UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF KENTUCKY
LOUISVILLE DIVISION

In re OnePoint Patient Care, LLC., Data Breach Litigation	Case No. Case No.: 3:24-cv-00649-RGJ **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Christopher Russo and Shannon Cobb ("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 OP Pharmacy, LLC a/k/a OnePoint Patient Care, LLC ("OnePoint" or "Defendant") based on personal knowledge and the investigation of counsel, and alleges as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard Plaintiffs' and other similarly situated individuals' ("Class Members," as defined *infra*) personally identifying information ("PII") and personal health information ("PHI").

2. OnePoint is a hospice-dedicated pharmacy and pharmacy benefits manager (PBM) headquartered in Kentucky.

3. On August 8, 2024, OnePoint detected suspicious activity on its computer network, indicating a data breach. Based on a subsequent forensic investigation, OnePoint determined that cybercriminals infiltrated its inadequately secured computer environment and thereby gained access to its data files (the "Data Breach" or "Breach").[1] Subsequent investigations determined that the Data Breach exposed the personal information of hundreds of thousands of individuals, approximately 528,000 of whom are living.

[1] *Notice of Data Security Incident*, OnePoint (Oct. 14, 2024), https://www.oppc.com/data-security-incident/.

4. According to OnePoint, the personal information accessed by cybercriminals involved a wide variety of PII and PHI, including names, dates of birth, addresses, Social Security numbers, medical treatment information, and prescription information (collectively, "Private Information").[2]

5. Defendant began sending out notice letters to its customers, stating that Defendant learned of the data breach on August 8, 2024. The letter indicates that, on August 15, 2024, Defendant learned that an unauthorized third party acquired some information from its network between August 6 and August 8, 2024.

6. As part of its business, and in order to gain profits, Defendant obtained and stored the Private Information of Plaintiffs and Class Members.

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

8. Defendant breached this duty and betrayed the trust of Plaintiffs and Class Members by failing to adequately protect Plaintiffs' and Class Members' Private Information—and failing to even encrypt or redact this highly sensitive information. This unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect its customers' sensitive data. Hackers targeted and obtained Plaintiffs' and Class Members' Private Information because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

9. Plaintiffs bring this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiffs and Class Members; (ii) adequately vet its data security practices; (iii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; and (iv) effectively secure hardware containing protected Private Information using reasonable and effective security

[2] *Notice of Data Security Incident*, *supra* at fn. 1

procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal law.

10. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to ensure that Defendant had adequate and reasonable safeguards and measures in place to protect the Private Information of Plaintiffs and Class Members after that information was transferred and entrusted to it in the regular course of business.

11. More specifically, Defendant failed to take and implement available steps to prevent an unauthorized disclosure of data, and failed to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption, storage, and destruction of data, even for internal use. As a result, the Private Information of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third parties.

12. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe and they should be entitled to injunctive and other equitable relief.

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

14. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) an increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's custody, control, or possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

15. Plaintiffs and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose Private Information was compromised and stolen as a result of the Data Breach and who remain at risk

due to Defendant's inadequate data security practices.

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

II. PARTIES

17. Plaintiff Christopher Russo is a citizen and resident of Arizona.

18. Plaintiff Shannon Cobb is a citizen and resident of McHenry, Illinois.

19. Defendant 16. OP Pharmacy, LLC a/k/a OnePoint Patient Care, LLC is an Arizona Limited Liability Company that has its principal place of business in Louisville, Kentucky located at 805 No. Whittington Pkwy., Suite 400. Upon information and belief, the membership of OnePoint is comprised of citizens and entities located in Kentucky.

III. JURISDICTION AND VENUE

20. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, (2) the action is a class action, (3) there are Class Members who are diverse from Defendant, and (4) there are more than 100 Class Members.

21. The Court has general personal jurisdiction over Defendant because Defendant has its principal place of business in this District.

22. Venue is likewise proper as to Defendant in this District under 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is in this District and/or have members who reside in this District, and therefore Defendant resides in this District pursuant to 28 U.S.C. § 1391(c)(2). Venue is further proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the Class's claims also occurred in this District.

IV. FACTUAL ALLEGATIONS

A. *Defendant's Business*

23. Defendant serves as a comprehensive pharmacy services partner, and states it is "the nation's premier hospice PBM and pharmacy."[3]

24. In the regular course of their business, Defendant collects highly private Private Information from its customers and other individuals who interact or otherwise transact with Defendant for business purposes. Defendant stores this highly sensitive information digitally.

25. Defendant promises it is committed to protecting the confidentiality, integrity, and availability of its customers' Private Information. Defendant represents to its customers (including Plaintiffs and Class Members) that it will employ adequate data security.

