18, 2025

Respectfully submitted.

/s/ J. Gerard Stranch, IV

J. Gerard Stranch, IV (BPR 23045)
Grayson Wells (BPR 039658)
Miles Schiller (BPR 041531)
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Ave., Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gstranch@stranchlaw.com
gwells@stranchlaw.com
mschiller@stranchlaw.com

Jeff Ostrow*
Kenneth J. Grunfeld*
KOPELOWITZ OSTROW P.A.
1 W. Las Olas Blvd., Suite 500
Fort Lauderdale, FL 33301
Tel: (954) 525-4100
ostrow@kolawyers.com
grunfeld@kolawyers.com

Liberato P. Verderame*
Marc H. Edelson*
EDELSON LECHTZIN LLP
411 S. State Street, Suite N300
Newtown, PA 18940

Tel: (215) 867-2399
medelson@edelson-law.com
lverderame@edelson-law.com

Andrew J. Shamis*
SHAMIS & GENTILE, P.A.
14 NE 1st Ave, Suite 705
Miami, FL 33132
Tel: (305) 479-2299
ashamis@shamisgentile.com

Pro hac vice forthcoming

Counsel for Plaintiffs and the Putative Class

CERTIFICATE OF SERVICE

I hereby certify that the foregoing Consolidated Class Action Complaint was filed and served via the court's CM/ECF electronic filing system on this 18th day of June 2025 upon following:

Casie D. Collignon
Keeley O. Cronin
BAKER & HOSTETTLER, LLP
1801 California Street
Suite 4400
Denver, CO 80202
ccollignon@bakerlaw.com
kcronin@bakerlaw.com

E. Todd Presnell
Kimberly Michelle Ingram-Hogan
BRADLEY ARANT BOULT CUMMINGS, LLP
1221 Broadway
Suite 2400
Nashville, TN 372203
tpresnell@bradley.com
kingram@bradley.com

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

June 28, 2024

EXHIBIT A

JAMES FORSYTHE

[redacted]

RE: NOTICE OF DATA BREACH

Dear James Forsythe:

Numotion values and respects the privacy of your information, which is why we are writing to advise you of a recent incident that may have involved some of your protected health information. This letter explains the incident, the steps we have taken in response, and provides information on steps you may take to help protect your information, should you feel it is appropriate to do so.

What Happened? On March 2, 2024, we discovered that we were the victim of a cyber-attack. Upon learning of the incident, we promptly began an investigation and worked to secure our systems. We also engaged a forensic security firm to assist with our investigation and confirm the security of our computer systems. The forensic investigation determined that an unknown, unauthorized third party accessed our computer systems between February 29, 2024, and March 2, 2024, and encrypted some of our computer files. The investigation also determined that the third party may have accessed and acquired certain files from our systems during this period.

What Information Was Involved? We have been reviewing the contents of the potentially acquired files to determine if they contain any protected health information and are notifying individuals on a rolling basis. We recently determined that the files contained protected health information that may have included your name, date of birth, Social Security number, equipment order details, supporting medical documentation and medical insurance information.

What We Are Doing. In addition to the actions described above, we have also taken steps to reduce the risk of this type of incident occurring in the future, including enhancing our technical security measures. We are also notifying you of the incident so that you can be aware and take steps to protect your information, if you feel it is appropriate to do so. Finally, although we are not aware of any instances of fraud or identity theft resulting from this incident, out of an abundance of caution, we are offering a complimentary one-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on prompt identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary, one-year membership, please see the additional information attached to this letter.**

What You Can Do. While we have no evidence that your protected health information has been misused, we encourage you to take advantage of the complimentary credit monitoring included in this letter. You can also find more information on steps to protect yourself against possible identity theft or fraud in the enclosed *Additional Important Information* page.

For More Information. We value the trust you place in Numotion with your privacy, and take our responsibility to safeguard protected health information seriously, and apologize for any inconvenience this incident might cause. For further information and assistance, please call 866-528-8846 from 8:00 AM to 5:30 PM Central Time, Monday through Friday.

EXHIBIT B

numotion
Mobility and independence start here.®

185 1 62115 ——————AUTO**ALL FOR AADC 535
JENNIFER SYLVESTER
[redacted]
, WI 53821-8496

March 11, 2025

Dear Jennifer Sylvester:

Numotion values and respects the privacy of your information, which is why we are writing to advise you of a recent incident that may have involved some of your personal information. We have no reason to believe that your information has been misused. Nonetheless, we are writing to advise you about the incident and to provide you with guidance on what you can do to protect yourself, should you feel it is appropriate to do so.

