**UNITED STATES DISTRICT COURT**
**EASTERN DISTRICT OF NEW YORK**

| | | |
|---|---|---|
| DAVID MAYO and MADELEINE E. SCHWARTZ, individually and on behalf of all others similarly situated, | : | Case No. |
| Plaintiffs, | : | |
| v. | : | **CLASS ACTION COMPLAINT** |
| NORTHWELL HEALTH, INC. and PERRY JOHNSON & ASSOCIATES, | : | **JURY TRIAL DEMANDED** |
| Defendants. | : | |

Plaintiffs DAVID MAYO and MADELEINE E. SCHWARTZ ("Plaintiffs") bring this Class Action Complaint ("Complaint") against Defendants NORTHWELL HEALTH, INC. and PERRY JOHNSON & ASSOCIATES ("Northwell" and "PJ&A" or, collectively, "Defendants") individually and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

## INTRODUCTION

1. This Class Action arises from a breach of sensitive information in the possession and custody and/or control of Defendants (the "Data Breach").

2. The Data Breach resulted in the unauthorized disclosure, exfiltration, and theft of consumers' highly personal information, including names, Social Security numbers, dates of service, ("personal identifying information" or "PII"), and clinical test information ("protected health information" or "PHI"). Plaintiffs refers to both PII and PHI collectively as "Sensitive Information."

3. According to a letter received by Plaintiffs from Defendants, the Data Breach occurred between March 27, 2023, and May 2, 2023. Defendants advise they became aware of the Data Breach on May 2, 2023. Accordingly, cybercriminals had unrestricted and unrestrained access to Plaintiffs' and the Class's highly private Sensitive Information for perhaps as much as five weeks. Discovery may reveal that this occurred for a longer period of time.

4. Defendants sent Plaintiffs a letter on November 3, 2023 ("Notice Letter") to inform them of the Data Breach. Thus, Defendants inexplicably waited six months before informing Class Members of the Data Breach, even though Plaintiffs and the Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

5. Defendants' Breach Notice failed to tell their consumers how many people were impacted, how the breach happened, or why it took Defendants nearly two months to begin notifying victims that hackers had gained access to highly private Sensitive Information.

6. News reporting indicates that approximately 3.9 million individuals were impacted by the Data Breach.[1]

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

8. Defendants knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII and PHI misuse.

[1] https://thecyberexpress.com/northwell-health-data-breach-patient-data-leak/ (Last Accessed on November 13, 2023).

9. In failing to adequately protect Plaintiffs' and the Class's Sensitive Information, failing to timely and adequately notify them about the breach, and by obfuscating the nature of the breach, Defendants violated state and federal law and harmed an unknown number of their consumers.

10. Plaintiffs and members of the proposed Class are victims of Defendants' negligence and inadequate cyber security measures and have been damaged as detailed herein.

11. Accordingly, Plaintiffs, individually and on behalf of a class of similarly situated individuals, bring this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendants' possession.

## PARTIES

12. Plaintiff David Mayo is a natural person and citizen of New York, residing in Roslyn, New York, where he intends to remain.

13. Plaintiff Madeleine E. Schwartz is a natural person and citizen of New York, residing in West Hempstead, New York, where she intends to remain.

14. Defendant Northwell Health, Inc. is a nonprofit organization with its principal place of business in New Hyde Park, New York.

15. Defendant Perry Johnson & Associates is a corporation with its principal place of business in Henderson, Nevada.

## JURISDICTION AND VENUE

16. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because Plaintiffs and at least one member of the putative Class, as defined below, are citizens of a different state than Defendants; there are more than 100

putative class members; and, the amount in controversy exceeds $5 million exclusive of interest and costs.

17. This Court has general personal jurisdiction over Defendant Northwell because Defendant Northwell maintains its principal place of business in New Hyde Park, New York, regularly conducts business in New York, and has sufficient minimum contacts in New York.

18. This Court has general personal jurisdiction over Defendant PJ&A because it regularly conducts business in New York and has sufficient minimum contacts in New York.

19. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant Northwell's principal place of business is in this District, and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

## STATEMENT OF FACTS

20. Defendant Northwell is "the largest health system in New York" and consists of "more than 12,000 credentialed physicians, more than 19,000 nurses and more than 5,000 volunteers."[2]

21. Defendant Northwell treats over two million New Yorkers ever year.[3]

22. Defendant PJ&A is a medical vendor which offers medical coding, transcription, and reporting services to medical providers.

23. PJ&A provides transcription and dictation services to Northwell. To perform this work, Northwell provides PJ&A with certain Sensitive Information from its patients.

24. As part of their respective businesses, Defendants receive and maintain the Sensitive Information of thousands of consumers. In doing so, Defendants implicitly promise to

[2] https://www.northwell.edu/about-northwell (Last visited on November 13, 2023).
[3] https://www.northwell.edu/about-northwell (Last visited on November 13, 2023).

safeguard their Sensitive Information.

25. In collecting and maintaining consumers' Sensitive Information, Defendants agree to safeguard the data in accordance with state and federal law.

26. Defendants represent to consumers and the public that they possesses robust security features to protect PII and PHI and that they take their responsibility to protect PII and PHI seriously.

27. Defendant Northwell's website states: "We employ commercially reasonable measures to safeguard the collection, transmission and storage of the information we collect. These measures vary based on the sensitivity of the information that we collect, process and store and the current state of technology. We use software programs to monitor traffic to identify unauthorized attempts to upload or change information or other types of malicious use. Information collected from these sources may be used to help identify an individual in the event of a criminal investigation or as required by any legal process."[4]

28. Defendant PJ&A's website states: "PJ&A recognizes the importance of information security. Comprehensive policies and procedures are used to ensure that all access to patient data is restricted. HIPAA compliance requires an enterprise to implement, maintain and review a variety of controls. The PJ&A platform enables HIPAA compliance through advanced technology for dictation, transcription and patient data accessibility."[5]

29. On information and belief, Defendants have not implemented reasonable cybersecurity safeguards or policies to protect their consumers' Sensitive Information or supervised their IT or data security agents and employees to prevent, detect, and stop breaches of their systems. As a result, Defendants leave significant vulnerabilities in their systems for

[4] https://www.northwell.edu/privacy-policies-disclaimers
[5] https://www.pjats.com/hipaa-compliancy/

cybercriminals to exploit and gain access to consumers' Sensitive Information.

***The Data Breach***

30. Defendants collect and maintain consumers' Sensitive Information in their computer systems.

31. On or about May 2, 2023, Defendant PJ&A became aware that its network may have been breached.

32. Following a forensic investigation, PJ&A discovered that cybercriminals had—between March 27, 2023, and May 2, 2023—accessed a set of electronically stored personal information stored on their network.

33. Specifically, cybercriminals obtained access to Northwell patient data between April 7, 2023, and April 19, 2023.

34. Defendants' Breach Notice admits that Plaintiffs' and Class Members' Sensitive Information was accessed without authorization.

35. The compromised Sensitive Information includes names, Social Security numbers, dates of birth, addresses, medical record numbers, hospital account numbers, admission diagnoses, and dates and times of service.

36. In collecting and maintaining Sensitive Information, Defendants implicitly agree that they will safeguard the data using reasonable means according to their internal policies, as well as state and federal law.

37. Defendants' investigation revealed that their cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of thousands of their consumers' highly private Sensitive Information.

38. On November 3, 2023, more than seven months after the Breach first occurred,

and six months after Defendants first learned of the Breach, Defendants finally began notifying Plaintiffs and Class Members about the Data Breach.

39. Through their Breach Notice, Defendants recognized the actual imminent harm and injury that flowed from the Data Breach, so they encouraged breach victims to remain vigilant for incidents of fraud or identity theft by reviewing their account statements and free credit reports for any unauthorized activity.

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

***The Data Breach Was a Foreseeable Risk of which Defendants Were on Notice.***

41. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry and healthcare adjacent industry preceding the date of the breach.

42. In light of recent high profile data breaches at other healthcare partner and provider companies, Defendants knew or should have known that their electronic records and consumers' Sensitive Information would be targeted by cybercriminals.

43. Cyberattacks on medical systems and healthcare partner and provider companies like Defendants have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because

they often have lesser IT defenses and a high incentive to regain access to their data quickly."[6]

44. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendants.