26. The Privacy Policy available on Defendant's website describes the type of sensitive information it collects as part of its business. The Privacy Policy covers how the medical information it receives from patients can be used and disclosed.[4] The Privacy Policy states:

> "We are committed to protecting privacy of your medical information. While you receive pharmacy services from us, we create records of the pharmacy services that we provide to you. We need these records to provide you with quality pharmacy services and to comply with law."[5]

27. Defendant, via its Privacy Policy, explicitly represents that it is required by law (including but not limited to HIPAA) to maintain the privacy and security of individuals' medical information and to provide individuals with notice if a breach occurs that may have compromised the privacy or security of that medical information.[6]

28. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to third parties. Defendant had a legal duty to keep its customers' Private Information safe and confidential.

---

[3] *About Us*, OnePoint, https://www.oppc.com/about-us/ (last visited Nov. 19, 2024).

[4] *Privacy Policy*, OnePoint, https://www.oppc.com/privacy-policy/ (last visited Nov. 19, 2024).

[5] *Id.*

[6] *Id.*

29. Defendant had obligations created by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

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

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

B. *The Data Breach*

32. According to the Notice of Data Breach Incident published on Defendant's website on or about October 14, 2024, Defendant learned of the Data Breach on or around August 8, 2024.[7]

33. Upon learning about the data breach incident, Defendant initiated an internal investigation and attempted to take steps to contain the cyber-attack. On or about August 15, 2024, Defendant learned that, between August 6 and 8, 2024, "someone obtained some individuals' personal information from [Defendant's] systems without authorization."[8]

34. The cybercriminals responsible for the Data Breach accessed and removed files containing the Private Information of Plaintiffs and Class Members, including customer names, residence information, medical record number, diagnosis and prescription information, and Social Security numbers.[9]

35. Despite knowing about the breach as early as August 8, 2024, Defendant did not post a notice of the Data Breach to its website until approximately October 14, 2024. This inexplicable delay further exacerbated the harms to Plaintiffs and Class Members.

---

[7] *Notice of Data Security Incident, supra,* n.1.

[8] *Id.*

[9] *Id.*

36. 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 Private Information. Nor did Defendant take the precautions and measures needed to ensure Defendant's data security protocols were sufficient to protect the Private Information in its custody, control, or possession.

37. As a result, the third-party accessed and acquired files containing unencrypted Private Information of Plaintiffs and Class Members.

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

39. Defendant's failure to promptly notify Plaintiffs and Class Members that their Private Information was accessed and stolen virtually ensured that the unauthorized third parties who exploited those security lapses could monetize, misuse, or disseminate that Private Information before 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.

40. In fact, the ransomware group INC Ransom has already claimed credit for the breach, "claiming on its dark web leak site to have encrypted and exfiltrated OPPC data in September."[10]

41. Plaintiffs further believe their Private Information, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals like INC Ransom that commit cyberattacks of this type.

[10] *Breach Roundup, supra,* n.3

C. *Defendant Acquires, Collects, and Stores Plaintiffs' and Class Members' Private Information*

42. Defendant derives a substantial economic benefit from providing services to its customers, and as a part of providing those services, Defendant retains and stores the Private Information of its customers and of other individuals who interact or otherwise transact with Defendant for business purposes, including that of Plaintiffs and Class Members.

43. By obtaining, collecting, and storing the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting the Private Information from disclosure.

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

45. Plaintiffs and Class Members relied on Defendant to keep their Private Information confidential and maintained securely, to use this information for business purposes only, to provide the information only to trusted and secure vendors and other third parties, and to make only authorized disclosures of this information.

46. Defendant could have prevented this Data Breach by properly securing the Private Information of Plaintiffs and Class Members.

47. Through its Privacy Policy, Defendant made promises to consumers to maintain and protect Private Information, demonstrating an understanding of the importance of securing Private Information.

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

D. *Defendant Knew or Should Have Known of the Risk Because Institutions in Possession of Private Information Are Particularly Susceptible to Cyberattacks*

49. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches targeting institutions that collect and store Private Information, like Defendant, preceding the date of the Data Breach.

50. 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,[11] Yahoo,[12] Marriott International,[13] Chipotle, Chili's, Arby's,[14] and others.[15]

51. Data thieves regularly target companies that receive and maintain Private Information due to the highly sensitive nature of that information in their custody. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

52. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[16]

53. In light of recent high profile data breaches at other industry leading companies, including Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known the Private Information it collected and maintained would be targeted by cybercriminals.

---

[11] 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/.

[12] 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.

[13] 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/.

[14] 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.

[15] *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.

[16] 2021 Data Breach Annual Report, Identity Theft Resource Center (Jan. 2022), https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf.

