SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF WESTCHESTER

| | |
|---|---|
| NONI WAHAB, GINA ADDORISIO, DANIEL OUGRIN, LAVERNE CARR, DIANE YOUNG, as parent and guardian of Q.Y., a minor, and STEPHEN SCHLAUGIES, individually and on behalf of all others similarly situated,<br><br>Plaintiffs,<br><br>v.<br><br>BOSTON CHILDREN'S HEALTH PHYSICIANS, LLP and ATSG, INC.,<br><br>Defendants. | Index No. 73692/2024<br><br>*JURY TRIAL DEMANDED* |

**CONSOLIDATED CLASS ACTION COMPLAINT**

Plaintiffs Noni Wahab, Gina Addorisio, Daniel Ougrin, Laverne Carr, Diane Young, as parent and guardian of Q.Y., a minor, and Stephon Schlaugies ("Plaintiffs"), individually and on behalf of all others similarly situated ("Class Members"), brings this action against Defendants Boston Children's Health Physicians, LLP ("BCHP") and ATSG, Inc. ("ATSG") (collectively, "Defendants"), and alleges, upon personal knowledge as to their own actions and their counsel's investigation, and upon information and belief as to all other matters, as follows:

## I. INTRODUCTION

1. BCHP is a pediatric primary and specialty care physician group that operates in New York and Connecticut.[1] BCHP collects a significant amount of data including personally identifiable information including patient names, Social Security numbers, addresses, and dates of birth, and protected health information ("PHI") including medical record numbers, health

[1] https://bchp.childrenshospital.org/ (last visited Dec. 23, 2024).

insurance information, billing information, and treatment information (collectively, "Private Information").

2. ATSG is an IT company that touts itself as a global leader in transformation technology solutions. One of ATSG's clients was BCHP.

3. Upon information and belief, on or about September 10, 2024, an unauthorized party accessed Defendants' computer systems ("Data Breach"). First, an IT vendor informed Defendants on September 6, 2024 that "it identified unusual activity in its systems."[2] Then, an "investigation with a third-party forensic firm" revealed that "an unauthorized third-party gained access to [Defendant's] network on September 10, 2024, and took certain files from our network."[3] As a result of this, the Private Information of Plaintiffs and Class Members was compromised due to Defendants' complete failure to protect it and their unwillingness to act lawfully after the Data Breach occurred.

4. Against this backdrop, Plaintiffs bring this action on behalf of all similarly situated persons whose Private Information was compromised as a result of Defendants' failure: (i) to adequately protect the Private Information of Plaintiffs and Class Members; (ii) to warn Plaintiffs and Class Members of their inadequate information security practices; and (iii) to avoid continuing to retain and use the Private Information of Plaintiffs and Class Members without adequate safeguards. Defendants' conduct amounts to negligence and violates federal and state statutes.

5. Plaintiffs and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) lost or diminished value of their Private Information; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax

[2] Sample Notice Letter, attached hereto as ***Exhibit A*** ("Notice"); *see also* https://www.jdsupra.com/legalnews/boston-children-s-health-physicians-3819740/.
[3] *Id*.

fraud, and/or unauthorized use of their Private Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and, significantly, (iv) the continued and certainly an increased risk to their Private Information.

## II. PARTIES

6. Plaintiff Noni Wahab is a natural person and citizen of New York, where she intends to remain. She is a Data Breach victim and received the Notice dated October 4, 2024.

7. Plaintiff Gina Addorisio is a natural person and citizen of New York, where she intends to remain. She is a Data Breach victim and received the Notice dated October 4, 2024.

8. Plaintiff Daniel Ougrin is a natural person and citizen of New York, where he intends to remain. He is a Data Breach victim and received the Notice dated October 4, 2024.

9. Plaintiff Laverne Carr is a natural person and citizen of New York, where she intends to remain. She is a Data Breach victim and received the Notice dated October 4, 2024.

10. Plaintiff Diane Young is a natural person and citizen of New York, where she intends to remain. Her minor child Q.Y. is a Data Breach victim and received the Notice dated October 4, 2024.

11. Plaintiff Stephen Schlaugies is a natural person and citizen of New York, where he intends to remain. He is a Data Breach victim and received the Notice dated October 4, 2024.

12. Defendant BCHP is a New York limited liability partnership with its headquarters and principal place of business located at 400 Columbus Avenue, Suite 200 East, Valhalla, New York 10595.

13. Defendant ATSG is a New York corporation with its headquarters and principal place of business located at 1 Pennsylvania Plaza, New York, New York 10119.

## III. JURISDICTION AND VENUE

14. Jurisdiction and venue are proper in this County because Defendants are located in and conduct business from their offices in this County, and because Defendants' misconduct, which is the basis of this action, occurred in this County.

## IV. GENERAL ALLEGATIONS

***Defendants' Businesses***

15. BCHP is a physician group offering its services (despite its name) primarily in the states of New York and Connecticut.[4] It has more than 300 clinicians across more than 60 locations, and specializes in a variety of pediatric and adult practices.[5]

16. BCHP is an affiliate hospital of the Children's Hospital Corporation d/b/a Boston Children's Hospital, which touts itself as one of the best hospitals in the nation and is widely regarded for its research and advancements in pediatric care.[6]

17. In order to conduct its business, BCHP requires that its adult and pediatric patients provide it with their Private Information.

18. ATSG is an IT solution provider that touts itself to be "a global leader in transformational technology solutions for today's digital enterprise."[6] ATSG boasts a total revenue of $93.4 million.[7] ATSG's IT services are specialized for corporations, government organizations and healthcare providers who manage highly sensitive data. ATSG thus must oversee, manage, and protect the Private Information of its clients' patients and customers.