***Plaintiff Mayo's Experience***

45. As a requisite to receiving medical services from Defendants, Plaintiff provided his Sensitive Information to Defendants and trusted that the information would be safeguarded according to state and federal law. Upon receipt, Sensitive Information was entered and stored in Defendants' network and systems.

46. Plaintiff is very careful about sharing his Sensitive Information, and he has never knowingly transmitted unencrypted Sensitive Information.

47. Plaintiff stores any documents containing his Sensitive Information in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts. Had he known Defendants failed to follow basic industry security standards and failed to implement systems to protect his Sensitive Information, he would not have provided that information to Defendants.

48. The Breach Notice dated November 3, 2023, from Defendants notified Plaintiff that their network had been accessed and Plaintiff's Sensitive Information was involved in the Data Breach, which included Plaintiff's name, date of birth, address, medical record number, hospital account number and medical treatment information such as the name of treatment facility, name of healthcare providers, admission diagnosis and dates of service.

49. Plaintiff has spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his

[6] Secret Service Warn of Targeted, Law360, https://www.law360.com/articles/1220974/fbi-secret-service-warn-of- targeted-ransomware (last visited November 13, 2023).

accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Moreover, this time was spent at Defendants' direction by way of the Data Breach notice where Defendants advised Plaintiff to mitigate his damages by, among other things, reviewing his healthcare statements for accuracy.

50. Even with the best response, the harm caused to Plaintiff cannot be undone.

51. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Sensitive Information—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

52. He also lost his benefit of the bargain by paying for medical services that failed to provide the data security that was promised.

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

54. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from his Sensitive Information being placed in the hands of unauthorized third parties and possibly criminals.

55. Future identity theft monitoring is reasonable and necessary and such services will include future costs and expenses.

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

***Plaintiff Schwartz's Experience***

57. As a requisite to receiving medical services from Defendants, Plaintiff provided her Sensitive Information to Defendants and trusted that the information would be safeguarded

according to state and federal law. Upon receipt, Sensitive Information was entered and stored in Defendants' network and systems.

58. Plaintiff is very careful about sharing her Sensitive Information, and she has never knowingly transmitted unencrypted Sensitive Information.

59. Plaintiff stores any documents containing her Sensitive Information in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for her various online accounts. Had she known Defendants failed to follow basic industry security standards and failed to implement systems to protect her Sensitive Information, she would not have provided that information to Defendants.

60. The Breach Notice dated November 3, 2023, from Defendants notified Plaintiff that their network had been accessed and Plaintiff's Sensitive Information was involved in the Data Breach, which included Plaintiff's name, date of birth, address, medical record number, hospital account number and medical treatment information such as the name of treatment facility, name of healthcare providers, admission diagnosis and dates of service.

61. Plaintiff has spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Moreover, this time was spent at Defendants' direction by way of the Data Breach notice where Defendants advised Plaintiff to mitigate her damages by, among other things, reviewing her healthcare statements for accuracy.

62. Even with the best response, the harm caused to Plaintiff cannot be undone.

63. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Sensitive Information—a form of intangible property that Plaintiff

entrusted to Defendants, which was compromised in and as a result of the Data Breach.

64. She also lost her benefit of the bargain by paying for medical services that failed to provide the data security that was promised.

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

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

67. Future identity theft monitoring is reasonable and necessary and such services will include future costs and expenses.

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

***The Value of PII and PHI***

69. It is well known that PII and PHI, and social security numbers and financial account information in particular, is an invaluable commodity and a frequent target of hackers.

70. According to Javelin Strategy & Research, in 2017 alone over 16.7 million individuals were affected by identity theft, causing $16.8 billion to be stolen.[7]

71. People place a high value not only on their PII and PHI, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.[8]

[7] Javelin Strategy & Research, *Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study* (Feb. 6, 2018), https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin.

[8] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*,

72. People are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as your DNA to hackers."[9] There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiffs and Class members cannot obtain new numbers unless they become a victim of social security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems . . . and won't guarantee . . . a fresh start."[10]

73. The PII and PHI 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. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[11] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[12] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[13]

74. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an

https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141444.pdf.

[9] Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, Kiplinger, (Feb. 10, 2015), https://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html.

