COMMONWEALTH OF MASSACHUSETTS

MIDDLESEX, ss.

SUPERIOR COURT
DEPARTMENT OF THE TRIAL COURT
CA. NO: 2481CV02873

WILLIAM MATIASEK, DIANE REMICK, DONNA PRUITT, KAREN PICARDI, and DIANA CERRONE on behalf of all others similarly situated,

Plaintiffs,

v.

MYSTIC VALLEY ELDER SERVICES, INC.,

Defendant.

CLASS ACTION
CONSOLIDATED COMPLAINT

In re Mystic Valley Elder Services, Inc.

CLASS ACTION CONSOLIDATED COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiffs William Matiasek, Diane Remick, Donna Pruitt, Karen Picardi, and Diana Cerrone ("Plaintiffs"), individually and on behalf of all others similarly situated, and on behalf of the general public, bring this Consolidated Class Action Complaint, against Defendant, Mystic Valley Elder Services, Inc. ("Mystic Valley Elder Services," "MVES," or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiffs allege the following based on personal knowledge and the investigation of counsel.

I. INTRODUCTION

1. With this action, Plaintiffs seek to hold Defendant responsible for the harms they caused Plaintiffs and similarly situated persons in the preventable data breach of Defendant's inadequately protected computer network.

2. Defendant provides care and services to seniors and individuals with disabilities.

3. As part of its business, Defendant obtained and stored the highly sensitive personal identifiable information ("PII") and protected health information ("PHI") of Plaintiffs and Class members.

4. By taking possession and control of Plaintiffs' and Class members' PII and PHI, Defendant assumed a duty to securely store and protect the Personal Information of Plaintiffs and the Class.

5. Defendant breached this duty and betrayed the trust of Plaintiffs and Class members by failing to properly safeguard and protect their PII and PHI, thus enabling cybercriminals to access, acquire, appropriate, compromise, disclose, encumber, exfiltrate, release, steal, misuse, and/or view it.

6. On April 5, 2024, unauthorized cybercriminals successfully infiltrated Defendant's computer network and likely "accessed and acquired certain files from [its] systems," including files containing the PII and PHI of Plaintiffs and Class Members (the "Data Breach").[1] According to the forensic investigation, the PII and PHI exposed during the Data Breach included, names, dates of birth, passport numbers, taxpayer identification numbers, financial account numbers, payment card numbers, online credentials, Social Security numbers, driver's license numbers, health insurance information, and medical information ("Personal Information").[2]

7. On October 22, 2024—or more than *six months after the Data Breach*—Defendant reported the incident to the authorities and began sending notices to individuals whose information was accessed in the Data Breach.[3]

[1] *See* MVES breach letter, available at: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/39b8a2d8-4720-4f85-9dd7-8929d9a7a168.html
[2] https://www.mves.org/data-privacy-incident/.
[3] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/39b8a2d8-4720-4f85-9dd7-8929d9a7a168.html

8. According to Defendant's public statements, the Personal Information of approximately 87,236 individuals was compromised in the Data Breach.[4]

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

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

11. Plaintiffs bring this class action lawsuit to hold Defendant responsible for its reckless failure to use statutorily required or reasonable industry cybersecurity measures to protect Class members' Personal Information.

12. Upon information and belief, Defendant breached its duties and obligations in one or more of the following ways: (1) failing to design or being negligent in the design, implementation, monitoring, and maintenance of reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiffs and Class Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the PII; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to

[4] *Id.*

mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack; and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

13. As a result of the Data Breach, Plaintiffs and Class members have already suffered damages. For example, now that their Personal Information has been released into the criminal cyber domains, Plaintiffs and Class members are at imminent and impending risk of identity theft. This risk will continue for the rest of their lives, as Plaintiffs and Class members are now forced to deal with the danger of identity thieves possessing and using their Personal Information.

14. Additionally, Plaintiffs and Class members have already lost time and money responding to and mitigating the impact of the Data Breach, which efforts are continuous and ongoing.

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

II. THE PARTIES

Plaintiffs

16. Plaintiff William Matiasek is a citizen and resident of Middlesex County, Massachusetts. Plaintiff Matiasek received Defendant's Data Breach Notice.

17. Plaintiff Diane Remick is a citizen and resident of Suffolk County, Massachusetts. Plaintiff Remick received Defendant's Data Breach Notice.

18. Plaintiff Donna Pruitt is a citizen and resident of Suffolk County, Massachusetts. Plaintiff Pruitt received Defendant's Data Breach Notice.

19. Plaintiff Karen Picardi is a citizen and resident of Middlesex County, Massachusetts. Plaintiff Pruitt received Defendant's Data Breach Notice.

20. Plaintiff Diana Cerrone is a citizen and resident of Suffolk County, Massachusetts. Plaintiff Cerrone received Defendant's Data Breach Notice.

Defendant Mystic Valley Elder Services

21. Defendant, Mystic Valley Elder Services, Inc., is a non-profit corporation formed under the laws of Massachusetts and with its principal place of business at 300 Commercial Street, #19, Malden, Massachusetts 02148.

III. JURISDICTION AND VENUE

22. This Court has personal jurisdiction over Defendant by virtue of its formation and operations in the Commonwealth at all times relevant hereto.

23. This Court has jurisdiction over the claims contained herein as they relate to Plaintiffs and the putative class because the claims for damages for Plaintiffs and all putative class members exceed fifty thousand dollars ($50,000.00).

24. Venue in this matter is proper as Plaintiff Matiasek resides in Middlesex County, Massachusetts. Further, Defendant's principal place of business is located in Middlesex County.

IV. FACTUAL ALLEGATIONS

A. Background

25. Defendant provides care and services to seniors and individuals with disabilities.

26. In order for individuals to obtain services from Defendant, Defendant requires current and prospective clients to provide Defendant with their highly sensitive personal and medical information, including but not limited to their full names, Social Security numbers, dates of birth, medical information including, but not limited to, patient account numbers, doctors' names, lab test details, patients' history, and other protected health information.

27. Current and former customers and patients of Defendant, such as Plaintiffs and Class members, made their Personal Information available to Defendant with the reasonable expectation that any entity with access to this information would keep that sensitive and personal information confidential and secure from illegal and unauthorized access. They similarly expected that, in the event of any unauthorized access, they would be provided with prompt and accurate notice.

28. This expectation was objectively reasonable and based on obligations imposed on Defendant by statute, regulations, industry custom, and standards of general due care.

29. By obtaining, collecting, and storing Plaintiffs' and Class Members' Personal Information, Defendant assumed legal and equitable duties and knew or should have known that they were thereafter responsible for protecting Plaintiffs' and Class Members' Personal Information from unauthorized disclosure.

30. Plaintiffs and Class Members relied on Defendant to keep their Personal Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

31. Unfortunately for Plaintiffs and Class members, Defendant failed to carry out its duty to safeguard sensitive Personal Information. Defendant failed to implement necessary data security safeguards. As a result, it failed to protect Plaintiffs and Class members from having their Personal Information accessed and stolen during the Data Breach.

B. The Data Breach and Defendant's Belated Notice

32. On April 5, 2024, Defendant identified unusual activity on certain systems within its computer network.[5] Following an investigation, which concluded on July 11, 2024, forensic

[5] *See* https://www.mves.org/data-privacy-incident/.

experts confirmed that cybercriminals infiltrated Defendant's insufficiently secured computer network, improperly "accessed MVES' computer systems," and potentially "acquired" sensitive files containing the personal information of Plaintiffs and Class members.[6]

33. According to Defendant, the Personal Information accessed by cybercriminals involved a wide variety of PII and PHI, names, dates of birth, passport numbers, taxpayer identification numbers, financial account numbers, payment card numbers, online credentials, Social Security numbers, driver's license numbers, health insurance information, and medical information.[7] In total, Defendant injured at least 87,236 persons—via the exposure of their Personal Information—in the Data Breach.[8]

34. Despite the breadth and sensitivity of the PII/PHI that was exposed, and the attendant consequences to customers and patients as a result of the exposure, Defendant failed to disclose the Data Breach or notify victims until October 22, 2024, more than six months after the breach was identified. This delay further exacerbated the harms to Plaintiffs and Class members.