19. Defendants collect and store Plaintiffs' and the proposed Class Members' Private

[4] https://bchp.childrenshospital.org/about (last visited Dec. 23, 2024).
[5] *Id*.
[6] https://childrenshospital.org/about-us (last visited Dec. 23, 2024).
[7] Zoominfo, *ATSG*, https://www.zoominfo.com/c/axispoint-technology-solutions-group-inc/454983374 (last visited Dec. 23, 2024).

Information on their computer systems, including but not limited to full names, Social Security numbers, dates of birth, medical record numbers, health insurance information, billing information, and treatment information.

20. When BCHP collects this Private Information, it promises to use reasonable care to protect and safeguard the Private Information from unauthorized disclosure.

21. BCHP maintains a Notice of Privacy Practices which states, "We are required by law to maintain the confidentiality of health information that identifies our patients," and enumerates specific purposes for which Defendants may disclose patient Private Information without authorization.[8]

22. On information and belief, BCHP maintained identical or substantially similar policies prior to the Data Breach.

23. None of the purposes for which BCHP may disclose patient Private Information without authorization include the Data Breach which came to pass.

24. BCHP represented to its patients that they would take adequate measures to safeguard their Private Information, and Plaintiffs and Class Members relied on BCHP's representations when they agreed to provide their Private Information to BCHP.

25. Despite their alleged commitments to securing sensitive patient data, BCHP did not follow industry standard practices in securing patients' Private Information and failed to protect the Private Information of Plaintiffs and the proposed Class Members from unauthorized disclosure in the Data Breach.

[8] *See* https://bchp.childrenshospital.org/sites/default/files/2024-01/BCHP-Notice-of-Privacy-Practices-English-Rev-10-2023-2.pdf (last visited Dec. 23, 2024).

***Obligations of Defendants***

26. Plaintiffs and Class Members relied on BCHP's promises to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their Private Information.

27. Defendants had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' Private Information from involuntary disclosure to third parties.

28. The healthcare sector is a favored target by cybercriminals, yet recent studies, including one by the Massachusetts Institute of Technology, found medical centers lagged behind other businesses in safeguarding their computer systems. A Tenable study analyzing healthcare sector breaches from January 2020 to February 2021 reported that "records were confirmed to have been exposed in nearly 93% of the breaches."

29. Despite recognizing their duty to do so, on information and belief, Defendants have not implemented reasonably necessary cybersecurity safeguards or policies to protect its patients' Private Information or supervised their IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, Defendants leave significant vulnerabilities in their systems for cybercriminals to exploit and gain access to patients' Private Information.

30. As a result of Defendants' failure to implement and follow basic security procedures, the Private Information of Plaintiffs and Class Members was more likely than not accessed, disclosed, and/or acquired and is now in the hands of criminals.

31. Once information is placed onto the Internet, it is virtually impossible to remove. Plaintiffs and Class Members now and will forever face a substantial increased risk of identity theft. Consequently, Plaintiffs and Class Members have had to spend, and will continue to spend,

significant time and money in the future to protect themselves due to Defendants' failures.

32. Additionally, as a result of Defendants' failure to follow industry standard security procedures, Plaintiffs and Class Members received a diminished value for the services Defendants was to provide.

33. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiffs and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access, intrusion, and/or acquisition.

34. Moreover, Defendants now put the burden squarely on Plaintiffs and Class Members to enroll in the credit monitoring services, among other steps Plaintiffs and Class Members must take to protect themselves. Time is a compensable and extremely valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.

35. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week; leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'" Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, patients now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

36. Plaintiffs and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek renumeration for the loss of valuable time as another element of damages.

***The Data Breach***

37. On or about October 4, 2024, Defendants sent out notices to individuals like Plaintiffs and Class Members ("Notice of Data Breach"). The Notice of Data Breach to Plaintiffs stated, in relevant part:

> ***What Happened?*** On September 6, 2024, our IT vendor informed us that it identified unusual activity in its systems. On September 10, 2024, we detected unauthorized activity on limited parts of the BCHP network and immediately initiated our incident response protocols, including shutting down our systems as a protective measure. We also began an investigation with a third-party forensic firm and determined that an unauthorized third-party gained access to our network on September 10, 2024, and took certain files from our network.
>
> ***What Information May Have Been Involved?*** The files may have included your name, Social Security number, and one or more of the following: address, date of birth, medical record number, health insurance information, billing information and limited treatment information . . .