[10] Social Security Admin., *Identity Theft and Your Social Security Number*, at 6-7, https://www.ssa.gov/pubs/EN-05-10064.pdf.

[11] *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/.

[12] *Here's How Much Your Personal 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/.

[13] *In the Dark*, VPNOverview, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[14]

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

76. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[15]

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

[14] Social Security Administration, *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf.
[15] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft.

change.

78. 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 and Social Security numbers are worth more than 10x on the black market."[16]

79. 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.

80. The fraudulent activity resulting from the Data Breach may not come to light for years.

81. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII and PHI is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), 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.[17]

82. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII and PHI of Plaintiffs and Class members, including Social Security numbers, and of the foreseeable consequences that would occur if their data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class members as a result of a breach.

---

[16] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT 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.

[17] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

83. Plaintiffs and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and Class members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

84. Defendant was, or should have been, fully aware of the unique type and the significant volume of data contained in the PII and PHI that Defendant stored unencrypted, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

85. 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 PII and PHI of Plaintiffs and Class members.

***Defendants Failed to Comply with Industry Standards***

86. In light of the numerous high-profile data breaches targeting companies like Target, Neiman Marcus, eBay, Anthem, Deloitte, Equifax, Marriott, T-Mobile, and Capital One, Defendant is, or reasonably should have been, aware of the importance of safeguarding PII and PHI, as well as of the foreseeable consequences of its systems being breached.

87. Security standards commonly accepted among businesses that store PII and PHI using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Monitoring for suspicious or irregular traffic to servers;

c. Monitoring for suspicious credentials used to access servers;

d. Monitoring for suspicious or irregular activity by known users;

e. Monitoring for suspicious or unknown users;

f. Monitoring for suspicious or irregular server requests;

g. Monitoring for server requests for PII and PHI;

h. Monitoring for server requests from VPNs; and

i. Monitoring for server requests from Tor exit nodes.

88. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendants failed to follow these cybersecurity best practices, including failure to train staff.

89. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[18] and protection of PII and PHI[19] which includes basic security standards applicable to all types of businesses.

90. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

[18] Start with Security: A Guide for Business, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[19] Protecting Personal Information: A Guide for Business, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting personalinformation.pdf.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hacker attacks.

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

91. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[20]

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

[20] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

93. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

94. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees.

95. Upon information and belief, Defendants failed to comply with at least one––or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

96. Because Defendant was entrusted with PII and PHI, they had, and have, a duty to keep the PII and PHI secure.

97. Plaintiffs and Class members reasonably expect that when their PII and PHI is provided to a sophisticated business for a specific purpose, that business will safeguard their PII and PHI and use it only for that purpose.

98. Nonetheless, Defendant failed to prevent the Data Breach. Had Defendant properly maintained and adequately protected its systems, it could have prevented the Data Breach.

***Defendants Failed to Adhere to FTC guidelines.***

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

a. protect the sensitive consumer information that they keep;

b. properly dispose of Sensitive Information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

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

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

102. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

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

***Defendants Violated HIPAA***

104. HIPAA circumscribes security provisions and data privacy responsibilities

designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[21]

105. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[22]

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

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

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

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

d. Failing to ensure compliance with HIPAA security standards by Defendants in

[21] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, inter alia: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

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

violation of 45 C.F.R. § 164.306(a)(4);

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

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

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

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

107. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendants failed to comply with safeguards mandated by HIPAA regulations.

***Plaintiffs and the Proposed Class Have Been Injured***

108. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their Sensitive Information that can be directly traced to Defendants.

109. As a result of Defendants carelessness, recklessness, negligence and inadequacy, Plaintiffs' and Class Members' Sensitive Information has been compromised and they now face an ongoing risk of identity theft, which is heightened here by the loss of Social Security numbers – the gold standard for identity thieves. The exposed Sensitive Information of Plaintiffs and Class Members can, and likely will, be sold repeatedly on the dark web.