54. Further, cybercriminals seek out private health information at a greater rate than other sources of personal information. In a 2024 report, the healthcare compliance company Protenus found that there were 1,161 medical data breaches in 2023 with over 171 million patient records exposed.[17] This is an increase from the 1,138 medical data breaches which exposed approximately 59 million records that Protenus compiled in 2023.[18]

55. Private Information is a valuable property right.[19] The value of Private Information as a commodity is measurable.[20] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[21] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[22] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

56. As a result of the real and significant value of these data, identity thieves and other cybercriminals have openly posted credit card numbers, Social Security numbers, Private Information, and other sensitive information directly on various internet websites, making the information publicly available. This information from various breaches, including the

[17] *2024 Breach Barometer*, Protenus - Industry Report, https://protenus.com/hubfs/Breach_Barometer/Latest%20Version/Protenus%20-%20Industry%20Report%20-%20Privacy%20-%20Breach%20Barometer%20-%202024.pdf (last visited Nov. 19, 2024).

[18] *Id*.

[19] Marc van Lieshout, *The Value of Personal Data*, ResearchGate (May 2015) https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data, ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible[.]").

[20] Robert Lowes, *Stolen EHR Charts Sell for $50 Each on Black Market*, Medscape (April 28, 2014), http://www.medscape.com/viewarticle/824192.

[21] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD iLibrary (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[22] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, Interactive Advertising Bureau (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

information exposed in the Data Breach, can be readily aggregated with other such data and become more valuable to thieves and more damaging to victims.

57. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[23] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[24]

58. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security numbers, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[25] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[26]

59. Criminals can use stolen Private Information to extort a financial payment by "leveraging details specific to a disease or terminal illness."[27] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[28]

---

[23] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HealthTech Magazine (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[24] *Id.*

[25] Adam Greenberg, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC Media (July 16, 2013), https://www.scworld.com/news/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

[26] *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain,* FBI Cyber Division (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[27] Steger, *supra* note 19.

[28] *Id.*

60. Consumers place a high value on the privacy of their data, as they should. Researchers shed light on how much consumers value their data privacy—and the figure is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[29]

61. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Private Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

62. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

63. Defendant was, or should have been, fully aware of the unique type and the significant volume of data it collected and maintained and, thus, the significant number of individuals who would be harmed by the exposure of that data.

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

65. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members, and Defendant's failure to adequately vet its vendors.

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

---

[29] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*: *An Experimental Study*, Information Systems Research (June 2011), https://www.jstor.org/stable/23015560?seq=1.

67. Upon information and belief, the data has been made available for sale on the dark web by a known Ransomware group INC Ransom, who took credit for the cyberattack in September.

E. *Value of Personally Identifiable Information*

68. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[30] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[31]

69. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[32]

70. For example, PII can be sold at a price ranging from $40 to $200.[33] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[34]

71. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, payment 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—names and Social Security numbers—is impossible to "close" and difficult, if not impossible, to change.

---

[30] 17 C.F.R. § 248.201 (2016).
[31] *Id.*
[32] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.
[33] Brian Stack, *Here's How Much Your Private Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.
[34] *In the Dark*, VPNOverview.com, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 8, 2024).

72. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[35]

73. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing, or even give false information to police.

74. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in 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.[36]

F. *Defendant Failed to Comply with FTC Guidelines*

75. The FTC has promulgated numerous guides for businesses which 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.

76. In October 2016, the FTC updated its publication, *Protecting Private Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection

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

[36] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extend Is Unknown*, U.S. Gov't Accountability Off. (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last visited Nov. 19, 2024).

system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into 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.

77. 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.

78. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer 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.

79. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its data security practices, and those of its vendors. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

80. Defendant was at all times fully aware of its obligation to protect the Private Information it was entrusted with, yet failed to comply with such obligation. Defendant was also aware of the significant repercussions that would result from its failure to do so.

G. *Defendant Failed to Comply with Industry Standards*

81. As noted above, experts studying cybersecurity routinely identify institutions like Defendant as being particularly vulnerable to cyberattacks because of the value of the Private Information which it collects and maintains.

82. Some industry best practices that should be implemented by institutions dealing with sensitive Private 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 these industry best practices.

83. Other best cybersecurity practices that are standard at large institutions that store Private Information 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.

84. Defendant failed to meet the minimum standards of, e.g., the NIST Cybersecurity Framework, and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established industry standards in reasonable cybersecurity readiness.

85. These foregoing frameworks are existing and applicable industry standards in the corporate sector and Defendant failed to comply with these accepted standards, thereby opening the door to cybercriminals and causing the Data Breach.

86. Despite Defendant's obligations, Defendant failed to appropriately monitor and maintain its data security systems in a meaningful way so as to prevent the Data Breach.

87. Had Defendant properly maintained its systems and adequately protected them, it could have prevented the Data Breach.