38. In other words, Defendants' cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of patients' Private Information.

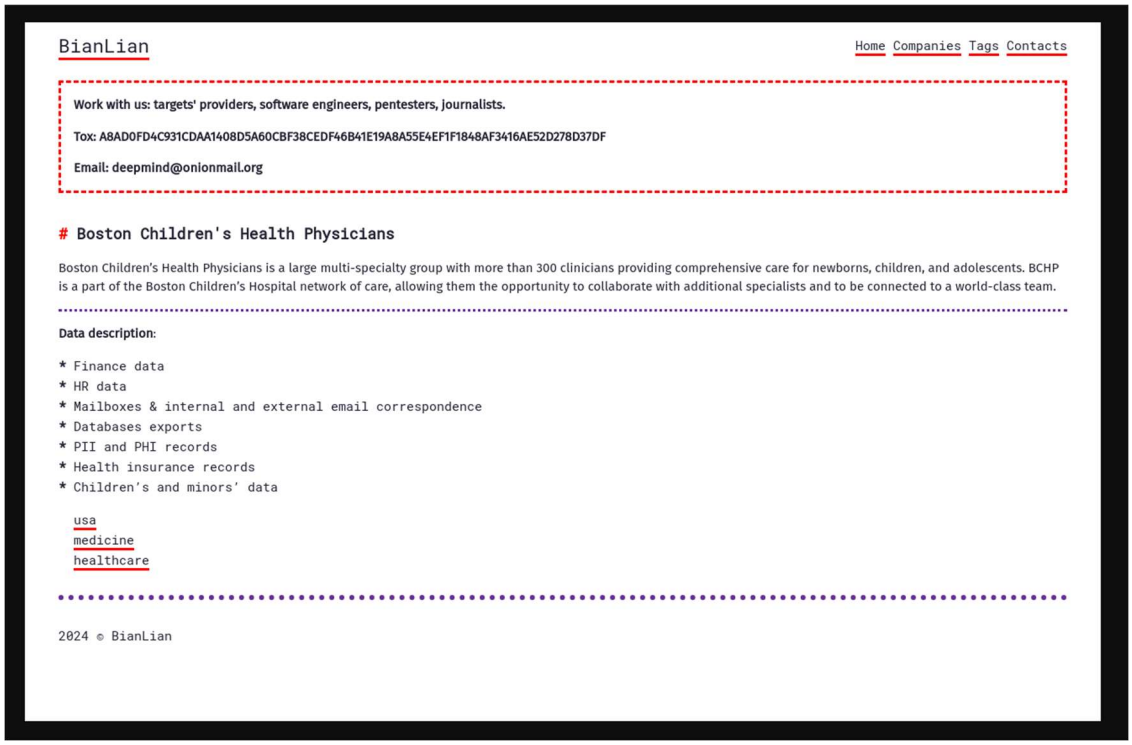
39. The details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected.

40. On information and belief, the notorious and aggressive BianLian ransomware gang took credit for the Data Breach.[9] An incredibly active and successful hacker collective with

[9] Breach Sense, https://www.breachsense.io/breaches/baers/ (last visited Dec. 23, 2024).

over 118 victims[10], BianLian was known to employ double extortion model by encryption victims' systems after exfiltrating the data.[11] However, BianLian recently announced to have shifted its focus from encrypting its victims' files to exfiltrating data found on compromised or weak networks and using them for extortion.[12] Defendants knew or should have known of the tactics that hackers like BianLian employ.

41. With the Sensitive Information secured and stolen by BianLian, the hackers then purportedly issued a ransom demand to BCH. However, BCH has provided no public information on the ransom demand or payment.




42. On information or belief, BianLian is anticipated to release all stolen information

[10] Bill Toulas, *BianLian ransomware gang shifts focus to pure data extortion*, https://www.bleepingcomputer.com/news/security/bianlian-ransomware-gang-shifts-focus-to-pure-data-extortion/ (last visited Dec. 23, 2024).
[11] America's Cyber Defense Agency, *Cybersecurity & Infrastructure Security Agency* https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-136a (last visited Dec. 23, 2024).
[12] *Supra* n.10.

onto the dark web for access, sale, and download following the deadline of the ransom demand to Defendants.[13]

43. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiffs and Class Members, causing their Private Information to be exposed.

44. To prevent and detect network server intrusions, Defendants could and should have implemented, as recommended by the United States Government, the following non-exhaustive list of measures:

- Utilize strict access controls, remove backdoor connections, and limit virtual private networks.
- Maintain adequate file system and boot management, stay updated with vendor-supported software, and verify software and configuration settings.
- Use centralized servers, configure authentication, authorization, and accounting, implement the principle of 'least privilege.
- Incorporate specific usernames and account settings, change default passwords, eliminate unnecessary accounts, and store passwords with safe algorithms.
- Configure logging and centralized remote log servers, obtain necessary log information, and synchronize clocks.
- Refrain from using cleartext services, verify appropriate encryption strength, use secure protocols, restrict access to services, and turn off unneeded network services.
- Turn off Internet Protocol service routing and turn on routing authentication.
- Enable port security and disable default virtual local area networks, unused ports, port monitoring, and proxy Address Resolution Protocol.

45. Given that Defendants was storing the Private Information of the patients it was providing services to, Defendants could and should have implemented all the above measures to prevent and detect network server intrusions.

46. On information and belief, Defendants failed to adequately train and supervise their

[13] #StopRansomware, CISA, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-136a (last visited Dec. 23, 2023).

IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over patients' Private Information.

47. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the aforementioned measures to prevent network server intrusions, resulting in the Data Breach and the exposure of the Private Information of individuals like Plaintiffs and Class Members.

***The Data Breach Was Foreseeable Because the Healthcare Sector is Particularly Vulnerable to Cyber Attacks.***

48. Defendants were on notice that companies in the healthcare industry are targets for data breaches.

49. Defendants were on further notice regarding the increased risks of inadequate cybersecurity. Indeed, cyberattacks against the healthcare industry have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain Private Information." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."

50. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year. In 2017, a new record high of 1,579 breaches were reported representing a 44.7 percent increase.

51. That trend continues. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in

2020.

52. In February 2022, the cybersecurity arm of the U.S. Department of Health and Human Services ("HHS") issued a warning to hospitals and healthcare systems about a dramatic rise in cyberattacks, urging facilities to shore up their cyber defenses. Indeed, just days before, HHS's cybersecurity arm issued yet another warning about increased cyberattacks that urged vigilance with respect to data security.

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

54. In the context of data breaches, healthcare is "by far the most affected industry sector." Further, cybersecurity breaches in the healthcare industry are particularly devastating, given the frequency of such breaches and the fact that healthcare providers maintain highly sensitive and detailed Private Information. A Tenable study analyzing publicly disclosed healthcare sector breaches from January 2020 to February 2021 reported that "records were confirmed to have been exposed in *nearly 93% of the breaches*."

55. Defendants were also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."

56. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.

57. The healthcare sector consistently reports one of the highest number of breaches among all measured sectors, with the highest rate of exposure per breach. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage. Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.

58. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."

***Defendants Acquires, Collects, and Stores Plaintiffs' and Class Members' Personal Information.***

59. In the course of their regular business operations, Defendants acquired, collected, and stored Plaintiffs' and Class Members' Private Information.

60. As a condition of their relationship with Plaintiffs and Class Members, Defendants required that Plaintiffs and Class Members entrust Defendants with highly confidential Private Information.

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

62. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

63. Yet, despite the prevalence of public announcements of these data breach and data security compromises, Defendants failed to take appropriate steps to protect Plaintiffs' and Class Members' Private Information from being compromised.

***Securing Private Information and Preventing Breaches***

64. Defendants could have prevented this Data Breach by properly securing their networks and encrypting the Private Information of Plaintiffs and Class Members. Alternatively, Defendants could have destroyed the data, especially decade-old data from former patients. Further, Defendants could have prevented this Data Breach by properly overseeing patients' Private Information – including assuring that Private Information collected was properly protected and maintained and adhered to a reasonable deletion schedule.

65. Defendants' 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.

66. Indeed, despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being compromised.

67. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 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."

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

***Value of Personal Identifiable Information***

69. The Personal Information 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. Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web. Criminals can also purchase access to entire company data breaches from $900 to $4,500.

70. 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

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.

71. 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.

72. 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."

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

74. 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."

75. 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.

76. Indeed, cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiffs' and the Class's Private Inf. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiffs' and the Class's financial accounts.

77. The Private Information of Plaintiffs and Class Members was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the Private Information for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

78. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information 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.

79. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, including Social Security numbers and/or PHI, and of the foreseeable consequences that would occur if the Private Information was compromised, including, specifically, the significant costs that would be

imposed on Plaintiffs and Class Members a result.

80. 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 Personal Information.

81. Defendants were, or should have been, fully aware of the unique type and the significant volume of data stored on and/or shared on their systems and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

82. To date, Defendants have suggested credit monitoring services for twelve months and Defendants have offered nothing.

83. Further, there is a market for Plaintiffs' and Class Members PHI, and the stolen PHI has inherent value.

84. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase Private Information on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

85. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing

and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."

86. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

***Defendants' Conduct Violates the Rules and Regulations of HIPAA and HITECH.***

87. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients, or in this case, 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.

88. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of Private Information is properly maintained.

89. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, et seq. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Defendants left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

90. Defendants are a covered entity pursuant to HIPAA. *See* 45 C.F.R. § 160.102. Defendants must therefore comply with the HIPAA Privacy Rule and Security Rule. See 45 C.F.R.

Part 160 and Part 164, Subparts A through E.

91. Defendants are a covered entity pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

92. Plaintiffs' and Class Members' Private Information is "protected health information" as defined by 45 CFR § 160.103.

93. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

94. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

95. Plaintiffs' and Class Members' Private Information is "unsecured protected health information" as defined by 45 CFR § 164.402.

96. Plaintiffs' and Class Members' unsecured PHI has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

97. Plaintiffs' and Class Members' unsecured PHI acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

98. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

99. Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons

in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

100. After receiving notice that they were victims of a data breach that required the filing of a Breach Report in accordance with 45 CFR § 164.408(a), it is reasonable for recipients of that notice, including Plaintiffs and Class Members in this case, to believe that future harm (including identity theft) is real and imminent, and to take steps to mitigate that risk of future harm.

101. The Data Breach could have been prevented if Defendants implemented HIPAA mandated, industry standard policies and procedures for securely disposing of Private Information when it was no longer necessary and/or had honored their obligations to Plaintiffs and Class Members.

102. It can be inferred from Defendants' Data Breach that it either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Plaintiffs and Class Members' Private Information.

103. Defendants' security failures include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendants creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and

correct security violations in violation of 45 CFR 164.308(a)(1);

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

g. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

h. Failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

i. Failing to ensure compliance with HIPAA security standard rules by Defendants' workforce in violation of 45 CFR 164.306(a)(4);

j. 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

k. 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);

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

m. Retaining information past a recognized purpose and not deleting it.

104. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendants to provide notice of the breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

105. Because Defendants has failed to comply with industry standards, while monetary relief may cure some of Plaintiffs and Class Members' injuries, injunctive relief is necessary to ensure Defendants' approach to information security is adequate and appropriate. Defendants still maintain the Private Information of Plaintiffs and Class Members; and without the supervision of the Court via injunctive relief, Plaintiffs and Class Members' Private Information remains at risk of subsequent data breaches.

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

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

107. Several best practices have been identified that a minimum should be implemented by employers in possession of Private Information, like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendants failed to follow these industry best practices, including a failure to implement multi-factor authentication.

108. 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.

109. 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.

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

***Plaintiff Nomi Wahab's Experience***

111. Plaintiff Nomi Wahab (for purposes of this section, "Plaintiff") first learned of the Data Breach when she received her Notice Letter on or about October 4, 2024. The Notice Letter informed Plaintiff that her Private Information was compromised in the Data Breach.

112. As a result of the Data Breach, Plaintiff has spent time dealing with the consequences of the Data Breach. This time has been lost forever and cannot be recaptured.

113. Plaintiff has taken it upon herself to research the Data Breach. Plaintiff has suffered mental anguish and stress as a result of the Data Breach as alleged herein.

114. Upon information and belief, Plaintiff's Private Information was in Defendants' computer systems during the Data Breach and remains in Defendants' possession.

115. Plaintiff is very careful about sharing Private Information. Plaintiff has never knowingly transmitted unencrypted Private Information over the Internet or any other unsecured source. Plaintiff stores any documents containing her Private Information in a safe and secure location. Moreover, Plaintiff diligently chooses unique usernames and passwords for online accounts.