What Happened? Numotion recently learned that someone accessed certain employee email accounts without authorization on several occasions between September 2, 2024, and November 18, 2024. Numotion has no reason to believe that anyone was trying to access personal information in the accounts, and there is no indication that any information has been used for fraud or identity theft. Nevertheless, out of an abundance of caution, Numotion undertook an extensive review of the emails that may have been accessed.

What Information Was Involved? On January 22, 2025, we determined that the email accounts contained some of your personal information, including your name, in combination with one or more of the following: medical information.

What We Are Doing. In addition to the actions described above, we have also taken steps to reduce the risk of this type of incident occurring in the future, including enhancing our technical security measures. We are also notifying you of the incident so that you can be aware and take steps to protect your information, if you feel it is appropriate to do so.

What You Can Do. While we have no evidence that your personal information has been misused, we encourage you review the enclosed Additional Important Information page for steps to protect yourself against possible identity thef fraud.

For More Information. We value the trust you place in us to protect your privacy, take our responsibility to safeguard y personal information seriously, and apologize for any inconvenience this incident might cause. For further informa and assistance, please call (866) 450-2357 from 8 a.m. until 5:30 p.m. Central Time, Monday through Friday, exclu major U.S. holidays.

Sincerely,

Numotion

62115

EXHIBIT C

numotion
Mobility and independence start here.

March 7, 2025

278 1 87915 ********** AUTO**ALL FOR AADC 920
JASON A PEFFLEY
[redacted]

Dear Jason Peffley:

Numotion values and respects the privacy of your information, which is why we are writing to advise you of a recent incident that may have involved some of your personal information. We have no reason to believe that your information has been misused. Nonetheless, we are writing to advise you about the incident and to provide you with guidance on what you can do to protect yourself, should you feel it is appropriate to do so.

What Happened? Numotion recently learned that someone accessed certain employee email accounts without authorization on several occasions between September 2, 2024, and November 18, 2024. Numotion has no reason to believe that anyone was trying to access personal information in the accounts, and there is no indication that any information has been used for fraud or identity theft. Nevertheless, out of an abundance of caution, Numotion undertook an extensive review of the emails that may have been accessed.

What Information Was Involved? On January 22, 2025, we determined that the email accounts contained some of your personal information, including your name, in combination with one or more of the following: medical information and health insurance policy name.

What We Are Doing. In addition to the actions described above, we have also taken steps to reduce the risk of this type of incident occurring in the future, including enhancing our technical security measures. We are also notifying you of the incident so that you can be aware and take steps to protect your information, if you feel it is appropriate to do so.

What You Can Do. While we have no evidence that your personal information has been misused, we encourage you to review the enclosed *Additional Important Information* page for steps to protect yourself against possible identity theft or fraud.

For More Information. We value the trust you place in us to protect your privacy, take our responsibility to safeguard your personal information seriously, and apologize for any inconvenience this incident might cause. For further information and assistance, please call (866) 450-2357 from 8 a.m. until 5:30 p.m. Central Time, Monday through Friday, excluding major U.S. holidays.

Sincerely,

Numotion

Credit Reports: By law, you may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies. The three national credit reporting agencies have also agreed to provide free weekly online credit reports. You can obtain your free credit report by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action. Alternatively, you may elect to purchase a copy of your credit report by contacting the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax 1-866-349-5191 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	Experian 1-888-397-3742 www.experian.com P.O. Box 2002 Allen, TX 75013	TransUnion 1-800-888-4213 www.transunion.com P.O. Box 1000 Chester, PA 19016

Fraud Alerts: By law, you have the right to place a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

District of Columbia Residents: District of Columbia residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at 441 4th Street, NW, Washington, DC 20001, 202-727-3400, oag@dc.gov, https://oag.dc.gov/.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, http://www.marylandattorneygeneral.gov/.

New Mexico Residents: Individuals have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; https://ag.ny.gov/consumer-frauds/identity-theft; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Oregon Residents: Oregon residents are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. Oregon residents can contact the Oregon Attorney General at 1162 Court St. NE, Salem, OR 97301-4096; 503-378-4400; https://www.doj.state.or.us/.

Rhode Island Residents: We believe that this incident affected 903 Rhode Island residents. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

You may place a security freeze on your credit reports. A security freeze can be placed without any charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies' online security freeze request procedures:

Equifax Security Freeze 1-888-298-0045 https://www.equifax.com/personal/credit-report-services/credit-freeze/ P.O. Box 105788 Atlanta, GA 30348	Experian Security Freeze 1-888-397-3742 https://www.experian.com/freeze/center.html P.O. Box 9554 Allen, TX 75013	TransUnion Security Freeze 1-800-916-8800 https://www.transunion.com/credit-freeze P.O. Box 160 Woodlyn, PA 19094

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail or, if available, comply with the consumer reporting agencies' online procedures for lifting a security freeze, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.