H. *Defendant Breached Its Duties to Safeguard Plaintiffs' and Class Members' Private Information*

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

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

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

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

92. Defendant breached its obligations to Plaintiffs and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard its computer systems and data and failed to audit, monitor, or ensure the integrity of its data security practices. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect customers' and other related individuals' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

e. Failing to adhere to industry standards for cybersecurity as discussed above; and

f. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

93. Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

94. Defendant also 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).

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

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

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

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

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

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

101. Had Defendant remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

I. *Common Injuries & Damages*

102. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages,

including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of the value of their Private Information; (e) invasion of privacy; and (f) the continued risk to their Private 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 Plaintiffs' and Class Members' Private Information.

103. 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' Private Information.

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

J. *The Data Breach Increases Victims' Risk of Identity Theft*

105. Due to the Data Breach, Plaintiffs and Class Members are at a heightened risk of identity theft for years to come.

106. The unencrypted Private Information of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers, such as the ransomware group who took credit for this Data Breach. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class Members.

107. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft-related crimes

discussed below.

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

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

110. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[37]

111. With "Fullz" packages, cybercriminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

112. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, driver's license numbers, and other unregulated sources and

[37] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, Social Security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, KrebsOnSecurity (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm.

identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

113. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that almost 20% of victims of identity misuse needed more than a month to resolve issues stemming from identity theft.[38]

114. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[39] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[40] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use Private Information "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [41] The FTC also warns, "If the thief's health information is mixed with yours it could affect the medical care you're able to get or the health insurance benefits you're able to use."[42]

115. A report published by the World Privacy Forum and presented at the U.S. FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

---

[38] *2023 Consumer Impact Report*, Identity Theft Resource Center (2023), https://www.idtheftcenter.org/publication/2023-consumer-impact-report/ (last visited Nov. 19, 2024).

[39] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, World Privacy Forum (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.

[40] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk . . .*, *supra* note 21.

[41] *What to Know About Medical Identity Theft*, Federal Trade Commission Consumer Advice (May 2021), https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited Nov. 19, 2024).

[42] *Id*.

a. Changes to their healthcare records, most often the addition of falsified information through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.

b. Significant bills for medical goods and services neither sought nor received.

c. Issues with insurance, co-pays, and insurance caps.

d. Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.

e. Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

f. As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.

g. Phantom medical debt collection based on medical billing or other identity information.

h. Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own. [43]

116. There may also be time lags between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. On average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[44]

[43] *See* Dixon and Emerson, *supra* note 35.

[44] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, Journal of Systemics, Cybernetics and Informatics (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

117. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[45] For example, with the Private Information stolen in the Data Breach, identity thieves can open financial accounts, apply for credit, collect government benefits, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[46] These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class Members.

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

119. It is within this context that Plaintiffs and all other Class Members must now live with the knowledge that their Private Information is forever in cyberspace and was taken by someone intending to use that information for any number of improper purposes and scams, including making the information available for sale on the black-market.

K. *The Data Breach was Preventable*

120. Data breaches are preventable.[47] 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."[48] she added that "[o]rganizations that collect, use, store, and share sensitive personal

[45]"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").

[46] https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/.

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

[48]*Id.* at 17.

data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[49]

121. "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*."[50]

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

L. *Loss of Time to Mitigate Risk of Identity Theft and Fraud*

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

124. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and re-securing their own computer networks; and checking their financial accounts for any indication of fraudulent activity, which may take years to detect.

125. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches in which it noted that victims of identity theft