116. Once an individual's Private Information is for sale and access on the dark web, as Plaintiff's Private Information is here as a result of the Data Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.

117. Plaintiff has suffered actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendants for the purpose of receiving healthcare services from Defendants, which was compromised in and as a result of the Data Breach.

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

119. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from Private Information, especially her Social Security number, in combination with her name, being placed in the hands of unauthorized third parties and criminals.

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

***Plaintiff Gina Addorisio's Experience***

121. Plaintiff Gina Addorisio (for purposes of this section, "Plaintiff") first learned of the Data Breach when she received her Notice Letter on or about October 4, 2024. The Notice Letter informed Plaintiff that her Private Information was compromised in the Data Breach.

122. As a result of the Data Breach, Plaintiff has spent time dealing with the consequences of the Data Breach. This time has been lost forever and cannot be recaptured.

123. Following the Data Breach, Plaintiff has experienced an increase in phishing emails, texts, and phone calls.

124. Upon information and belief, Plaintiff's Private Information was in Defendants' computer systems during the Data Breach and remains in Defendants' possession.

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

126. Plaintiff has suffered actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendants for the purpose of receiving healthcare services from Defendants, which was compromised in and as a result of the Data Breach.

127. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from Private Information, especially her Social Security number, in combination with her name, being placed in the hands of unauthorized third parties and criminals.

128. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and

safeguarded from future breaches.

***Plaintiff Daniel Ougrin's Experience***

129. Plaintiff Daniel Ougrin (for purposes of this section, "Plaintiff") first learned of the Data Breach when he received his Notice Letter on or about October 4, 2024. The Notice Letter informed Plaintiff that his Private Information was compromised in the Data Breach.

130. As a result of the Data Breach, Plaintiff has spent time dealing with the consequences of the Data Breach. This time has been lost forever and cannot be recaptured.

131. Upon information and belief, Plaintiff's Private Information was in Defendants' computer systems during the Data Breach and remains in Defendants' possession.

132. Plaintiff is very careful about sharing Private Information. Plaintiff has never knowingly transmitted unencrypted Private Information over the Internet or any other unsecured source. Plaintiff stores any documents containing his Private Information in a safe and secure location. Moreover, Plaintiff diligently chooses unique usernames and passwords for online accounts.

133. Shortly after and as a result of the Data Breach, Plaintiff Ougrin experienced a large increase in spam and suspicious phone calls, texts, and emails.

134. Plaintiff has suffered actual injury in the form of damages to and diminution in the value of Private Information—a form of intangible property that Plaintiff entrusted to Defendants for the purpose of receiving healthcare services from Defendants, which was compromised in and as a result of the Data Breach.

135. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from Private Information, especially his Social Security number, in combination with his name, being placed in the hands of unauthorized third parties and criminals.

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

***Plaintiff Laverne Carr's Experience***

137. Plaintiff Laverne Carr (for purposes of this section, "Plaintiff") first learned of the Data Breach when she received her Notice Letter on or about October 4, 2024. The Notice Letter informed Plaintiff that her Private Information was compromised in the Data Breach.

138. As a result of the Data Breach, Plaintiff has spent time dealing with the consequences of the Data Breach. This time has been lost forever and cannot be recaptured.

139. Upon information and belief, Plaintiff's Private Information was in Defendants' computer systems during the Data Breach and remains in Defendants' possession.

140. Plaintiff has suffered actual injury in the form of damages to and diminution in the value of Private Information—a form of intangible property that Plaintiff entrusted to Defendants for the purpose of receiving healthcare services from Defendants, which was compromised in and as a result of the Data Breach.

141. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from Private Information, especially her Social Security number, in combination with her name, being placed in the hands of unauthorized third parties and criminals.

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

***Plaintiff Q.Y's Experience***

143. Plaintiff Diane Young and her minor child Q.Y. (for purposes of this section,

"Plaintiff") first learned of the Data Breach when she received her Notice Letter on or about October 4, 2024. The Notice informed Plaintiff that Q.Y.'s Private Information was compromised in the Data Breach.

144. As a result of the Data Breach, Plaintiff has spent time dealing with the consequences of the Data Breach. This time has been lost forever and cannot be recaptured.

145. Upon information and belief, Q.Y.'s Private Information was in Defendants' computer systems during the Data Breach and remains in Defendants' possession.

146. Plaintiff has suffered actual injury in the form of damages to and diminution in the value of Private Information—a form of intangible property that Plaintiff entrusted to Defendants for the purpose of receiving healthcare services from Defendants, which was compromised in and as a result of the Data Breach.

147. Q.Y. is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from Private Information, especially Q.Y.'s Social Security number, in combination with her name, being placed in the hands of unauthorized third parties and criminals.

148. Plaintiff has a continuing interest in ensuring that Q.Y.'s Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

***Plaintiff Stephen Schlaugies' Experience***

149. Plaintiff Stephen Schlaugies (for purposes of this section, "Plaintiff") first learned of the Data Breach when he received his Notice Letter on or about October 4, 2024. The Notice informed Plaintiff that his Private Information was compromised in the Data Breach.

150. As a result of the Data Breach, Plaintiff has spent time dealing with the consequences of the Data Breach. This time has been lost forever and cannot be recaptured.

151. Upon information and belief, Plaintiff's Private Information was in Defendants' computer systems during the Data Breach and remains in Defendants' possession.

152. Plaintiff has suffered actual injury in the form of damages to and diminution in the value of Private Information—a form of intangible property that Plaintiff entrusted to Defendants for the purpose of receiving healthcare services from Defendants, which was compromised in and as a result of the Data Breach.

153. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from Private Information, especially his Social Security number, in combination with his name, being placed in the hands of unauthorized third parties and criminals.