35. Omitted from the notice were the details of the root cause of the Data Breach, why it took Defendant six months to notify affected clients of the Data Breach, the date Defendant identified that Personal Information had been accessed, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Personal Information remains protected.

36. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class members of the Data Breach's critical facts. Without

[6] *Id.*
[7] *Id.*
[8] *See* https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/39b8a2d8-4720-4f85-9dd7-8929d9a7a168.html.

these details, Plaintiffs' and Class members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

37. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and Class members, causing the exposure of Personal Information, such as encrypting the information or deleting it when it is no longer needed.

38. Based on the notice letter received by Plaintiffs, the type of cyberattack involved, and public news reports, it is plausible and likely that Plaintiffs' Personal Information was stolen in the Data Breach.

39. Upon information and belief, the unauthorized third-party cybercriminal gained access to the Personal Information and has engaged in (and will continue to engage in) misuse of the Personal Information, including marketing and selling Plaintiffs' and Class members' Personal Information on the dark web.

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

41. Upon information and belief, Defendant provides every patient with a HIPAA compliant disclosure form in which it represents that it will protect patients' Personal Information.

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

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

44. For example, as evidenced by the Data Breach's occurrence, the infiltrated network was not protected by sufficient multi-layer data security technologies or effective firewalls.

45. Similarly, based on the delayed discovery of the Data Breach, it is evident that the infiltrated network, that Defendant allowed to store Plaintiffs' Personal Information, did not have sufficiently effective endpoint detection.

46. Further, the fact that Personal Information was accessed in the Data Breach demonstrates that the Personal Information contained in the Defendant's network was not encrypted. Had the information been properly encrypted, the data thieves would have accessed only indecipherable data.

47. Plaintiffs and Class Members entrusted Defendant with sensitive and confidential information, including their Personal Information which includes information that is static, does not change, and can be used to commit a myriad of financial crimes.

48. The stolen Personal Information at issue has great value to the hackers, due to the large number of individuals affected and the fact that sensitive information was part of the data that was compromised.

C. Defendant's Many Failures Both Prior to and Following the Breach

49. Defendant collects and maintains vast quantities of Personal Information belonging to Plaintiffs and Class members as part of its normal operations. The Data Breach occurred as

direct, proximate, and foreseeable results of multiple failings on the part of Defendant.

50. First, Defendant inexcusably failed to implement reasonable security protections to safeguard its information systems and databases.

51. Second, Defendant failed to inform the public that its data security practices were deficient and inadequate. Had Plaintiffs and Class members been aware that Defendant did not have adequate safeguards in place to protect such sensitive Personal Information, they would have never provided such information to Defendant.

52. In addition to the failures that lead to the successful breach, Defendant's failings in handling the breach and responding to the incident exacerbated the resulting harm to the Plaintiffs and Class members.

53. Defendant's delay in informing victims of the Data Breach that their Personal Information was compromised virtually ensured that the cybercriminals who stole this Personal Information could monetize, misuse and/or disseminate that Personal Information before the Plaintiffs and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiffs and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

54. Additionally, Defendant's attempt to ameliorate the effects of this data breach with limited complimentary credit monitoring is woefully inadequate. Plaintiffs' and Class members' Personal Information was accessed and acquired by cybercriminals for the express purpose of misusing the data. As a consequence, they face the real, immediate, and likely danger of identity theft and misuse of their Personal Information. This can, and in some circumstances already has, caused irreparable harm to their personal, financial, reputational, and future well-being. This harm

is even more acute because much of the stolen Personal Information, such as healthcare data, is immutable.

55. In short, Defendant's myriad failures, including the failure to timely detect an intrusion and failure to timely notify Plaintiffs and Class members that their personal and medical information had been stolen due to Defendant's security failures, allowed unauthorized individuals to access, misappropriate, and misuse Plaintiffs' and Class members' Personal Information for four months before Defendant finally granted victims the opportunity to take proactive steps to defend themselves and mitigate the near- and long-term consequences of the Data Breach.

D. Data Breaches Pose Significant Threats

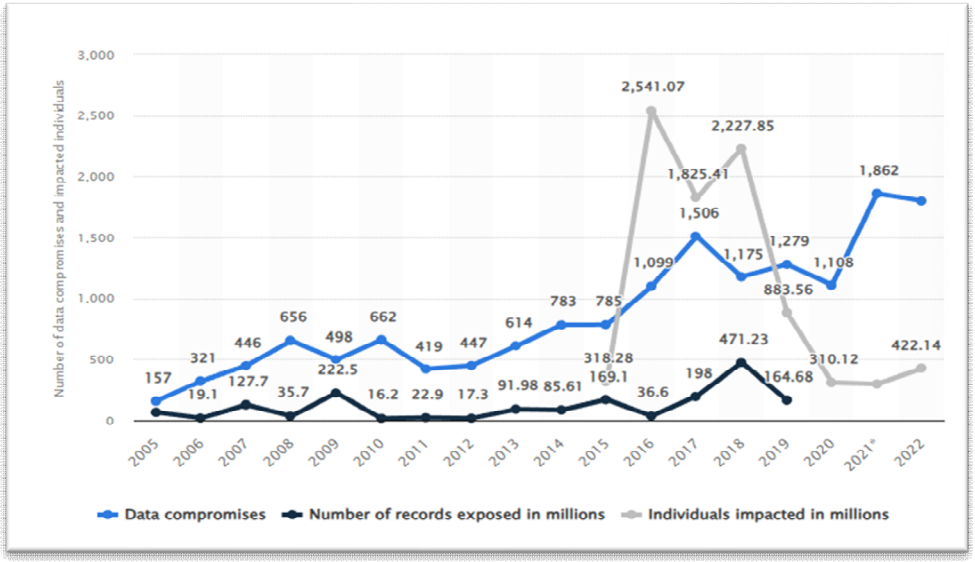
56. Data breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors. It is well known that PII, and Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers.

57. In 2022, the Identity Theft Resource Center's Annual End-of-Year Data Breach Report listed 1,802 total compromises involving 422,143,312 victims for 2022, which was just 50 compromises short of the current record set in 2021.[9] The HIPAA Journal's 2022 Healthcare Data Breach Report reported 707 compromises involving healthcare data, which is just eight shy of the record of 715 set in 2021 and still double that of the number of similar such compromises in 2017 and triple the number of compromises in 2012.[10]

58. Statista, a German entity that collects and markets data relating to, among other things, data breach incidents and the consequences thereof, confirms that the number of data

[6] *2022 End of Year Data Breach Report*, Identity Theft Resource Center (January 25, 2023), available at: https://www.idtheftcenter.org/publication/2022-data-breach-report/?utm_source=press+release&utm_medium=web&utm_campaign=2022+Data+Breach+Report
[10] *2022 Healthcare Data Breach Report*, The HIPAA Journal (January 24, 2023), available at: https://www.hipaajournal.com/2022-healthcare-data-breach-report/.

breaches has been steadily increasing since it began a survey of data compromises in 2005 with 157 compromises reported that year, to a peak of 1,862 in 2021, to 2022's total of 1,802.[11] The number of impacted individuals has also risen precipitously from approximately 318 million in 2015 to 422 million in 2022, which is an increase of nearly 50%.[12]



59. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[13] For example, with the Personal Information stolen in the Data Breach, identity thieves can open financial accounts, apply for credit, collect government benefits, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal benefits, give breach victims' names to police during arrests, and

[11] *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2022*, Statista, available at: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.
[12] *Id.*
[13] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

many other harmful forms of identity theft.[14] These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class members.

