UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

PEYTON MCQUILLEN and CYNTHIA STOW, *on behalf of themselves and all others similarly situated*,	§	
Plaintiffs,	§	CASE NO. 2:24-CV-2271
vs.	§	CLASS ACTION COMPLAINT
CENCORA, INC. f/k/a AMERISOURCE-BERGEN CORPORATION, a Pennsylvania corporation, and THE LASH GROUP, LLC, a Delaware corporation,	§	JURY TRIAL DEMANDED
Defendants.	§	

Plaintiffs Peyton McQuillen and Cynthia Stow ("Plaintiffs") bring this Class Action Complaint against Cencora, Inc. f/k/a AmerisourceBergen Corporation and The Lash Group, LLC ("Defendants"), individually and on behalf of all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to their own actions and their counsel's investigations, and upon information and belief as to all other matters:

INTRODUCTION

1. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard certain personally identifiable information ("PII") and protected health information ("PHI"), which they held in their possession, including, but not limited to, Plaintiffs' and Class Members' full names, addresses, dates of birth, health diagnoses, medications, and prescriptions (collectively, "Private Information").

2. Defendant Cencora, Inc. f/k/a AmerisourceBergen Corporation "is a global healthcare solutions leader driving innovative partnerships with global manufacturers, providers, and pharmacies to improve product access and efficiency throughout the healthcare supply chain." Cencora Corporation website, available at https://investor.cencora.com/overview/default.aspx (last

visited May 28, 2024). It is in the Eastern Pennsylvania area.

3. Defendant The Lash Group, LLC represents itself as a subsidiary of AmerisourceBergen Corporation and as "a patient support services" company. *See* The Lash Group website, available at https://www.lashgroup.com/life-at-lash (last visited May 28, 2024). Cencora Corporation website, available at https://investor.cencora.com/overview/default.aspx. It is a Delaware entity located in the Eastern Pennsylvania area.

4. To provide their healthcare related services, Defendants collect and maintain Plaintiffs and Class Member Private Information, which included Protected Health Information ("PHI").

5. On February 21, 2024, Defendants became aware that an unauthorized party accessed Defendants' computer networks (the "Data Breach").

6. Defendants claim to have immediately investigated the Data Breach and confirmed that an unauthorized actor accessed Defendants' systems on February 21, 2024, and had access to files that included the following: full names, addresses, dates of birth, health diagnoses, medications, and prescriptions.

7. Defendants did not send notice of the Data Breach (the "Notice of Data Breach Letter") until on or around May 17, 2024, to Plaintiff Stow, and May 20, 2024, to Plaintiff McQuillen.

8. Plaintiffs' Notice of Data Breach states the following:

> On February 21, 2024, Cencora learned that data from its information systems had been exfiltrated, some of which could contain personal information. Upon initial detection of the unauthorized activity, Cencora immediately took containment steps and commenced an investigation with the assistance of law enforcement, cybersecurity experts and external lawyers. On April 10, 2024, we confirmed that some of your personal information was affected by the incident.
>
> Based on our investigation, personal information was affected, including potentially your first name, last name, addresses, date of birth, health diagnosis, and/or medications and prescriptions. There is no evidence that any of this information has been or will be publicly disclosed, or that any information was or will be misused for fraudulent

> purposes as a result of this incident, but we are communicating this to you so that you can take the steps outlined below to protect yourself.

9. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendants' inadequate safeguarding of Class Members' Personal and Private Health Information that they collected and maintained, and for failing to provide adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

10. Defendants maintained the Private Information in a reckless and negligent manner. In particular, the Private Information was maintained on Defendants' computer system and network in a condition vulnerable to cyberattack. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiffs' and Class Members' Personal and Private Health Information was a known risk to Defendants and thus Defendants were on notice that failing to take steps necessary to secure the Personal and Private Health Information from those risks left that information in a dangerous condition.

11. Because of the Data Breach, Plaintiffs and Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack and the substantial and imminent risk of identity theft.

12. By obtaining, collecting, using, and profiting 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 and intrusion. Defendants admits that the unencrypted Private Information impacted during the Data Breach.

13. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in

the hands of data thieves. The exposed Private Information of Plaintiffs and Class Members can-and likely will-be sold on the dark web. Indeed, Plaintiffs' and Class Members' Private Information has likely already been published on the dark web.

14. Hackers can offer for sale the unencrypted, unredacted Private Information to criminals. Plaintiffs and Class Members now face a lifetime risk of identity theft, though Defendants did not say Social Security numbers were included—though that is hard to believe.

15. This Private Information was compromised because of Defendants' negligent and/or careless acts and omissions and the failure to protect the Private Information of Plaintiffs and Class Members. In addition to Defendants' failure to prevent the Data Breach, after discovering the breach, Defendants waited months to report it to government agencies and affected individuals.

16. Because of this delayed response, Plaintiffs and Class Members had no idea their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their lifetimes.

17. Plaintiffs bring this action on behalf of all persons whose Private Information was compromised because of Defendants' failure to: (i) adequately protect the Private Information of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendants' inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendants' conduct amounts to negligence and violates federal and state statutes.

18. Plaintiffs and Class Members have suffered injury because of Defendants' conduct. These injuries include: (i) lost or diminished value of Private Information; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (iii) lost time and opportunity costs associated with

attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, lost time, and (iv) the continued and exacerbated to their Private Information which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up 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.

19. Defendants disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the Private Information of Plaintiffs and Class Members was safeguarded. Defendants also disregarded their rights by failing to take available steps to prevent an unauthorized disclosure of data and failing to follow applicable, required, and appropriate protocols, policies and procedures for the encryption of data, even for internal use.

20. Because of the Data Breach, the Private Information of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

21. Plaintiff Peyton McQuillen is a Citizen of Boca Raton, Florida and intends to remain there throughout this litigation. He was a patient of Defendants.

22. Plaintiff Cynthia Stow is a Citizen of Yadkinville, North Carolina and intends to remain there throughout this litigation. She was a patient of Defendants.

23. Defendant Cencora, Inc. f/k/a AmerisourceBergen Corporation is a Pennsylvania-entity with its principal place of business at 1 W 1st Ave, Conshohocken, PA 19428-1800.

JURISDICTION AND VENUE

24. This Court has subject matter jurisdiction over this action under the Class Action

Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members exceeds 100, many of whom have different citizenship from Defendants. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

25. This Court has personal jurisdiction over Defendants because they operate and are headquartered in this District and conduct substantial business in this District.

26. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(l) because a substantial part of the events giving rise to this action occurred in this District. Defendants are also based in this District, maintain Plaintiffs' and Class Members' Private Information in this District, and have caused harm to Plaintiffs and Class Members from or in this District.

FACTUAL ALLEGATIONS

Defendants' Business

27. Defendants provide healthcare solutions globally. In the ordinary course of receiving health care services from Defendants, each patient must provide (and Plaintiffs did provide) Defendant with sensitive, personal, and private information, such as their:

- Name, address, phone number, and email address;
- Date of birth;
- Social Security number
- Demographic information;
- Driver's license or state or federal identification;
- Information relating to the individual's dental and medical history;
- Insurance information and coverage; and
- Banking and/or credit card information.

28. Defendants also create and store medical/dental records and other protected health information for their patients, including records of treatments and diagnoses.

29. All of Defendants' employees, staff, entities, sites, and locations may share patient information with each other for various purposes, as should be disclosed in a HIPAA compliant privacy notice ("Privacy Policy") that Defendants are required to maintain.

30. Upon information and belief, Defendants' HIPAA Privacy Policies are provided to every patient prior to receiving treatment and upon request.

31. Defendants agreed to and undertook legal duties to maintain the protected health and personal information entrusted to them by Plaintiffs and Class Members safely, confidentially, and in compliance with all applicable laws, including the Health Insurance Portability and Accountability Act ("HIPAA").

32. The patient and employee information held by Defendants in their computer systems and networks included the Private Information of Plaintiffs and Class Members.

The Data Breach

33. On February 21, 2024, Defendants became aware that an unauthorized party accessed their computer network.

34. Following an investigation, Defendants confirmed that an unauthorized party had access to Plaintiffs' and Class Members' Private Information.