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

## V. CLASS ALLEGATIONS

155. Plaintiffs bring this class action on behalf of themselves and on behalf of all others similarly situated pursuant to C.P.L.R. § 901 (2015), *et seq*. and other applicable law.

156. The Class that Plaintiffs seek to represent is defined as follows:

> All individuals whose Private Information was compromised during the Data Breach that occurred on or about September 10, 2024 (the "Class").

157. Excluded from the Class is the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which a Defendants has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards,

sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

158. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

159. This action is brought and may be maintained as a class action because there is a well-defined community of interest among many persons who comprise a readily ascertainable class. A well-defined community of interest exists to warrant class-wide relief because Plaintiffs and all members of the Class were subjected to the same wrongful practices by Defendants, entitling them to the same relief.

160. The Class is so numerous that individual joinder of its members is impracticable.

161. Common questions of law and fact exist as to members of the Class and predominate over any questions which affect only individual members of the Class. These common questions include, but are not limited to:

a. Whether and to what extent Defendants had a duty to protect the Private Information of Plaintiffs and Class Members;

b. Whether Defendants had a duty not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendants had a duty not to use the Private Information of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the Private Information of Plaintiffs and Class Members;

e. When Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed

Plaintiffs and Class Members that their Private Information had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

h. 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;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to actual, damages, and/or statutory damages as a result of Defendants' wrongful conduct;

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and

m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

162. Plaintiffs are members of the Class they seek to represent, and their claims and injuries are typical of the claims and injuries of the other Class Members.

163. Plaintiffs will adequately and fairly protect the interests of other Class Members. Plaintiffs have no interests adverse to the interests of absent Class Members. Plaintiffs are

represented by legal counsel with substantial experience in class action litigation. The interests of Class Members will be fairly and adequately protected by Plaintiffs and their counsel.

164. Defendants have acted or refused to act on grounds that apply generally to the Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class as a whole.

165. A class action is superior to other available means for fair and efficient adjudication of the claims of the Class and would be beneficial for the parties and the court. Class action treatment will allow a large number of similarly situated persons to prosecute their common claims in a single forum, simultaneously, efficiently, and without the unnecessary duplication of effort and expense that numerous individual actions would require. The amounts owed to the many individual Class Members are likely to be relatively small, and the burden and expense of individual litigation would make it difficult or impossible for individual members of the class to seek and obtain relief. A class action will serve an important public interest by permitting such individuals to effectively pursue recovery of the sums owed to them. Further, class litigation prevents the potential for inconsistent or contradictory judgments raised by individual litigation. Plaintiffs are unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

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

166. Plaintiffs and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 165 above.

167. Plaintiffs and the Class provided and entrusted Defendants with certain Private Information as a condition of receiving healthcare services based upon the premise and with the

understanding that Defendants would safeguard their information, use their Private Information for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

168. Defendants have full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

169. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiffs and the Class involved an unreasonable risk of harm to Plaintiffs and the Class, even if the harm occurred through the criminal acts of a third party.

170. Defendants had a duty to exercise reasonable care in overseeing, safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that the Private Information of Plaintiffs and the Class in Defendants' possession was adequately secured and protected.

171. Defendants owed a duty to Plaintiffs and the Class to implement intrusion detection processes that would detect a data breach or unauthorized access to their systems in a timely manner.

172. Defendants also had a duty to exercise appropriate clearinghouse practices to remove Private Information they were no longer required to retain pursuant to regulations, including that of former patients.

173. Defendants also had a duty to employ proper procedures to detect and prevent the improper access, misuse, acquisition, and/or dissemination of the Private Information of Plaintiffs

and the Nationwide Class.

174. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between both Defendants and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendants with their confidential Private Information, a necessary part of their relationship with Defendants.

175. Defendants owed a duty to disclose the material fact that Defendants' data security practices were inadequate to safeguard the Private Information of Plaintiffs and the Class.

176. Defendants' Privacy Policies acknowledge Defendants' duty to adequately protect the personal and medical information of Plaintiffs and the Class.

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

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

179. Defendants' own conduct created a foreseeable risk of harm to Plaintiffs and the Class. Defendants' misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included their decisions not to comply with industry standards for the safekeeping of the Private Information of Plaintiffs and the Class, including basic encryption techniques freely available to Defendants.

180. Plaintiffs and the Class had no ability to protect their Private Information that was

in, and likely remains in, Defendants' possession.

181. Defendants were in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

182. Defendants had and continues to have a duty to adequately disclose that the Private Information of Plaintiffs and the Class within Defendants' possession, how it was compromised, and precisely the types of data that was compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

183. Defendants has admitted that the Private Information of Plaintiffs and the Class was wrongfully accessed, acquired, and/or released to unauthorized third persons as a result of the Data Breach.

184. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiffs and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Private Information of Plaintiffs and the Class during the time the Private Information was within Defendants' possession or control.

185. Defendants improperly and inadequately safeguarded the Private Information of each Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

186. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect the Plaintiffs and the Class in the face of increased risk of theft.

187. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and the Class by failing to have appropriate procedures in place to detect unauthorized access or intrusions and prevent dissemination of their Private Information. Additionally,

Defendants failed to disclose to Plaintiffs and the Class that Defendants' security practices were inadequate to safeguard the Private Information of Plaintiffs and the Class.

188. Defendants breached their duty to exercise appropriate clearinghouse practices by failing to remove Private Information they were no longer required to retain pursuant to regulations, including Private Information of former patients.

189. Defendants, through their actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiffs and the Class the existence and scope of the Data Breach.

190. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

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

192. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will continue to suffer injury.

193. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of 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 their continued possession.

194. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class are entitled to and demand actual, consequential, and nominal damages.