60. Personal Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.[15] This stolen Personal Information is then routinely traded on dark web black markets as a simple commodity.[16]

61. In addition, the severity of the consequences of a compromised Social Security number belies the ubiquity of stolen numbers on the dark web. Criminals and other unsavory groups can fraudulently take out loans under the victims' name, open new lines of credit, and cause other serious financial difficulties for victims:

> [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 can cause a lot of problems.[17]

62. This is exacerbated by the fact that the problems arising from a compromised Social Security number are exceedingly difficult to resolve. A victim is forbidden from proactively changing his or her number unless and until it is actually misused and harm has already occurred. And even this delayed remedial action is unlikely to undo the damage already done to the victims:

> Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state

[14] https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/.
[15] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/products/gao-07-737.
[16] *What is your identity worth on the dark web?* Cybernews (September 28, 2021), available at: https://cybernews.com/security/whats-your-identity-worth-on-dark-web/.
[17] United States Social Security Administration, *Identity Theft and Your Social Security Number*, United States Social Security Administration (July 2021), available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

> motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.[18]

63. A particularly troubling example of this effect is the development of "Fullz" packages. A "Fullz" packages is a dosser of information that cybercriminals and other unauthorized parties can assemble by cross-referencing the Personal Information compromised in a given data breach to publicly available data or data compromised in other data breaches. Automated programs can and are routinely used to create these dossiers and they typically represent an alarmingly accurate and complete profile of a given individual.

64. Therefore, through the use of these "Fullz" packages, stolen Personal Information from this Data Breach can be easily linked to Plaintiffs' and the proposed Class members' phone numbers, email addresses, and other sources and identifiers. Thus, even if certain information such as emails, phone numbers, or credit card or financial account were not compromised in this Data Breach, criminals can easily create a Fullz package to sell for profit.

65. Upon information and belief, this has already transpired (and will continue to transpire) for Plaintiffs and the Class. It is reasonable that the trier of fact will find that Plaintiffs and other Class members' stolen Personal Information is being misused, and that such misuse is fairly traceable to the Data Breach.

66. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained: "Compared to credit card information,

[18] *Id.*

personally identifiable information and Social Security numbers are worth more than 10x on the black market."[19]

67. The most sought after and expensive information on the dark web are stolen medical records which command prices from $250 to $1,000 each.[20] Medical records are considered the most valuable because unlike credit cards, which can easily be canceled, and social security numbers, which can be changed, medical records contain "a treasure trove of unalterable data points, such as a patient's medical and behavioral health history and demographics, as well as their health insurance and contact information."[21] With this bounty of ill-gotten information, cybercriminals can steal victims' public and insurance benefits and bill medical charges to victims' accounts.[22] Cybercriminals can also change the victims' medical records, which can lead to misdiagnosis or mistreatment when the victims seek medical treatment.[23] Victims of medical identity theft could even face prosecution for drug offenses when cybercriminals use their stolen information to purchase prescriptions for sale in the drug trade.[24]

68. The wrongful use of compromised medical information is known as medical identity theft and the damage resulting from medical identity theft is routinely far more serious than the harm resulting from the theft of simple PII. Victims of medical identity theft spend an

[19] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at* https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x- price-of-stolen-credit-card-numbers.html.
[20] Paul Nadrag, Capsule Technologies, *Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web*, Fierce Healthcare (January 26, 2021), available at: https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web.
[21] *Id.*
[22] *Medical Identity Theft in the New Age of Virtual Healthcare*, IDX (March 15, 2021), available at https://www.idx.us/knowledge-center/medical-identity-theft-in-the-new-age-of-virtual-healthcare. *See also* Michelle Andrews, *The Rise of Medical Identity Theft*, Consumer Reports (August 25, 2016), available at https://www.consumerreports.org/health/medical-identity-theft-a1699327549/.
[23] *Id.*
[24] *Id.*

average of $13,500 to resolve problems arising from medical identity theft and there are currently no laws limiting a consumer's liability for fraudulent medical debt (in contrast, a consumer's liability for fraudulent credit card charges is capped at $50).[25] It is also "considerably harder" to reverse the damage from the aforementioned consequences of medical identity theft.[26]

69. Instances of medical identity theft have grown exponentially over the years from approximately 6,800 cases in 2017 to just shy of 43,000 in 2021, which represents a seven-fold increase in the crime.[27]

70. In light of the dozens of high-profile health and medical information data breaches that have been reported in recent years, entities like Defendant charged with maintaining and securing customer and patient PII should know the importance of protecting that information from unauthorized disclosure. Indeed, Defendant knew, or certainly should have known, of the recent and high-profile data breaches in the health care industry: UnityPoint Health, Lifetime Healthcare, Inc., Community Health Systems, Kalispell Regional Healthcare, Anthem, Premera Blue Cross, and many others.[28] In addition, the Federal Trade Commission ("FTC") has brought dozens of cases against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data, including recent cases concerning health-related information against LabMD, Inc., SkyMed International, Inc., and others. The FTC publicized these enforcement actions to place companies like Defendant on notice of their obligation to safeguard customer and patient information.[29]

[25] Medical Identity Theft, AARP (March 25, 2022), available at: https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html.
[26] *Id.*
[27] *Id.*
[28] *See, e.g.*, *Healthcare Data Breach Statistics*, HIPAA Journal, available at: https://www.hipaajournal.com/healthcare-data-breach-statistics.
[29] *See, e.g.*, *In the Matter of SKYMED INTERNATIONAL, INC.*, C-4732, 1923140 (F.T.C. Jan. 26, 2021).

71. Given the nature of Defendant's Data Breach, and the long delay in notification to victims thereof, it is foreseeable that the compromised Personal Information has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiffs' and Class members' Personal Information can easily obtain Plaintiffs' and Class members' tax returns or open fraudulent credit card accounts in their names.

72. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.[30] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

73. To date, Defendant has offered its consumers only limited identity theft monitoring services. The services offered are inadequate to protect Plaintiffs and Class members from the threats they will face for years to come, particularly in light of the Personal Information at issue here.

74. Despite the prevalence of public announcements of data breach and data security compromises, its own acknowledgment of the risks posed by data breaches, and its own acknowledgment of its duties to keep Personal Information private and secure, Defendant failed to take appropriate steps to protect the Personal Information of Plaintiffs and Class members from misappropriation. As a result, the injuries to Plaintiffs and Class members were directly and

[30] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes (Mar 25, 2020), available at https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1. *See also Why Your Social Security Number Isn't as Valuable as Your Login Credentials*, Identity Theft Resource Center (June 18, 2021), available at https://www.idtheftcenter.org/post/why-your-social-security-number-isnt-as-valuable-as-your-login-credentials/.

proximately caused by Defendant's failure to implement or maintain adequate data security measures for its current and former patients and customers.

E. Plaintiffs' Experiences

Plaintiff William Matiasek's Experience

75. Plaintiff Matiasek's Personal Information was entrusted to MVES in exchange for elder services.

76. Plaintiff and Class members' Personal Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

77. Plaintiff Matiasek received a notice letter from Defendant dated October 22, 2024, informing him that his Personal Information was accessed in the Data Breach.

78. Plaintiff Matiasek is very careful about sharing his sensitive information.

79. Plaintiff Matiasek stores any documents containing his Personal Information in a safe and secure location. Plaintiff Matiasek has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

80. Because of the Data Breach, Plaintiff Matiasek's Personal Information is now in the hands of cybercriminals.

81. Plaintiff Matiasek has suffered actual injury from the exposure and theft of his Personal Information—which violates his right to privacy.

82. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number and private medical and health insurance information, Plaintiff Matiasek is now imminently at risk of crippling future identity theft and fraud.