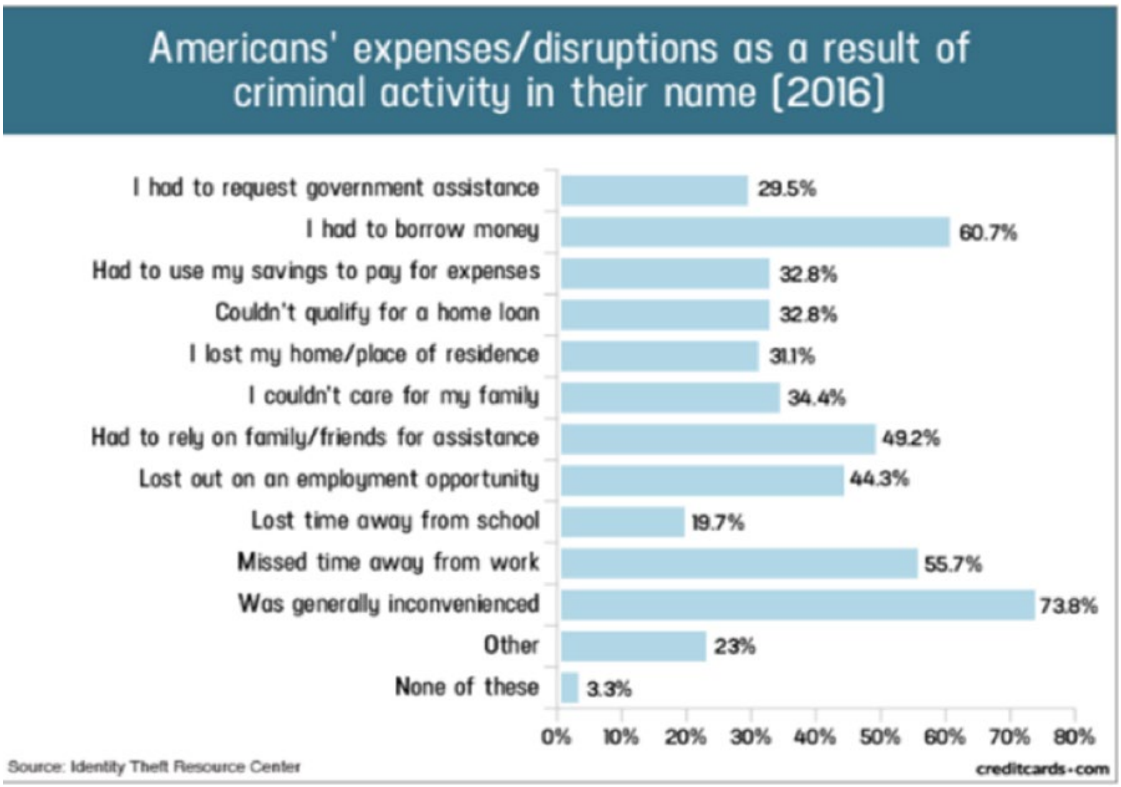
[49] *Id.* at 28.

[50] *Id.*

will face "substantial costs and time to repair the damage to their good name and credit record."[51]

126. These efforts are also consistent with the steps the FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[52]

127. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:



M. *Diminution of Value of Private Information*

128. Private Information is a valuable property right. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyberthefts include heavy

[51] *See* U.S. Gov't Accountability Office, *supra* note 32.
[52] *What To Do Right Away,* Federal Trade Commission, IdentityTheft.gov, https://www.identitytheft.gov/Steps (last visited Nov. 19, 2024).

prison sentences. Even this obvious risk-to-reward analysis illustrates beyond a doubt that Private Information has considerable market value.

129. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[53]

130. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[54]

131. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[55]

132. Conversely, sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[56]

133. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

N. *Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary*

134. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchased by criminals intending to utilize the Private

[53] David Lazarus, *Shadowy data brokers make the most of their cloak,* Los Angeles Times (Nov. 5, 2019, 5 AM PT), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.
[54] Datacoup, Inc, https://datacoup.com/ (last visited Nov. 19, 2024).
[55] *Frequently Asked Questions*, Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Oct. 8, 2024).
[56] Ashiq JA, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

Information for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; filing false tax returns; taking out loans or lines of credit; or filing false unemployment claims.

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

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

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

O. *Plaintiffs' Experience*

Plaintiff Christopher Russo

138. In exchange for medical services, Plaintiff Christopher Russo ("Plaintiff Russo") entrusted his Private Information to Defendant. Pursuant to HIPAA, OnePoint was required to protect and maintain the confidentiality of Private Information entrusted to it.

139. Plaintiff Russo received a notice letter from Defendant dated October 23, 2024, informing him that his Private Information—including his PII and PHI—was specifically identified as having been exposed to cybercriminals in the Data Breach.

140. Plaintiff Russo is very careful with his personal information.

141. Plaintiff Russo and Class Members' Private Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

142. Because of the Data Breach, Plaintiff Russo's Private Information is now in the hands of cyber criminals. Plaintiff Russo and all Class Members are now imminently at risk of crippling future identity theft and fraud.

143. As a result of the Data Breach, Plaintiff Russo 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 investigating the Data Breach, researching how best to ensure that he is protected from identity theft, reviewing account statements and other information, and taking other steps in an attempt to mitigate the harm caused by the Data Breach.

144. Plaintiff Russo has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of his valuable Private Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by his Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of his Private Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (d) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what he should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect his Private Information; and (e) continued risk to his Private 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 Private Information that was entrusted to Defendant.

Plaintiff Shannon Cobb

145. Plaintiff Shannon Cobb ("Plaintiff Cobb") is a customer of Defendant. Plaintiff Cobb provided Private Information to Defendant in the course of obtaining goods/services from Defendant.

146. Plaintiff Cobb provided Private Information to Defendant and trusted the company would use reasonable measures to protect it according to its policies, as well as state and federal

law. Defendant obtained and continues to maintain Plaintiff Cobb's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

147. At the time of the Data Breach, Defendant collected and retained Plaintiff Cobb's and Class Members' Private Information in its systems.