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

195. Plaintiffs and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 165 above.

196. 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 Defendants, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

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

198. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

199. Plaintiffs and the Class are within the class of persons that the FTC Act was intended to protect.

200. The harm that occurred because of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, 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.

201. Defendants' violations of HIPAA and HITECH also independently constitute negligence *per se*.

202. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of patients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

203. Plaintiffs and Class Members are within the class of persons that HIPAA privacy laws were intended to protect.

204. The harm that occurred because of the Data Breach is the type of harm HIPAA privacy laws were intended to guard against.

205. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their Private Information is used; iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) 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 tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendants' possession and are subject to further unauthorized disclosures so long as Defendants fails to

undertake appropriate and adequate measures to protect the Private Information of Plaintiffs and the Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class.

**COUNT III**
**Breach of Implied Contract**
***(On Behalf of Plaintiffs and the Class against Defendant BCHP)***

206. Plaintiffs and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 165 above.

207. Defendant BCHP (for purposes of this count, "Defendant") required Plaintiffs and the Class to provide and entrust their Personal Information as a condition of receiving healthcare services with Defendant.

208. Plaintiffs and the Class paid money to Defendant in exchange for services, as well as Defendant's promises to protect their protected health information and other Private Information from unauthorized disclosure.

209. In its written Privacy Policy, Defendant expressly promised Plaintiffs and Class Members that Defendant would only disclose Private Information under certain circumstances, none of which relates to the Data Breach.

210. Defendant promised to comply with HIPAA and HITECH standards and to make sure that Plaintiffs and Class Members' Private Information would remain protected.

211. As a condition of obtaining medical care from Defendant, Plaintiffs and the Class provided and entrusted their Private Information. In so doing, Plaintiffs the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such

information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

212. A meeting of the minds occurred, as Plaintiffs and Class Members agreed, *inter alia*, to provide accurate and complete Private Information and to pay Defendant in exchange for Defendant's collective agreement to, *inter alia*, protect their Private Information.

213. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of Defendant's implied promise to adequately safeguard this confidential personal and medical information.

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

215. Defendant has breached the implied contracts it made with Plaintiffs and the Class by making their Private Information accessible from the Internet (regardless of any mistaken belief that the information was protected) and failing to make reasonable efforts to use the latest security technologies designed to help ensure that the Private Information was secure, failing to encrypt Plaintiffs and Class Members' Private Information, failing to safeguard and protect their Private Information, and by failing to provide timely and accurate notice to them that Private Information was compromised as a result of the data breach.

216. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to comply with its promise to abide by HIPAA and HITECH.

217. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1).

218. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).

219. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1).

220. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii).

221. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

222. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3).

223. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations in violation of 45 CFR 164.306(a)(94).

224. Defendant further breached the implied contracts with Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that

is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq*.

225. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing both oversight and physical administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c).

226. Defendant further breached the implied contracts with Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

227. Defendant's failure to meet these promises constitutes breach of the implied contracts.

228. Because Defendant allowed unauthorized access to Plaintiffs and Class Members' Private Information and failed to safeguard the Private Information, Defendant breached its contracts with Plaintiffs and Class Members.

229. Defendant breached its contracts by not meeting the minimum level of protection of Plaintiffs and Class Members' protected health information and other Private Information, because Defendant did not prevent against the Data Breach.

230. Furthermore, the failure to meet its confidentiality and privacy obligations resulted in Defendant providing medical services to Plaintiffs and Class Members that were of a diminished value.

231. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Class are now subject to the present and continuing risk of fraud, and are suffering (and will continue to suffer) the ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality

of the stolen confidential data; the diminished value of services provided by Defendant; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

232. As a result of Defendant's breach of implied contract, Plaintiffs and the Class are entitled to and demand actual, consequential, and nominal damages.

## COUNT IV
### Breach of Third-Party Beneficiary Contract
***(On Behalf of Plaintiffs and the Class against Defendant ATSG)***

233. Plaintiffs and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 165 above.

234. Defendant ATSG (for purposes of this count, "Defendant") entered into various contracts with its clients, including healthcare providers, to provide software services to its clients.

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

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

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

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

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

## COUNT V
## Unjust Enrichment
***(On Behalf of Plaintiffs and the Class against Defendants)***

240. Plaintiffs and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 165 above.

241. This Count is pled in the alternative to Count III, Breach of Implied Contract.

242. Plaintiffs and the Class conferred a benefit upon Defendants in providing Private Information to Defendants.

243. 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 Private Information, as this was used to facilitate their services to Plaintiffs and the Class.

244. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information.

245. Instead of providing a reasonable level of security, or retention policies, which would have prevented the Data Breach, Defendants instead calculated to avoid their data security

obligations at the expense of Plaintiffs and the Class by utilizing cheaper, ineffective security measures. Plaintiffs and the Class, on the other hand, suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

246. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiffs' and the Class's Private Information because Defendants failed to adequately protect it.

247. Plaintiffs and the Class have no adequate remedy at law.

248. 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 VI
### Violation of New York General Business Law § 349
***(On Behalf of Plaintiffs and the Class against Defendant BCHP)***

249. Plaintiffs and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 165 above.

250. The New York General Business Law ("GBL") § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

251. By reason of the conduct alleged herein, Defendant BCHP (for purposes of this count, "Defendant") has engaged in unlawful practices within the meaning of GBL § 349. The conduct alleged herein is a "business practice" within the meaning of GBL § 349, and the deception occurred within New York State.

252. Defendant stored Plaintiffs' and Class Members' Private Information on the aforementioned servers. Defendant knew or should have known it did not employ reasonable,

industry standard, and appropriate security measures that complied "with federal regulations" and that would have kept Plaintiffs' and Class Members' Private Information secure and prevented the loss or misuse of Plaintiffs' and Class Members' Private Information. Further, Defendant knew or should have known that they each did not employ reasonable third-party safeguards and oversight to ensure that Plaintiffs' and Class Members' Private Information was protected.