83. Since the Data Breach, Plaintiff Matiasek has experienced a massive increase in the number of spam telephone calls he receives. The volume of calls is such that he has had to engage

his telephone provider to block incoming calls. Plaintiff Matiasek attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, the fact that he has never experienced anything like this prior to now, and the fact that he is very careful with his Personal Information.

84. In response to receiving the breach notification letter, Plaintiff Matiasek and his family spent hundreds of dollars to have a technology expert sweep Plaintiff Matiasek's devices and provide other protective services. These out-of-pockets expenses were incurred in an attempt to mitigate the risks associated with having his highly sensitive Personal Information exposed to cybercriminals.

85. Further, as a result of the Data Breach, Plaintiff Matiasek has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Matiasek has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing all account statements and other information, locating and hiring a technology expert, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities, obligations, and/or money-making opportunities.

86. The letter Plaintiff Matiasek received from Defendant specifically directed him to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised individuals affected by the breach to "remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements

and monitoring credit reports closely." [31] In addition, the breach notification letter listed several recommended steps that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, placing fraud alerts with credit reporting bureaus, and placing security freezes on credit reports.[32]

87. As a result of the Data Breach, Plaintiff Matiasek has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Personal Information. Plaintiff Matiasek fears that criminals will use his information to commit identity theft. Plaintiff Matiasek has lost numerous hours of sleep due to the stress and anxiety, prompting him to seek medical attention from a doctor.

88. Plaintiff Matiasek anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

89. Plaintiff Matiasek has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Personal Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Matiasek's Personal Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Matiasek's Personal Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Matiasek 's Personal Information; and (e) continued risk to Plaintiff Matiasek's Personal Information, which remains in the possession of Defendant and which is subject to further

[31] *See* MVES breach letter, available at: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/39b8a2d8-4720-4f85-9dd7-8929d9a7a168.html.
[32] *Id.*

breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information that was entrusted to Defendant.

Plaintiff Diane Remick's Experience

90. Plaintiff Remick's Personal Information was entrusted to MVES in exchange for elder services.

91. Plaintiff and Class members' Personal Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

92. Plaintiff Remick received a notice letter from Defendant dated October 22, 2024, informing her that her Personal Information was accessed as a result of the Data Breach.

93. Plaintiff Remick is very careful about sharing her sensitive information.

94. Plaintiff Remick stores any documents containing her Personal Information in a safe and secure location. Plaintiff Remick has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or any other unsecured source.

95. Because of the Data Breach, Plaintiff Remick's Personal Information is now in the hands of cybercriminals.

96. Plaintiff Remick has suffered actual injury from the exposure and theft of her Personal Information—which violates her right to privacy.

97. As a result of the Data Breach, which exposed highly valuable information, Plaintiff Remick is now imminently at risk of crippling future identity theft and fraud.

98. Since the Data Breach, Plaintiff Remick has experienced identity theft in the form of multiple Lyft rides being ordered using her information that she did not request. Plaintiff Remick attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time

proximity, the fact that she has never experienced anything like this prior to now, and the fact that she is very careful with her Personal Information.

99. As a result of the Data Breach, Plaintiff Remick has had no choice but to spend numerous hours attempting to mitigate the harm caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Remick has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing all account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities, obligations, and/or money-making opportunities.

100. The letter Plaintiff Remick received from Defendant specifically directed her to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised individuals affected by the breach to "remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely." [33] In addition, the breach notification letter listed several recommended steps that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, placing fraud alerts with credit reporting bureaus, and placing security freezes on credit reports.[34]

101. As a result of the Data Breach, Plaintiff Remick has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing

[33] *Id.*
[34] *Id.*

and misusing her Personal Information. Plaintiff Remick fears that criminals will use her information to commit identity theft.

102. Plaintiff Remick anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

103. Plaintiff Remick has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Personal Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Remick's Personal Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Remick's Personal Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Remick's Personal Information; and (e) continued risk to Plaintiff Remick's Personal Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information that was entrusted to Defendant.

Plaintiff Donna Pruitt's Personal Experience

104. Plaintiff Pruitt's Personal Information was entrusted to MVES in exchange for elder services.

105. Plaintiff and Class members' Personal Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

106. Plaintiff Pruitt received a notice letter from Defendant dated October 22, 2024, informing her that her Personal Information was accessed as a result of the Data Breach.

107. Plaintiff Pruitt is very careful about sharing her sensitive information.

108. Plaintiff Pruitt stores any documents containing her Personal Information in a safe and secure location. Plaintiff Pruitt has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or any other unsecured source.

109. Because of the Data Breach, Plaintiff Pruitt's Personal Information is now in the hands of cybercriminals.

110. Plaintiff Pruitt has suffered actual injury from the exposure and theft of her Personal Information—which violates her right to privacy.

111. As a result of the Data Breach, which exposed highly valuable information, Plaintiff Pruitt is now imminently at risk of crippling future identity theft and fraud.

112. Plaintiff Pruitt has already experienced identity theft as a result of the Data Breach. Indeed, in January 2025, Plaintiff Pruitt was notified that an unknown individual attempted to open a financial account in her name. In addition, since the Data Breach, Plaintiff Pruitt experienced multiple fraudulent charges on her payment card by an unknown person in California. In the months following the Data Breach, Plaintiff Pruitt has also received notice that her PII has been found on the dark web. Further, the number of spam telephone calls she receives has increased significantly. Plaintiff Pruitt attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, the fact that she has never experienced anything like this prior to now, and the fact that she is very careful with her Personal Information.

113. As a result of the Data Breach, Plaintiff Pruitt has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Pruitt has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate,

and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing all account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities, obligations, and/or money-making opportunities.

114. The letter Plaintiff Pruitt received from Defendant specifically directed her to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised individuals affected by the breach to ""remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely."[35] In addition, the breach notification letter listed several recommended steps that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, placing fraud alerts with credit reporting bureaus, and placing security freezes on credit reports.[36]

115. As a result of the Data Breach, Plaintiff Pruitt has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Personal Information. Plaintiff Pruitt fears that criminals will use her information to commit identity theft. In fact, Plaintiff Pruitt's PII has already been utilized for this purpose.

116. Plaintiff Pruitt anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

117. Plaintiff Pruitt has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Personal Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Pruitt's

[35] *Id.*
[36] *Id.*

Personal Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Pruitt's Personal Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Pruitt's Personal Information; and (e) continued risk to Plaintiff Pruitt's Personal Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information that was entrusted to Defendant.

Plaintiff Karen Picardi's Experience

118. Plaintiff Picardi's Personal Information was entrusted to MVES in exchange for elder services. Further, Plaintiff Picardi was an employee of MVES prior to receiving services.

119. Plaintiff and Class members' Personal Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

120. Plaintiff Picardi received a notice letter from Defendant dated October 22, 2024, informing her that her Personal Information was accessed as a result of the Data Breach.

121. Plaintiff Picardi is very careful about sharing her sensitive information.

122. Plaintiff Picardi stores any documents containing her Personal Information in a safe and secure location. Plaintiff Picardi has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or any other unsecured source.

123. Because of the Data Breach, Plaintiff Picardi's Personal Information is now in the hands of cybercriminals.

124. Plaintiff Picardi has suffered actual injury from the exposure and theft of her Personal Information—which violates her right to privacy.

125. As a result of the Data Breach, which exposed highly valuable information, Plaintiff Picardi is now imminently at risk of crippling future identity theft and fraud.

126. Since the Data Breach, Plaintiff Picardi has experienced identity theft. Specifically, following the Data Breach, Plaintiff Picardi experienced suspicious transactions on her bank and credit card accounts that required her to dispute those charges. Since the Data Breach, Plaintiff Picardi also experienced fraudulent inquiries being made on her credit report. Plaintiff Picardi has also noticed a significant increase in the number of spam telephone calls and phishing attempts she receives in the months following the Data Breach. Plaintiff Picardi attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, the fact that she has never experienced anything like this prior to now, and the fact that she is very careful with her Personal Information.