110. In addition to the ongoing risk of identity theft, those impacted by the Data Breach have suffered numerous actual and concrete injuries and damages, including:

a. invasion of privacy;

b. financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft;

c. loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk;

d. financial "out of pocket" costs incurred due to actual identity theft;

e. loss of time incurred due to actual identity theft;

f. loss of time due to increased spam and targeted marketing emails;

g. the loss of benefit of the bargain (price premium damages);

h. diminution of value of their Sensitive Information;

i. anxiety, annoyance and nuisance, and

j. the continued risk to their Sensitive Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Sensitive Information.

k. The loss of the opportunity to control how their Sensitive Information is used;

l. The compromise and continuing publication of their Sensitive Information;

m. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; and

n. Delay in receipt of tax refund monies.

## CLASS ACTION ALLEGATIONS

111. Plaintiffs sue on behalf of themselves and the proposed nationwide class ("Class"), defined as follows, pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3):

> **Nationwide Class**: All individuals residing in the United States whose Sensitive Information was compromised in the Defendants' Data Breach including all those who received notice of the breach.

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

113. Plaintiffs reserve the right to amend the class definition.

114. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiffs are representatives of the Class, consisting of approximately 2.5 million members, far too many to join in a single action;

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendants' possession, custody, and control;

c. **Typicality**. Plaintiffs' claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendants, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiffs will fairly and adequately protect the proposed Class's interests. Plaintiffs' interests do not conflict with the Class's interests, and they have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiffs' and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

   i. Whether Defendants had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's Sensitive Information;

   ii. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

   iii. Whether Defendants were negligent in maintaining, protecting, and securing Sensitive Information;

   iv. Whether Defendants breached contract promises to safeguard Plaintiffs' and the Class's Sensitive Information;

   v. Whether Defendants took reasonable measures to determine the extent

of the Data Breach after discovering it;

vi. Whether Defendants' Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiffs' and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiffs and the Class are entitled to damages, treble damages, or injunctive relief.

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

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

116. Plaintiffs realleges all previous paragraphs as if fully set forth below.

117. Plaintiffs and members of the Class entrusted their Sensitive Information to Defendants.

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

119. Defendants owed a duty of care to Plaintiffs and members of the Class because it was foreseeable that Defendants' failure to adequately safeguard their Sensitive Information in accordance with state-of-the-art industry standards concerning data security would result in

the compromise of that Sensitive Information. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and the Class's Sensitive Information by disclosing and providing access to this information to unauthorized third parties and by failing to properly supervise both the way the Sensitive Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

120. Defendants owed to Plaintiffs and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their Sensitive Information. Defendants also owed a duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiffs and the Class to take appropriate measures to protect their Sensitive Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

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

122. The risk that unauthorized persons would attempt to gain access to the Sensitive Information and misuse it was foreseeable. Given that Defendants hold vast amounts of Sensitive Information, it was inevitable that unauthorized individuals would attempt to access Defendants' databases containing the Sensitive Information.

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

124. Defendants breached their duties by failing to exercise reasonable care in supervising their employees, agents, contractors, vendors, and suppliers, and in handling and securing the Sensitive Information of Plaintiffs and the Class which actually and proximately caused the Data Breach and Plaintiffs' and the Class's injury. Defendants further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and members of the Class's injuries-in-fact. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiffs and the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

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

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

126. Plaintiffs realleges all previous paragraphs as if fully set forth below.

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

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

129. Defendants breached their duties to Plaintiffs and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Sensitive Information.

130. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and their consumers, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendants were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

131. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical

safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

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

133. Defendants violated their duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and the Class's Sensitive Information and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendants collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

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

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

136. But for Defendants' wrongful and negligent breach of the duties owed to Plaintiffs and members of the Class, Plaintiffs and members of the Class would not have been injured.

137. The injury and harm suffered by Plaintiffs and members of the Class were the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties and that their breach would cause Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure of their Sensitive Information.

138. Had Plaintiffs and the Class known that Defendants did not adequately protect their Sensitive Information, Plaintiffs and members of the Class would not have entrusted Defendants with their Sensitive Information.

139. Defendants' various violations and their failure to comply with applicable laws and regulations constitute negligence *per se*.

140. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of Sensitive Information; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Sensitive Information, entitling them to damages in an amount to be proven at trial.

141. Additionally, as a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and Class members have suffered and will suffer the continued risks of exposure of their Sensitive Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate

measures to protect their Sensitive Information in its continued possession.