253. Plaintiffs and Class Members never would have provided their Private Information to Defendant if they had been told or knew that Defendant would fail to maintain sufficient security to keep such Private Information from being taken by others.

254. Defendant violated GBL § 349 by misrepresenting, both by affirmative conduct and by omission, the safety of Defendant's storage and services, specifically the security thereof, and its ability to safely store and dispose of Plaintiffs' and Class Members' Private Information.

255. Defendant also violated GBL § 349 by failing to implement reasonable and appropriate security measures or follow industry standards for data security, and by failing to immediately notify Plaintiffs and Class Members of the Data Breach. If Defendant had complied with these legal requirements, Plaintiffs and Class Members would not have suffered the damages related to the Data Breach.

256. Defendant's practices, acts, policies, and course of conduct violate GBL § 349 in that:

a. Defendant actively and knowingly misrepresented or omitted disclosure of material information to Plaintiffs and Class Members at the time it provided such Private

Information that Defendant did not have sufficient security or mechanisms to protect Private Information; and

b. Defendant failed to give timely warnings and notices regarding the defects and problems with the security of its computer systems to protect Plaintiffs' and Class Members' Private Information. Defendant possessed actual knowledge of the inherent risks in inadequate data security.

257. Plaintiffs and the Class were entitled to believe, and did believe, that Defendant would take appropriate measures to keep their Private Information safe. Defendant did not disclose that Plaintiffs' and Class Members' Private Information was vulnerable to malicious actors, and Defendant was the only one in possession of that material information, which it had a duty to disclose.

258. The aforementioned conduct constitutes an unconscionable commercial practice in that Defendant has, by the use of false or deceptive statements and/or knowing intentional material omissions, misrepresented and/or concealed the inadequate nature of its security practices, resulting in the Data Breach.

259. Members of the public were deceived by Defendant's misrepresentations and failures to disclose.

260. Such acts by Defendant are and were deceptive acts or practices which are and/or were likely to mislead a reasonable consumer providing his or her Private Information to Defendant. Said deceptive acts and practices are material. The requests for and use of such Private Information in New York through deceptive means occurring in New York were consumer-oriented acts and thereby falls under the New York consumer protection statute, GBL § 349.

261. Defendant's wrongful conduct caused Plaintiffs and Class Members to suffer a consumer-related injury by causing them to incur substantial expense to protect from misuse of the Private Information by third parties and placing Plaintiffs and Class Members at serious risk for monetary damages.

262. As a direct and proximate result of Defendant's violations of the above, Plaintiffs and Class Members suffered damages including, but not limited to: unauthorized use of their Private Information; theft of their personal and financial information; costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts; damages arising from the inability to use their Private Information; costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address an attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, initiating and monitoring credit freezes, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Data Breach; the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals; damages to and diminution in value of their Private Information entrusted to Defendant; and the loss of Plaintiffs' and Class Members' privacy.

263. In addition to or in lieu of actual damages, because of the injury, Plaintiffs and the Class seek statutory damages for each injury and violation which has occurred.

## PRAYER FOR RELIEF

**WHEREFORE**, Plaintiffs, on behalf of themselves and Class Members, requests judgment against Defendants and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiffs and her Counsel to

represent the Class;

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

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. prohibiting Defendants from further deceptive practices and making untrue statements about the Data Breach and the stolen Private Information

iii. requiring Defendants 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;

iv. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

v. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and 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;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

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

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendants to routinely and continually conduct internal training

and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

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

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face because of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' 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 Defendants' 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;

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

E. For an award of restitution and damages in an amount to be determined;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

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

**DEMAND FOR JURY TRIAL**

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

Dated: January 2, 2025

Respectfully submitted,

*/s/ Jeff Ostrow*

Jeff Ostrow (*pro hac vice*)
**KOPELOWITZ OSTROW P.A.**
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Telephone: 954.332.4200
ostrow@kolawyers.com

Jean S. Martin
**Morgan & Morgan**
**Complex Litigation Group**
201 North Franklin Street, 7th Floor
Tampa, FL 33606
T: (813) 223-5505
E: jeanmartin@forthepeople.com

Christian P. Levis, Esq.
**LOWEY DANNENBERG, P.C.**
44 South Broadway, Suite 1100
White Plains, NY 10601
Phone: (914) 997-0500
clevis@lowey.com

*Interim Co-Lead Class Counsel*

Lori G. Feldman
**GEORGE FELDMAN MCDONALD, PLLC**
102 Half Moon Bay Drive
Croton-on-Hudson, NY 10520
Phone: (888) 421-4529
lfeldman@4-justice.com

*Interim Liaison Counsel for Plaintiffs*

Raina C. Borrelli
**STRAUSS BORRELLI PLLC**
980 N. Michigan Avenue, Suite 1610
Chicago IL, 60611
T: (872) 263-1100
F: (872) 263-1109
raina@straussborrelli.com

Gary M. Klinger
**MILBERG COLEMAN PLLC**
227 W. Monroe Street Suite 2100
Chicago, IL 60606
T: 866-252-0878
gklinger@milberg.com

Katherine M. Aizpuru (No. 5305990)
**TYCKO & ZAVAREEI LLP**
2000 Pennsylvania Avenue, NW, Suite 1010
Washington, D.C. 20006
Phone: (202) 973-0900
kaizpuru@tzlegal.com

Jason S. Rathod
**Migliaccio & Rathod LLP**
412 H Street NE
Washington, D.C. 20002
Phone: (202) 470-3520
jrathod@classlawdc.com

*Plaintiffs' Executive Committee Members*