127. As a result of the Data Breach, Plaintiff Picardi has had no choice but to spend numerous hours attempting to mitigate the harm caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Picardi has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing all account statements and other information, placing credit freezes on her accounts, communicating with her bank and credit card company regarding fraudulent charges, and screening phishing and spam calls, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities, obligations, and/or money-making opportunities.

128. The letter Plaintiff Picardi received from Defendant specifically directed her to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised individuals affected by the breach to "remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely." [37] In addition, the breach notification letter listed several recommended steps that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, placing fraud alerts with credit reporting bureaus, and placing security freezes on credit reports.[38]

129. As a result of the Data Breach, Plaintiff Picardi has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Personal Information. Plaintiff Picardi fears that criminals will use her information to commit further identity theft.

130. Plaintiff Picardi anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

131. Plaintiff Picardi has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Personal Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Picardi's Personal Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Picardi's Personal Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security

[37] *Id.*
[38] *Id.*

to protect Plaintiff Picardi's Personal Information; and (e) continued risk to Plaintiff Picardi's Personal Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information that was entrusted to Defendant.

Plaintiff Diana Cerrone's Experience

132. Plaintiff Cerrone's Personal Information was entrusted to MVES in exchange for elder services.

133. Plaintiff and Class members' Personal Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

134. Plaintiff Cerrone received a notice letter from Defendant dated October 22, 2024, informing her that her Personal Information was accessed as a result of the Data Breach.

135. Plaintiff Cerrone is very careful about sharing her sensitive information.

136. Plaintiff Cerrone stores any documents containing her Personal Information in a safe and secure location. Plaintiff Cerrone has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or any other unsecured source.

137. Because of the Data Breach, Plaintiff Cerrone's Personal Information is now in the hands of cybercriminals.

138. Plaintiff Cerrone has suffered actual injury from the exposure and theft of her Personal Information—which violates her right to privacy.

139. As a result of the Data Breach, which exposed highly valuable information, Plaintiff Cerrone is now imminently at risk of crippling future identity theft and fraud.

140. Since the Data Breach, Plaintiff Cerrone has experienced a noticeable increase in the number of spam telephone calls she receives. Plaintiff Cerrone attributes the foregoing

suspicious and unauthorized activity to the Data Breach given the time proximity, the fact that she has never experienced anything like this prior to now, and the fact that she is very careful with her Personal Information.

141. As a result of the Data Breach, Plaintiff Cerrone has had no choice but to spend numerous hours attempting to mitigate the harm caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Cerrone has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing all account statements and other information, screening and responding to spam calls and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities, obligations, and/or money-making opportunities.

142. The letter Plaintiff Cerrone received from Defendant specifically directed her to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised individuals affected by the breach to "remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely." [39] In addition, the breach notification letter listed several recommended steps that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, placing fraud alerts with credit reporting bureaus, and placing security freezes on credit reports.[40]

143. As a result of the Data Breach, Plaintiff Cerrone has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing

[39] *Id.*
[40] *Id.*

and misusing her Personal Information. Plaintiff Cerrone fears that criminals will use her information to commit identity theft.

144. Plaintiff Cerrone anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

145. Plaintiff Cerrone has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Personal Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Cerrone's Personal Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Cerrone's Personal Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Cerrone's Personal Information; and (e) continued risk to Plaintiff Cerrone's Personal Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information that was entrusted to Defendant.

F. Defendant had a Duty and Obligation to Protect Personal Information under the Law and the Applicable Standard of Care

146. Defendant was prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

147. Defendant is further required by various states' laws and regulations to protect Plaintiffs' and Class members' Personal Information.

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

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

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

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

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

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

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

1. Defendant Failed to Comply with HIPAA Guidelines

155. HIPAA requires, *inter alia*, that Covered Entities and Business Associates implement and maintain policies, procedures, systems and safeguards that ensure the

confidentiality and integrity of consumer and patient PII and PHI, protect against any reasonably anticipated threats or hazards to the security or integrity of consumer and patient PII and PHI, regularly review access to data bases containing protected information, and implement procedures and systems to detect, contain, and correct any unauthorized access to protected information. *See* 45 CFR § 164.302, *et seq.*

156. HIPAA, as applied through federal regulations, also requires Personal Information to be stored in a manner that renders it, "unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology. . . ." 45 CFR § 164.402.

157. Defendant is a covered entity under HIPAA (45 C.F.R. § 160.102) and are 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.

158. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[41] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

159. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

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

[41] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

161. 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.

162. "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.

163. HIPAA's Security Rule requires Defendant to 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.

164. 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).

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

166. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[42]

167. HIPAA requires a covered entity 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).

168. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information 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).

169. 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.[43] 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

[42]Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added).
[43] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.

business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[44]

170. Upon information and belief, Defendant's security failures include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;
b. Failing to mitigate the risks of a data breach and loss of data;
c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);
d. Failing to implement 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 in violation of 45 CFR 164.312(a)(1);
e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);
f. Failing to identify and respond to suspected or known security incidents;
g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);
h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);
i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

[44]https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 CFR 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

171. Upon information and belief, Defendant also failed to store the information it collected in a manner that rendered it, "unusable, unreadable, or indecipherable to unauthorized persons," in violation of 45 CFR § 164.402.

2. Defendant Failed to Follow FTC Act Requirements

172. 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. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

173. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[45] The guidelines note businesses should protect the Personal Information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and

[45] *Protecting Personal Information: A Guide for Business*, Federal Trade Comm'n (October 2016), available at https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last accessed August 15, 2023).

implement policies to correct security problems.[46] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[47] Defendant clearly failed to do any of the foregoing, as evidenced by the fact the Data Breach occurred, the fact that the Breach resulted in the theft of unencrypted data, and the amount of data exfiltrated.

174. The FTC further recommends that companies not maintain PII 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 the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

175. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by 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 the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

176. Additionally, the FTC Health Breach Notification Rule obligates companies that suffered a data breach to provide notice to every individual affected by the data breach, as well as notifying the media and the FTC. *See* 16 CFR 318.1, *et seq.*

177. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to

[46] *Id.*
[47] *Id.*

protect against unauthorized access to Plaintiffs' and Class members' Personal Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

178. Defendant was fully aware of its obligation to protect the Personal Information of its current and former consumers and patients, including Plaintiffs and Class members. Defendant is a sophisticated and technologically savvy business that relies extensively on technology systems and networks to maintain its practice, including storing its consumers' and patients' PII, protected health information, and medical information in order to operate its business.

179. Defendant had and continues to have a duty to exercise reasonable care in collecting, storing, and protecting the Personal Information from the foreseeable risk of a data breach. The duty arises out of the special relationship that exists between Defendant and Plaintiffs and Class members. Defendant alone had the exclusive ability to implement adequate security measures to its cyber security network to secure and protect Plaintiffs' and Class members' Personal Information.

3. Defendant Failed to Follow Industry Standards

180. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Personal Information that they collect and maintain.

181. Some industry best practices that should be implemented by businesses dealing with sensitive Personal Information, like Defendant, include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

182. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

183. Defendant should have also followed the minimum standards of any of the following frameworks: NIST Cybersecurity Framework Version 2.0 (including 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 CSC). These are all established standards in reasonable cybersecurity readiness.

184. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

4. Defendant's Own Stated Policies and Promises

185. Defendant's own published Notice of Privacy Practices ("Privacy Policy") states that they collect PII and PHI on their clients through their work with Medicaid and other health care providers.[48] However, the Privacy Policy assures that "MVES takes your privacy very seriously."[49]

[48] *See* https://live-mves.pantheonsite.io/wp-content/uploads/2020/09/MVES-NPP-FINAL.pdf (Last accessed February 18, 2025).
[49] *Id.*

186. Defendant's Privacy Policy further advises that beyond certain delineated exceptions, "MVES cannot use or share your health information with anyone without your written permission."[50]

187. Defendant's Privacy Policy further acknowledges that "by law" they must:

a. ***protect the privacy of your health information as described in this notice***;
b. explain our privacy practices to you; and
c. notify you if your unsecured health information is obtained by an unauthorized person.[51]

188. Defendant failed to live up to its own stated policies and promises with regards to data privacy and data security as cybercriminals were able to infiltrate its systems and steal the Personal Information belonging to Plaintiffs and Class members. Defendant further failed to live up to its own stated policy by failing to provide timely and sufficient notice of the Data Breach to affected individuals.

G. Plaintiffs and the Class Suffered Harm Resulting from the Data Breach

189. Like any data hack, the Data Breach presents major problems for all affected.[52]

190. The FTC warns the public to pay particular attention to how they keep personally identifying information including Social Security numbers and other sensitive data. As the FTC notes, "once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[53]

[50] *Id.*
[51] *Id.* (emphasis added).
[52] Paige Schaffer, *Data Breaches' Impact on Consumers*, Insurance Thought Leadership (July 29, 2021), available at https://www.insurancethoughtleadership.com/cyber/data-breaches-impact-consumers.
[53] *Warning Signs of Identity Theft*, Federal Trade Comm'n, available at https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft.

191. The ramifications of Defendant's failure to properly secure Plaintiffs' and Class members' Personal Information are severe. Identity theft occurs when someone uses another person's financial, and personal information, such as that person's name, address, Social Security number, and other information, without permission in order to commit fraud or other crimes.

192. According to data security experts, one out of every four data breach notification recipients become a victim of identity fraud.

193. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.

194. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiffs and the Class at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. According to a recent study published in the scholarly journal *Preventive Medicine Reports*, public and corporate data breaches correlate to an increased risk of identity theft for victimized consumers.[54] The same study also found that identity theft is a deeply traumatic event for the victims, with more than a quarter of victims still experiencing sleep problems, anxiety, and irritation even six months after the crime.[55]

195. There is also a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that has not yet been exploited by cybercriminals presents a concrete risk that the cybercriminals who now possess Class members' Personal Information will do so at a later date or re-sell it.

[54] David Burnes, Marguerite DeLiema, Lynn Langton, *Risk and protective factors of identity theft victimization in the United States*, Preventive Medicine Reports, Volume 17 (January 23, 2020), available at https://www.sciencedirect.com/science/article/pii/S2211335520300188?via%3Dihub.
[55] *Id.*

196. Data breaches have proven to be costly for affected organizations as well, with the average cost to resolve being $4.45 million dollars in 2023.[56] The average cost to resolve a data breach involving health information, however, is more than double this figure at $10.92 million.[57]

197. The theft of medical information, beyond the theft of more traditional forms of PII, is especially harmful for victims. Medical identity theft, the misuse of stolen medical records and information, has seen a seven-fold increase over the last five years and this explosive growth far outstrips the increase in incidence of traditional identity theft.[58] Medical Identity Theft is especially nasty for victims because of the lack of laws that limit a victim's liabilities and damages from this type of identity theft (*e.g.*, a victim's liability for fraudulent credit card charges is capped at $50), the unalterable nature of medical information, the sheer costs involved in resolving the fallout from a medical identity theft (victims spend, on average, $13,500 to resolve problems arising from this crime), and the risk of criminal prosecution under anti-drug laws.[59]

198. In response to the Data Breach, Defendant offered to provide certain individuals whose Personal Information was exposed in the Data Breach with a limited term of credit monitoring. However, this is inadequate to protect victims of the Data Breach from the lifelong risk of harm imposed on them by Defendant's failures.

---

[56] *Cost of a Data Breach Report 2023*, IBM Security, available at https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700072379268622&p5=p&gclid=CjwKCAjwxOymBhAFEiwAnodBLGiGtWfjX0vRlNbx6p9BpWaOo9eZY1i6AMAc6t9S8IKsxdnbBVeUbxoCtk8QAvD_BwE&gclsrc=aw.ds.

[57] *Id.*

[58] Medical Identity Theft, AARP (March 25, 2022), available at: https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html.

[59] *Id.*

199. Moreover, the credit monitoring offered by Defendant is fundamentally inadequate to protect them from the injuries resulting from the unauthorized access and exfiltration of their sensitive Personal Information.

200. Here, due to the Breach, Plaintiffs and Class members have been exposed to injuries that include, but are not limited to:

a. Theft of Personal Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts as a direct and proximate result of the Personal Information stolen during the Data Breach;

c. Damages arising from the inability to use accounts that may have been compromised during the Data Breach;

d. Costs associated with time spent to address and mitigate the actual and future consequences of the Data Breach, such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, placing freezes and alerts on their credit reports, contacting their financial institutions to notify them that their personal information was exposed and to dispute fraudulent charges, imposition of withdrawal and purchase limits on compromised accounts, including but not limited to lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance, and annoyance of dealing with all issues resulting from the Data Breach, if they were fortunate enough to learn of the Data Breach despite Defendant's delay in disseminating notice in accordance with state law and HIPAA;

e. The imminent and impending injury resulting from potential fraud and identity theft posed because their Personal Information is exposed for theft and sale on the dark web; and

f. The loss of Plaintiffs' and Class members' privacy.

201. Plaintiffs and Class members have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their Personal Information being accessed by cybercriminals, risks that will not abate within the limited time of credit monitoring offered by Defendant.

202. As a direct and proximate result of Defendant's acts and omissions in failing to protect and secure Personal Information, Plaintiffs and Class members have been placed at a substantial risk of harm in the form of identity theft, and they have incurred and will incur actual damages in an attempt to prevent identity theft.

203. Plaintiffs retain an interest in ensuring there are no future breaches; in addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of both themselves and similarly situated individuals whose Personal Information was accessed in the Data Breach.

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

204. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some of the biggest cybersecurity breaches: Target,[60] Yahoo,[61] Marriott International,[62] Chipotle, Chili's, Arby's,[63] and others.[64]

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

---

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

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

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

[63] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.

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

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

I. Cyber Criminals Will Use Plaintiffs' and Class Members' Personal Information to Defraud Them

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

208. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[65] For example, with the Personal Information stolen in the Data Breach, identity thieves can open financial accounts, apply for credit, collect government benefits, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[66] These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class members.

209. Personal Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.[67]

---

[65] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").
[66] https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/.
[67] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/products/gao-07-737.

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

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

212. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to personally identifiable information, they will use it.[68]

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

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[69]

214. As described above, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[70]

---

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

[69] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/products/gao-07-737.

[70] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

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

216. Victims of the Data Breach, like Plaintiffs and other Class members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their credit because of the Data Breach.[71]

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

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

a. Trespass, damage to, and theft of their personal property including Personal Information;

b. Improper disclosure of their Personal Information;

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

[71] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

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

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

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

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

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

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

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

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

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

220. Plaintiffs and Class members are desperately trying to mitigate the damage that Defendant has caused them but, given the Personal Information Defendant made accessible to hackers, they are certain to incur additional damages. Because identity thieves have their Personal Information, Plaintiffs and all Class members will need to have identity theft monitoring protection for the rest of their lives.

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

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

222. Data breaches are preventable.[72] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[73] she added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[74]

223. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[75]

224. As discussed *supra*, Defendant failed to follow HIPAA requirements, failed to follow FTC guidelines, and failed to implement industry-standard data security. Had Defendant followed these standards and requirements, the Data Breach would have been prevented.

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

---

[72]Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

[73]*Id.* at 17.

[74]*Id.* at 28.