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

142. Plaintiffs reallege all previous paragraphs as if fully set forth below.

143. Plaintiffs and Class Members were required to provide their Private Information to Defendants as a condition of their use of Defendants' services.

144. Plaintiffs and Class Members paid money to Defendants in exchange for services, along with Defendants' promise to protect their Private Information from unauthorized access and disclosure.

145. Implicit in the agreement between Plaintiffs and Class Members and the Defendants to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses, and (f) retain the Private Information only under conditions that kept such information secure and confidential.

146. When Plaintiffs and Class Members provided their PII and PHI to Defendants, they entered into implied contracts with Defendants pursuant to which Defendants agreed to reasonably protect such information.

147. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and

regulations and were consistent with industry standards.

148. Plaintiffs and Class Members would not have entrusted their Private Information to Defendants in the absence of the implied contract between them and Defendants to keep their information reasonably secure, including monitoring its computer systems and networks to ensure that it adopted reasonable data security measures.

149. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendants.

150. Defendants breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

151. As a direct and proximate result of Defendants' breaches of the implied contracts, Class Members sustained damages as alleged herein.

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

153. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, e.g., (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide and continue to provide adequate credit monitoring to all Class Members.

**COUNT IV**
**BREACH OF THIRD-PARTY BENEFICIARY CONTRACT**
**(On Behalf of Plaintiffs and the Class Against Defendant PJ&A)**

154. Plaintiffs reallege all previous paragraphs as if fully set forth below.

155. Plaintiffs and Class Members were required to provide their Private Information to Defendants as a condition of their use of Defendants' services.

156. Upon information and belief, Defendant PJ&A entered into contracts with its

customers to provide transcription services to them; services that included data security practices, procedures, and protocols sufficient to safeguard the Private Information that was entrusted to it.

157. Such contracts were made expressly for the benefit of Plaintiffs and the Class, as it was their Private Information that Defendants agreed to receive, store, utilize, transfer, and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties and Plaintiffs and Class Members were direct and express beneficiaries of such contracts.

158. Defendants knew or should have known that if it were to breach these contracts with its customers, Plaintiffs and Class Members would be harmed.

159. Defendants breached their contracts with customers by, among other things, failing to adequately secure Plaintiffs and Class Members' Private Information, and, as a result, Plaintiffs and Class Members were harmed by Defendants' failure to secure their Private Information.

160. As a direct and proximate result of Defendants' breach, Plaintiffs and Class Members are at a current and ongoing risk of identity theft, and Plaintiffs and Class Members sustained incidental and consequential damages including: (i) financial "out-of-pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out-of-pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) diminution of value of their Private Information; (vii) future costs of identity theft monitoring; (viii) and the continued risk to their Private Information, which remains in Defendants' control, and which is subject to further breaches, so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private

Information.

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

162. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

**COUNT V**
**Breach of Fiduciary Duty**
**(On Behalf of Plaintiffs and the Class)**

163. Plaintiffs reallege all previous paragraphs as if fully set forth below.

164. In providing their Private Information to Defendants, Plaintiffs and Class Members justifiably placed a special confidence in Defendants to act in good faith and with due regard for the interests of Plaintiffs and Class Members to safeguard and keep confidential that Private Information.

165. Defendants accepted the special confidence Plaintiffs and Class Members placed in it, as evidenced by its assertion that it is committed to protecting the privacy of Plaintiffs' personal information as included in the Data Breach notification letter.

166. In light of the special relationship between Defendants, Plaintiffs, and Class Members, whereby Defendants became a guardian of Plaintiffs and Class Members' Private Information, Defendants became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its customers, including Plaintiffs and Class Members for the safeguarding of Plaintiffs and Class Members' Private Information.

167. Defendants has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its customer relationships, in particular, to keep secure the Private Information of its customers.

168. Defendants breached its fiduciary duties to Plaintiffs and Class Members by failing to protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

169. Defendants breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs and Class Members' Private Information.

170. As a direct and proximate result of Defendants' breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to:

a. Actual identity theft;

b. The compromise, publication, and/or theft of their Private Information;

c. Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information;

d. Lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft;

e. The continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession;

f. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and

g. The diminished value of the services they paid for and received.