148. Plaintiff Cobb's and Class Members' Private Information was compromised in the Data Breach and stolen by cybercriminals.

149. Plaintiff Cobb has been injured by the compromise of her Private Information.

150. Plaintiff Cobb takes reasonable measures to protect her Private Information. Plaintiff Cobb has never knowingly transmitted unencrypted Private Information over the internet or other unsecured source.

151. Plaintiff Cobb stores any documents containing Private Information in a safe and secure location and diligently chooses unique usernames and passwords for online accounts.

152. Had Plaintiff Cobb known that Defendant does not adequately protect Private Information, she would not have agreed to provide sensitive Private Information to Defendant and would not have agreed to be a customer of Defendant.

153. As a result of and following the Data Breach, Plaintiff Cobb has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach to protect herself from identity theft and fraud. Plaintiff Cobb has monitored, and continues to monitor, accounts, credit reports and credit scores, and has sustained emotional distress. This is time that was lost and unproductive and took away from other activities and duties.

154. Plaintiff Cobb suffered lost time, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy.

155. Plaintiff Cobb has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals that will continue for her lifetime.

156. Defendant obtained and continues to maintain Plaintiff Cobb's Private Information, and thus has a continuing legal duty and obligation to protect that Private Information from

unauthorized access and disclosure. Plaintiff Cobb's Private Information was compromised and disclosed as a result of the Data Breach.

157. As a result of the Data Breach, Plaintiff Cobb anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, she is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

158. Further, Plaintiff Cobb is and will remain at risk of harm in the future because Defendant continues to maintain her confidential Private Information but does not take adequate steps to protect that information from a data breach. Accordingly, her Private Information faces an imminent risk of disclosure in a future Defendant data breach.

V. CLASS ALLEGATIONS

159. Pursuant to Federal Rule of Civil Procedure 23, Plaintiffs seek certification of the following class (the "Class"):

> **Nationwide Class**
> All living individuals residing in the United States whose Private Information was disclosed in the Data Incident, including all living persons who were sent a notice of the Data Incident by Defendant.

160. Excluded from the Settlement Class are all persons who are: (a) directors and officers of Defendant; and (b) the Judge assigned to the Action, that Judge's immediate family, and Court staff.

161. Plaintiffs reserve the right to modify or amend the definition of the proposed Class, as well as to add subclasses, before the Court determines whether certification is appropriate.

162. The proposed Class meets the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3).

163. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiffs believe the proposed Class includes approximately 528,000 individuals who have been damaged by Defendant's conduct as alleged herein. The precise number of Class Members is unknown to Plaintiffs but may be ascertained from Defendant's records.

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

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant's conduct violated the FTCA;

c. When Defendant learned of the Data Breach;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

e. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

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

g. Whether Defendant owed duties to Class Members to safeguard their Private Information;

h. Whether Defendant breached its duties to Class Members to safeguard their Private Information;

i. Whether hackers obtained Class Members' Private Information via the Data Breach;

j. Whether Defendant had legal duties to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

k. Whether Defendant breached its duties to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

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

m. What damages Plaintiffs and Class Members suffered as a result of Defendant's misconduct;

n. Whether Defendant's conduct was negligent;

o. Whether Defendant breached implied contracts with Plaintiffs and Class Members;

p. Whether Defendant was unjustly enriched;

q. Whether Plaintiffs and Class Members are entitled to damages;

r. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

s. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

165. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through Defendant's common misconduct. Plaintiffs are advancing the same claims and legal theories on behalf of himself and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

166. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel are competent and experienced in litigating class actions, including data privacy litigation of this kind.

167. Predominance. Defendant has engaged in common courses of conduct toward Plaintiffs and Class Members. For example, all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated 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.

168. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is

superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

169. Class certification is also appropriate under Federal Rule of Civil Procedure 23(b)(2). Defendant has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

170. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names, email and/or postal addresses, and phone numbers of Class Members affected by the Data Breach.

CLAIMS FOR RELIEF

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

171. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

172. Defendant solicited, gathered, and stored the Private Information of Plaintiffs and the Class as part of the operation of its business.

173. Upon accepting and storing the Private Information of Plaintiffs and Class Members, Defendant undertook and owed a duty to Plaintiffs and Class Members to exercise reasonable care to secure and safeguard that information and to use secure methods to do so.

174. Defendant had full knowledge of the sensitivity of the Private Information, the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information was wrongfully disclosed, and the importance of adequate security.

175. Defendant knew the risks of collecting and storing Plaintiffs' and all other Class Members' Private Information and the importance of maintaining secure systems. Defendant knew of the many data breaches that targeted healthcare providers in recent years.