[75]*Id.*

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

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

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

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

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

V. CLASS ACTION ALLEGATIONS

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

232. Plaintiffs bring all claims as class claims under Massachusetts Rule of Civil Procedure 23. Plaintiffs assert all claims on behalf of the Nationwide Class, defined as follows:

> All persons residing in Massachusetts whose Personal Information was compromised as a result of the Data Breach, including those who were sent breach notification letters from Defendant.

233. Plaintiffs reserve the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

234. The proposed Class meets the requirements of Massachusetts Rule of Civil Procedure 23.

235. **Numerosity:** The proposed Class is believed to be so numerous that joinder of all members is impracticable. The exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Defendant and obtainable by Plaintiffs only through the discovery process. On information and belief, the number of affected individuals estimated to be 85,133.[76] The members of the Class will be identifiable through information and records in Defendant's possession, custody, and control.

236. **Commonality:** There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

[76] *See* *https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=A8CE368FF3CD746604432995F9EAB5A9* (last accessed February 18, 2025).

b. Whether Defendant failed to adequately safeguard Plaintiffs' and the Class's Personal Information;

c. Whether Defendant's email and computer systems and data security practices used to protect Plaintiffs' and Class members' Personal Information violated the FTC Act, and/or state laws and/or Defendant's other duties discussed herein;

d. Whether Defendant owed a duty to Plaintiffs and the Class to adequately protect their Personal Information, and whether it breached this duty;

e. Whether Defendant knew or should have known that its computer and network security systems and business email accounts were vulnerable to a data breach;

f. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach;

g. Whether Defendant breached contractual duties owed to Plaintiffs and the Class to use reasonable care in protecting their Personal Information;

h. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and the Class;

i. Whether Defendant continues to breach duties to Plaintiffs and the Class;

j. Whether Plaintiffs and the Class suffered injury as a proximate result of Defendant's actions or failures to act;

k. Whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief;

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

m. Whether Defendant's actions alleged herein constitute recklessness and a breach of Defendant's obligations; and

n. Whether Plaintiffs and Class members are entitled to punitive damages.

237. **Typicality:** Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through Defendant's uniform misconduct. The same event and conduct that gave rise to Plaintiffs' claims are identical to those that give rise to the claims of every other Class member because Plaintiffs and each member of the Class had their sensitive Personal Information compromised in the same way by the same conduct of Defendant.

238. **Adequacy:** Plaintiffs is an adequate representative of the Class because his interests do not conflict with the interests of the Class that Plaintiffs seek to represent; Plaintiffs have retained counsel competent and highly experienced in data breach class action litigation; and Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and Plaintiffs' counsel.

239. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult, if not impossible, for members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

240. Class certification is proper because Defendant has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

241. Class certification is also proper because Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' Personal Information was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

242. A class action is superior to other available methods for the fair and efficient adjudication of the controversy.

243. Class certification is also appropriate because this Court can designate particular claims or issues for class-wide treatment and may designate one or more Subclasses.

244. 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 letters by Defendant.

VI. CAUSES OF ACTION

COUNT ONE

NEGLIGENCE

245. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein.

246. Defendant gathered and stored the Personal Information of Plaintiffs and Class Members as part of its business.

247. Plaintiffs and Class Members entrusted Defendant with their Personal Information with the understanding that Defendant would safeguard their information.

248. Defendant had full knowledge of the sensitivity of the Personal Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Personal Information were wrongfully disclosed.

249. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Personal Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

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

251. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the Personal Information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

252. For instance, HIPAA required Defendant to notify victims of the Breach within 60 days of the discovery of the Data Breach. Defendant did not begin to notify Plaintiffs or Class Members of the Data Breach until months after learning that unauthorized persons had accessed and acquired the private, protected, personal information of Plaintiffs and the Class.

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

254. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its clients. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential Personal Information, a necessary part of being clients of the Defendant.

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

256. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Class.

257. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former clients' Personal Information it was no longer required to retain pursuant to regulations.

258. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

259. Defendant had and continues to have a duty to adequately disclose that the Personal Information of Plaintiffs and the Class within Defendant's possession might have been

compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Personal Information by third parties.

260. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect Class Members' Personal Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

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

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

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

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

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

f. Failing to remove former patients' Personal Information it was no longer required to retain pursuant to regulations,

g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

261. Defendant violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

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

263. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against.

264. Defendant's violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

265. The FTC has pursued enforcement actions against businesses, which, as a result of their failures to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

266. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

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

268. Defendant had full knowledge of the sensitivity of the Personal Information and the types of harm that Plaintiffs and the Class could and would suffer if the Personal Information were wrongfully disclosed.

269. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Personal Information of Plaintiffs and the Class, the critical importance of providing adequate security of that Personal Information, and the necessity for encrypting Personal Information stored on Defendant's systems.

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

271. Plaintiffs and the Class had no ability to protect their Personal Information that was in, and possibly remains in, Defendant's possession.

272. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

273. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

274. Defendant has admitted that the Personal Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

275. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Personal Information of Plaintiffs and the Class would not have been compromised.

276. There is a close causal connection between Defendant's failure to implement security measures to protect the Personal Information of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The Personal Information of Plaintiffs and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Personal Information by adopting, implementing, and maintaining appropriate security measures.

277. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Personal Information; (iii) lost or diminished value of Personal Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) Plaintiffs' Personal Information being disseminated on the dark web; (x) nominal damages; and (xi) the continued and certainly increased risk to their Personal Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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 Personal Information.

278. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class 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.

279. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Personal Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Personal Information in its continued possession.

280. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

281. Defendant's negligent conduct is ongoing, in that it still holds the Personal Information of Plaintiffs and Class Members in an unsafe and insecure manner.

282. Plaintiffs and Class members are therefore entitled to damages, including restitution and unjust enrichment, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT TWO

BREACH OF IMPLIED CONTRACT

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

284. Plaintiffs and Class Members were required to provide Defendant with their Personal Information in order to receive care and/or elder or disability services.

285. When Plaintiffs and Class Members provided their Personal Information to Defendant when seeking care or services, they entered into implied contracts in which Defendant

agreed to comply with its statutory and common law duties to protect their Personal Information and to timely notify them in the event of a Data Breach.

286. Defendant represented through its Privacy Policy to Plaintiffs and the Class that they would safeguard their information in accordance with State and Federal laws and provide timely notification in the event their Personal Information was compromised.

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

288. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' Personal Information and failing to provide them with timely and accurate notice of the Data Breach. Indeed, it took Defendant months to warn Plaintiffs and Class Member of their imminent risk of identity theft. Defendant also failed to notify Plaintiffs and the Class Members with specificity what information was compromised, leaving Plaintiffs and Class Members unsure as to the extent of the information that was compromised.

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

COUNT THREE

BREACH OF FIDUCIARY DUTY

290. Plaintiffs incorporate by reference the foregoing paragraphs as if fully set forth herein.

291. At all relevant times hereto, Defendant owed, and owes, a fiduciary duty to Plaintiffs and the Class, including its duty to keep Plaintiffs and Class Members' Personal Information reasonably secure.

292. The fiduciary duty to patients is explicated under the procedures set forth in the Health Insurance Portability and Accountability Act Privacy Rule, including, without limitation the procedures and definitions of 45 C.F.R. §160.103 and 45 C.F.R. §164.530, which required Defendant to apply appropriate administrative, technical, and physical safeguards to protect the privacy of patient information and to secure the health care information it maintains and to keep it free from disclosure.

293. Defendant breached its fiduciary duty to Plaintiffs by failing to implement sufficient safeguards and by disclosing Plaintiffs' and other Class Members' Personal Information to unauthorized third parties.

294. As a direct result of Defendant's breach of its fiduciary duty of confidentiality and the disclosure of Plaintiffs' confidential Personal Information, Plaintiffs and the Class Members have suffered damages.