171. As a direct and proximate result of Defendants' breaches of its fiduciary duties, Plaintiffs and Class Members will suffer other forms of injury and/or harm, and other economic and non-economic losses.

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

172. Plaintiffs reallege all previous paragraphs as if fully set forth below.

173. Plaintiffs and members of the Class conferred a benefit upon Defendants in providing Sensitive Information to Defendants.

174. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiffs and the Class. Defendants also benefited from the receipt of Plaintiffs' and the Class's Sensitive Information, as this was used to facilitate the services and goods they sold to their consumers, including Plaintiffs' and the Class.

175. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiffs and the Class's Sensitive Information because Defendants failed to adequately protect their Sensitive Information. Plaintiffs and the proposed Class would not have provided their Sensitive Information to Defendants had they known Defendants would not adequately protect their Sensitive Information.

176. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and members of the Class all unlawful or inequitable proceeds received by them

because of their misconduct and Data Breach.

**COUNT VII**
**Violation Of The New York Deceptive Trade Practices Act ("GBL")**
**(New York Gen. Bus. Law § 349)**
**(On Behalf of Plaintiffs and the Class)**

177. Plaintiffs reallege all previous paragraphs as if fully set forth below.

178. Defendants engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

a. Misrepresenting material facts to Plaintiffs and the Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Class Members' Sensitive Information from unauthorized disclosure, release, data breaches, and theft;

b. Misrepresenting material facts to Plaintiffs and the Class by representing that they did and would comply with the requirements of federal and state laws pertaining to the privacy and security of Class Members' Sensitive Information;

c. Omitting, suppressing, and/or concealing material facts of the inadequacy of their privacy and security protections for Class Members' Sensitive Information;

d. engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Class Members' Sensitive Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws; and,

e. engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to the Class in a timely and accurate manner, contrary

to the duties imposed by N.Y. Gen. Bus. Law § 899-aa (2).

179. Defendants knew or should have known that their network and data security practices were inadequate to safeguard the Class Members' Sensitive Information entrusted to it, and that the risk of a data breach or theft was highly likely.

180. Defendants should have disclosed this information because Defendants were in a superior position to know the true facts related to the defective data security.

181. Defendants' failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiffs and Class Members) regarding the security of Defendants' network and aggregation of Sensitive Information.

182. The representations upon which consumers (including Plaintiffs and Class Members) relied were material representations (e.g., as to Defendants' adequate protection of Sensitive Information), and consumers (including Plaintiffs and Class Members) relied on those representations to their detriment.

183. Defendants' conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendants' conduct, Plaintiffs and other Class Members have been harmed, in that they were not timely notified of the Data Breach, which resulted in profound vulnerability to their personal information and other financial accounts.

184. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Class Members' Sensitive Information and that the risk of a data security incident was high.

185. Defendants' acts, practices, and omissions were done in the course of Defendants' business of furnishing employment benefit services to consumers in the State of New York.

186. As a direct and proximate result of Defendants' unconscionable, unfair, and deceptive acts and omissions, Plaintiffs' and Class Members' Sensitive Information was disclosed to third parties without authorization, causing and will continue to cause Plaintiffs and Class Members damages.

187. As a direct and proximate result of Defendants' multiple, separate violations of GBL §349, Plaintiffs and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiffs and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiffs' and Class Members' Sensitive Information; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their Sensitive Information; (g) the diminution in the value of the services bargained for as Plaintiffs and Class Members were deprived of the data protection and security that Defendants promised when Plaintiffs and the proposed class entrusted Defendants with their Sensitive Information; and (h) the continued and substantial risk to Plaintiffs' and Class Members' Sensitive Information, which remains in the Defendants' possession with inadequate measures to protect Plaintiffs' and Class Members' Sensitive Information.

188. As a result, Plaintiffs and the Class Members have been damaged in an amount to be proven at trial.

189. Plaintiffs bring this action on behalf of themselves and Class Members for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiffs, Class Members and the public from Defendants' unfair, deceptive, and unlawful practices. Defendants' wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

190. Plaintiffs and Class Members seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, in junctive relief, and/or attorney's fees and costs.

191. On behalf of themselves and other members of the Class, Plaintiffs seek to enjoin the unlawful acts and practices described herein, to recover actual damages or fifty dollars, whichever is greater, three times actual damages, and reasonable attorneys' fees.