176. Given the nature of Defendant's business, the sensitivity and value of the Private Information it maintains, and the resources at its disposal, Defendant should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

177. Defendant owed Plaintiffs and the Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard such data and providing notification to Plaintiffs and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

178. Defendant had duties to protect and safeguard the Private Information of Plaintiffs and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive Private Information. Additional duties that Defendant owed Plaintiffs and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, email accounts, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class Members' Private Information was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiffs' and Class Members' Private Information in its possession by using reasonable and adequate security procedures and systems;

c. To implement processes to quickly detect a data breach, security incident, or intrusion involving its business email system, networks and servers; and

d. To promptly notify Plaintiffs and Class Members of any data breach, security incident, or intrusion that affected or may have affected their Private Information.

179. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the Private Information that Plaintiffs and the Class had entrusted to it.

180. Defendant breached its duty of care by failing to adequately protect Plaintiffs' and Class Members' Private Information. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the Private Information in its possession;

b. Failing to protect the Private Information in its possession by using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train its employees to avoid phishing emails;

d. Failing to use adequate email security systems, including healthcare industry standard SPAM filters, DMARC enforcement, and/or Sender Policy Framework enforcement to protect against phishing emails;

e. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Private Information;

f. Failing to adequately train its employees to not store Private Information longer than absolutely necessary for the specific purpose that it was sent or received;

g. Failing to consistently enforce security policies aimed at protecting Plaintiffs' and the Class's Private Information;

h. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and

i. Failing to promptly notify Plaintiffs and Class Members of the Data Breach that affected their Private Information.

181. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class Members' Private Information to unauthorized individuals.

182. But for Defendant's negligent conduct or breach of the above-described duties

owed to Plaintiffs and Class Members, their Private Information would not have been compromised.

183. As a result of Defendant's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Private Information; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their Private Information which remains in Defendant's possession; and (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Private Information compromised as a result of the Data Breach.

COUNT II
Negligence Per Se
(On Behalf of Plaintiffs and the Class)

184. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

185. In addition to its duties under common law, Defendant had additional duties imposed by statute and regulations, including the duties under the FTC Act. The harms which occurred as a result of Defendant's failure to observe these duties, including the loss of privacy, lost time and expense, and significant risk of identity theft are the types of harm that these statutes and regulations intended to prevent.

186. Defendant's duties arise from, *inter alia*, Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendant, of failing to employ reasonable measures to protect and secure Private Information.

187. Defendant violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiffs' and all other Class Members' Private Information and not complying with

applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtains and stores, and the foreseeable consequences of a data breach involving Private Information including, specifically, the substantial damages that would result to Plaintiffs and the other Class Members.

188. Defendant's violations of Section 5 of the FTCA constitutes negligence per se.

189. Plaintiffs and Class Members are within the class of persons that Section 5 of the FTCA were intended to protect.

190. The harm occurring as a result of the Data Breach is the type of harm Section 5 of the FTCA was intended to guard against.

191. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiffs' and Class Members' Private Information to unauthorized individuals.

192. The injury and harm that Plaintiffs and the other Class Members suffered was the direct and proximate result of Defendant's violations of law, including Section 5 of the FTCA. Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Private Information; (iii) breach of the confidentiality of their Private Information; (iv) deprivation of the value of their Private Information, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) actual or attempted fraud.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

193. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

167. Defendant offered to provide services to its customers, including Plaintiffs and Class Members, in exchange for payment.

168. Defendant also required Plaintiffs and Class Members to provide it with their Private Information in order to receive services.

169. In turn, Defendant impliedly promised to protect Plaintiffs' and Class Members' Private Information through adequate data security measures.

170. Plaintiffs and Class Members accepted Defendant's offer by providing their valuable Private Information to Defendant in exchange for Plaintiffs and Class Members receiving Defendant's services, and then by paying for and receiving the same.

171. Plaintiffs and Class Members would not have done the foregoing but for the above-described agreement with the company.

172. A meeting of the minds occurred when Plaintiffs and Class Members agreed to, and did, provide their Private Information to Defendant in exchange for, amongst other things, the protection of such information.

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

174. However, Defendant breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect their Private Information and by failing to provide timely and accurate notice to them that their Private Information was compromised as a result of the Data Breach.

175. In sum, Plaintiffs and Class Members have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

176. As a reasonably foreseeable result of the Data Breach, Plaintiffs and Class Members were harmed by Defendant's failure to use reasonable data security measures to store their Private

Information, including but not limited to, the actual harm through the loss of their Private Information to cybercriminals.

177. Accordingly, Plaintiffs and Class Members are entitled to damages in an amount to be determined at trial, along with their costs and attorneys' fees incurred in this action.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

178. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

179. This count is brought in the alternative to Plaintiffs' breach of implied contract claims.

180. Upon information and belief, Defendant funds their data security measures entirely from its general revenue, including from payments made by or on behalf of its customers, like Plaintiff, for services.