295. As a direct result of Defendant's breach of its fiduciary duty and the disclosure of Plaintiffs' and Class Members' Personal Information, Plaintiffs and the Class have suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, and humiliation.

296. Plaintiffs and the other Class Members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of the Personal Information; (iii) loss of privacy; (iv) out-of-pocket expenses

incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; (vii) loss of the benefit of the bargain; and (viii) emotional distress. At the very least, Plaintiffs and the Class are entitled to nominal damages.

COUNT FOUR

UNJUST ENRICHMENT

297. Plaintiffs incorporate by reference the preceding allegations as if fully set forth herein.

298. Plaintiffs bring this claim individually and on behalf of the Class in the alternative to their contract-based claims.

299. Upon information and belief, MVES funds its data security measures from its general revenue, including payments made by or on behalf of Plaintiffs and the Class Members.

300. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

301. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased healthcare services from Defendant and/or its agents and in so doing provided Defendant with their PII and PHI. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PII and PHI protected with adequate data security.

302. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII and PHI of Plaintiffs and Class Members for business purposes.

303. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII and PHI. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

304. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by its common law and statutory duties.

305. Defendant failed to secure Plaintiffs' and Class Members' PII and PHI and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

306. Defendant acquired the PII and PHI through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

307. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their PII and PHI, they would not have agreed to provide their PII and PHI to Defendant.

308. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

309. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

COUNT FIVE

MASSACHUSETTS CONSUMER PROTECTION ACT CH. 93A, §§ 1 *et seq.*

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

311. Defendant, Plaintiffs and the Class Members are each a "person" as defined by the Massachusetts Consumer Protection Act ("MCPA"), MASS. GEN. LAWS Ch. 93A, §1(a).

312. By offering elder care and other services, Defendant is engaged in "trade" or "commerce" defined as "the advertising, the offering for sale, rent or lease, the sale, rent, lease or distribution of any services and any property, tangible or intangible, real, personal or mixed, any security . . . and any contract of sale of a commodity for future delivery, and any other article, commodity, or thing of value wherever situate, and shall include any trade or commerce directly or indirectly affecting the people of this commonwealth." MASS. GEN. LAWS Ch. 93A, §1(b).

313. Defendant obtained Plaintiffs' and Class Members' PII through advertising, offering, and/or distributing goods and services to Plaintiffs and Class Members and the Data Breach occurred at least in part through the use of the internet, an instrumentality of interstate commerce.

314. Defendant is engaged in trade or commerce that directly or indirectly affects the people of the Commonwealth of Massachusetts.

315. Under MASS. GEN. LAWS Ch. 93A, §2(a), "unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."

316. Defendant violated MASS. GEN. LAWS Ch. 93A, §2(a) in that it has engaged in "unfair or deceptive acts or practices in the conduct of any trade or commerce."

317. Defendant had a duty to keep the Personal Information of Plaintiffs and the Class Members safe and secure under the various laws and regulations discussed hereinabove.

318. Defendant failed to adequately protect and secure the Personal Information of Plaintiffs and the Class Members and failed to comply with its obligations to protect and secure the Personal Information.

319. Defendant failed to comply with industry standards for the protection and security of the Personal Information.

320. Defendant failed to comply with its own privacy practice relating to the protection and security of the Personal Information.

321. Defendant failed to disclose that it did not have adequate security practices in place to safeguard the Personal Information.

322. Criminals were able to access the Personal Information through the Data Breach.

323. Defendant had a duty to timely notify its clients, including Plaintiffs and the Class Members, of the Data Breach, including under MASS. GEN. LAWS Ch. 93H, §3, the Massachusetts Security Breach statute.

324. Defendant failed to timely notify its customers, including Plaintiffs and Class Members, of the Data Breach.

325. The aforementioned actions and omissions constitute unfair or deceptive acts or practices under MASS. GEN. LAWS Ch. 93A, §2(a).

326. Such acts by Defendant were likely to mislead a reasonable person purchasing and/or using Defendant's services.

327. Said acts are material in that a reasonable person would consider them important in deciding whether to purchase and/or use Defendant's services. If Plaintiffs the Class Members had

known that Defendant had inadequate computer systems and data security practices to properly safeguard their PII, they would not have paid for Defendant's services or would have paid less than they did.

328. Defendant acted with disregard for the security of Plaintiffs' and Class Members' PII. Defendant knew or should have known that MVES had inadequate computer systems and data security practices to safeguard such information, and Defendant knew or should have known that hackers were attempting to access the PII in healthcare companies' databases, such as MVES's.

329. As a result of the aforementioned actions and omissions, Plaintiffs and Class Members have suffered, and will continue to suffer, injury in an amount to be determined at trial, including, but not limited to: the loss of the benefit of their bargain with Defendant; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses incurred protecting themselves from fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

330. As a result of the aforementioned actions and omissions, Plaintiffs and Class Members seek their actual damages, statutory damages, double or treble damages, their costs and reasonable attorneys' fees, and any injunctive or equitable relief needed to secure Personal Information in the possession, custody, and control of Defendant and its agents. *See* MASS. GEN. LAWS Ch. 93A, § 9.

331. Further, as a direct result of Defendant's violations of the MCPA, Plaintiffs and Class Members are entitled to injunctive relief, including, but not limited to:

a. Ordering that Defendant implement measures that ensure that the PII of Defendant's current and former customers is appropriately encrypted and safeguarded when stored on Defendant's network or systems;

b. Ordering that Defendant purge, delete, and destroy in a reasonable secure manner PII not necessary for its provision of services;

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

d. Ordering Defendant to meaningfully educate its current and former customers about the threats they face as a result of the accessibility of their PII to third parties, as well as the steps Defendant's current and former customers must take to protect themselves.

332. A demand identifying the claimant and reasonably describing the unfair or deceptive act or practice and the injury suffered was mailed or delivered to Defendant at least thirty (30) days prior to the filing of a pleading alleging this claim for relief. *See* MASS. GEN. LAWS Ch. 93A, § 9(3). By letter dated October 31, 2024, Plaintiff Matiasek, on behalf of himself and Class Members, sent Defendant notice under this provision. Defendant has not yet responded to Plaintiffs' demand.

COUNT SIX

DECLARATORY/INJUNCTIVE RELIEF

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

334. As previously alleged, Plaintiffs and members of the Class entered into an implied contract that required Defendant to provide adequate security for the Personal Information it collected from Plaintiffs and the Class.

335. Defendant owes a duty of care to Plaintiffs and the members of the Class that requires it to adequately secure Personal Information.

336. Defendant still possess Personal Information regarding Plaintiffs and members of the Class.

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

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

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

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

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

VII. PRAYER FOR RELIEF

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

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

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

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

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

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

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

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

iv. Ordering that Defendant cease transmitting Personal Information via unencrypted email;

v. Ordering that Defendant cease storing Personal Information in email accounts;

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

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

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

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

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

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

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

VIII. DEMAND FOR JURY TRIAL

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

DATED: March 11, 2025

/s/ Jessica Peake

Jessica Peake, Esq. (BBO# 707591)
Mazow McCullough PC
10 Derby Square,
Salem, MA 01970

Phone (978) 744-8000
Fax (978) 744-8012
jsp@helpinginjured.com

A. Brooke Murphy, admitted *pro hac vice*
MURPHY LAW FIRM
4116 Wills Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
Telephone: (405) 389-4989
abm@murphylegalfirm.com

Leigh S. Montgomery*
Texas Bar No. 24052214
lmontgomery@eksm.com
EKSM, LLP
1105 Milford Street
Houston, Texas 77006
Phone: (888) 350-3931
Fax: (888) 276-3455

Kevin Laukaitis*
LAUKAITIS LAW LLC
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
T: (215) 789-4462
klaukaitis@laukaitislaw.com

Plaintiffs' Executive Counsel

**Pro Hac Vice application to be submitted*