192. Also as a direct result of Defendants' violation of GBL § 349, Plaintiffs and the Class Members are entitled to damages as well as injunctive relief, including, but not limited to, ordering Defendants to: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

**COUNT VIII**
**Declaratory and Injunctive Relief**
**(On Behalf of Plaintiffs and the Class)**

193. Plaintiffs reallege all previous paragraphs as if fully set forth below.

194. Plaintiffs pursue this claim under the Federal Declaratory Judgment Act, 28 U.S.C.

§ 2201, et seq.

195. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

196. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class Members' Sensitive Information, and whether Defendants is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from future data breaches that compromise their Sensitive Information. Plaintiffs and the Class remain at imminent risk that further compromises of their Sensitive Information will occur in the future.

197. The Court should also issue prospective injunctive relief requiring Defendants to employ adequate security practices consistent with law and industry standards to protect employee and patient Sensitive Information.

198. Defendants still possess the Sensitive Information of Plaintiffs and the Class.

199. To Plaintiffs' knowledge, Defendants have made no announcement that it has changed their data storage or security practices relating to the Sensitive Information, beyond the vague claim in the Data Breach Letter that it is "[taking] steps to enhance the security of our computer systems and the data we maintain."

200. To Plaintiffs' knowledge, Defendants have made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

201. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach of Defendants' computers. The risk of another such breach is real, immediate, and substantial.

202. As described above, actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual 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 Sensitive Information and Defendants' failure to address the security failings that led to such exposure.

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

204. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Among other things, if another data breach occurs of Defendants' computers, Plaintiffs and Class Members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

205. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendants' computers, thus eliminating the additional injuries that would result to Plaintiffs and the Class.

206. Plaintiffs and Class Members, therefore, seek a declaration (1) that Defendants' existing data security measures do not comply with their contractual obligations and duties of care to provide adequate data security, and (2) that to comply with contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendants engage internal security personnel to conduct testing, including audits on Defendants' systems, on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

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

c. Ordering that Defendants audit, test, and train their security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Defendants purge, delete, and destroy, in a reasonably secure manner, any Sensitive Information not necessary for their provision of services;

e. Ordering that Defendants conduct regular database scanning and security checks; and

f. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, client personally identifiable information.

## PRAYER FOR RELIEF

Plaintiffs and the Class demand a jury trial on all claims so triable and request that the

Court enter an order:

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

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

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

D. Enjoining Defendants from further deceptive practices and making untrue statements about the Data Breach and the stolen Sensitive Information;

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

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

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

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

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

J. Granting such other or further relief as may be appropriate under the circumstances.

**DEMAND FOR JURY TRIAL**

Plaintiffs hereby demand that this matter be tried before a jury.

Dated: November 16, 2023

**THE SULTZER LAW GROUP P.C.**

By: /s/ Jason P. Sultzer

Jason P. Sultzer, Esq.
Philip J. Furia, Esq.
85 Civic Center Plaza, Suite 200
Poughkeepsie, NY 12601
Tel: (845) 483-7100
Fax: (888) 749-7747
sultzerj@thesultzerlawgroup.com
furiap@thesultzerlawgroup.com

**LEEDS BROWN LAW, P.C**
Jeffrey K. Brown, Esq.
Andrew Costello, Esq.
One Old Country Road - Suite 347
Carle Place, NY 11514
Tel: (516) 873-9550
jbrown@leedsbrownlaw.com
acostello@leedsbrownlaw.com

**LEVIN SEDRAN & BERMAN LLP**
Charles E. Schaffer *
Nicholas J. Elia *
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Phone: (215) 592-1500
cschaffer@lfsblaw.com
nelia@lfsblaw.com

**GOLDENBERG SCHNEIDER, LPA**
Jeffrey S. Goldenberg *
Todd B. Naylor *
4445 Lake Forest Drive, Suite 490
Cincinnati, Ohio 45242
Phone: (513) 345-8291
Facsimile: (513) 345-8294
jgoldenberg@gs-legal.com
tnaylor@gs-legal.com

*Counsel for Plaintiffs and the Class*

* *Pro hac vice forthcoming*

# ClassAction.org



---