181. As such, a portion of the value and monies derived from payments made by its customers for services 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.

182. Plaintiffs and Class Members conferred a monetary benefit on Defendant in providing it with their valuable Private Information.

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

184. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

185. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profit at the expense of Plaintiffs and

Class Members by utilizing cheaper, ineffective security measures.

186. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profit over the requisite security.

187. Defendant failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their Private Information provided.

188. If Plaintiffs and Class Members knew that OnePoint had not secured their PII, they would not have agreed to disclose their data to OnePoint's clients.

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

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

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

192. Plaintiffs and Class Members have no adequate remedy at law.

193. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) an increase in spam calls, texts, and/or emails; and (vi) the continued and certainly

increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's custody, control, and possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

194. Defendant, upon information and belief, has therefore engaged in opportunistic and unethical conduct by profiting from conduct that it knew would create a significant and highly likely risk of substantial and certainly impending harm to Plaintiffs and the Class in direct violation of Plaintiffs' and Class Members' interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its wrongful conduct.

195. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct.

196. This can be accomplished by establishing a constructive trust from which Plaintiffs and Class Members may seek restitution or compensation.

COUNT V
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiffs and the Class)

197. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

198. Plaintiffs and Class Members provided Defendant their Private Information in confidence, believing that Defendant would protect that information. Plaintiffs and Class Members would not have provided Defendant with this information had they known it would not be adequately protected. Defendant's acceptance and storage of Plaintiffs' and Class Members' Private Information created a fiduciary relationship between Defendant, on the one hand, and Plaintiffs and Class Members, on the other hand. In light of this relationship, Defendant must act

primarily for the benefit of its customers, which includes safeguarding and protecting Plaintiffs' and Class Members' Private Information.

199. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship. Defendant breached that duty by failing to properly protect the integrity of its systems containing Plaintiffs' and Class Members' Private Information, failing to comply with the data security guidelines set forth by FTC and industry standards, and otherwise failing to safeguard Plaintiffs' and Class Members' Private Information that it collected.

200. 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.

201. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Private Information; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their Private Information which remains in Defendant's possession; and (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Private Information compromised as a result of the Data Breach.

COUNT VI
Declaratory and Injunctive Relief, 28 U.S.C. § 2201
(On Behalf of Plaintiffs and the Class)

202. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

203. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C.

§ 2201.

204. Defendant owes a duty of care to Plaintiffs and Class Members that required it to adequately secure their Private Information.

205. Defendant still possesses Plaintiffs' and Class Members' Private Information, yet does not adequately protect Private Information against the threat of a data breach.

206. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and Class Members.

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

208. There is no reason to believe that Defendant's employee training and security measures are any more adequate now than they were before the Data Breach.

209. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing data security measures do not comply with its contractual obligations and duties of care to provide adequate data security, and (2) that to comply with its obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, being ordered as follows:

a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

b. ordering that Defendant engage internal security personnel to conduct testing, including 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;

c. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

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

e. ordering that Defendant audit, test, and train its security personnel and employees regarding any new or modified data security policies and procedures;

f. ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, any Private Information not necessary for its provision of services;

g. ordering that Defendant conduct regular database scanning and security checks; and

h. prohibiting Defendant from maintaining Private Information of Plaintiffs and Class Members on a cloud-based database;

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

j. ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive Private Information;

k. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding paragraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

l. requiring Defendant to meaningfully educate all class members about the threats they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

m. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2

Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

n. such other and further relief as this Court may deem just and proper.

PRAYER FOR RELIEF

WHEREFORE**,** Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court enter an Order:

A. Certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class, pursuant to Federal Rule of Civil Procedure 23;

B. Granting equitable relief and enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class Members;

C. Granting injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members;

D. For an award of actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;

E. For an award of punitive damages, as allowable by law;

F. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;

G. Pre- and post-judgment interest on any amounts awarded; and

H. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

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

Dated: April 18, 2025

Respectfully submitted,

By: */s/ A. Brooke Murphy*

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

Tyler Bean
SIRI GLIMSTAD LLP
101 North Seventh Street, #827
Louisville, KY 40202
Telephone: 772-783-8463
Fax: 646-417-5967

Andrew W. Ferich (admitted *pro hac vice*)
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: (310) 474-9111
Facsimile: (310) 474-8585
aferich@ahdootwolfson.com

Jeff Ostrow (admitted *pro hac vice*)
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd., Suite 500
Fort Lauderdale, FL 33301
Tel: 954-525-4100
ostrow@kolawyers.com

Counsel for Plaintiffs and the Putative Class

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on April 18, 2025, a true and correct copy of the above and foregoing was filed with the Clerk of Court via the Court's CM/ECF system for electronic service on all counsel of record.

/s/ A. Brooke Murphy
A. Brooke Murphy