35. The Private Information accessed and exfiltrated was likely not encrypted because if properly encrypted, then cybercriminals would not have acquired and accessed Plaintiffs' and Class Members' Private Information.

36. Defendants had obligations under contract, industry standards, and common law to reasonably protect and safeguard Plaintiffs' and Class Members' Private Information from unauthorized access.

37. Defendant had obligations created by HIPAA, contract, industry standards, common law, and representations made to Class Members, to keep Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

38. The patient information held by Defendants in computer system and network included the Private Information of Plaintiffs and Class Members.

39. By obtaining, collecting, using, and profiting from Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible to protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

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

41. Plaintiffs and Class Members relied on Defendants to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosure of this Private Information.

42. Plaintiffs and Class Members directly or indirectly entrusted Defendants with sensitive and confidential information, including their Private Information, which includes information that is static, does not change, and can be used to commit myriad financial crimes.

43. Plaintiffs and Class Members relied on Defendants 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 Defendants safeguard their Private Information.

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

45. On information and belief, Defendants maintained the Private Information of Plaintiffs

and Class Members, including, but not limited to, the following: full names, addresses, dates of birth, and Private Health information.

46. 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 the exposure of Private Information.

47. Because Defendants failed to use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiffs and Class Members, upon information and belief, cybercriminals infiltrated Defendants' systems and stole Plaintiffs' and Class Members' Private Information.

48. The unencrypted PII and PHI of Plaintiffs and Class Members will likely end up for sale on the dark web as that is the *modus operandi* of hackers. In addition, unencrypted PII and PHI may fall into the hands of companies that will use the detailed PII and PHI for targeted marketing without the approval of Plaintiffs and Class Members. In turn, unauthorized individuals can easily access the PII and PHI of Plaintiffs and Class Members.

49. Defendants admitted that Private Information potentially impacted in the Data Breach contained full names, addresses, dates of birth, and private health information.

50. Because Defendants failed to properly protect safeguard Plaintiffs' and Class Members' Private Information, an unauthorized third party was able to access Defendants' network, and access Plaintiffs' and Class Members' Private Information stored on Defendants' systems.

Plaintiffs' Experience

51. Plaintiffs entrusted their Private Information to Defendants to receive health-related services from Defendants.

52. Plaintiffs' Private Information was within the possession and control of Defendants at the time of the Data Breach.

53. Plaintiffs provided their Private Information to Defendants and trusted that the information would be safeguarded according to internal policies and state and federal law.

54. On or around May 17 and May 20, 2024, Defendants notified Plaintiff Stow and Plaintiff McQuillen, respectively, that Defendants' networks had been accessed and Plaintiffs' Private Information may have been involved in the Data Breach.

55. The HHS requires "[i]f a breach of unsecured protected health information affects *500 or more individuals*, a covered entity must notify the Secretary of the breach without unreasonable delay and in *no case later than 60 calendar days* from the discovery of the breach."[1] Further, if "the number of individuals affected by a breach is uncertain at the time of submission, the covered entity should provide an estimate," and later provide an addendum or correction to HSS.[2] Plaintiffs have been unable to find such a notice.

56. Plaintiffs are very careful about sharing their sensitive Private Information. Plaintiffs have never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

57. Plaintiffs store any documents containing their sensitive Private Information in a safe and secure location or destroy the documents. Moreover, Plaintiffs diligently choose unique usernames and passwords for their various online accounts.

58. Because of the Data Breach, Defendants directed Plaintiffs to take certain steps to protect their Private Information and otherwise mitigate their damages.

59. Because of the Data Breach, Plaintiffs spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and

[1] https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html (last viewed May 29, 2024) (emphasis added).
[2] *Id.*

self-monitoring their accounts to ensure no fraudulent activity has occurred and set up a credit alert. This time has been lost forever and cannot be recaptured. And this time was spent at Defendants' direction by way of the Data Breach notice where Defendants recommended that Plaintiffs mitigate their damages by, among other things, monitoring their accounts for fraudulent activity.

60. Even with the best response, the harm caused to Plaintiffs cannot be undone.

61. Plaintiffs suffered actual injury in the form of damages to and diminution in the value of Plaintiffs' Private Information-a form of intangible property that Plaintiffs entrusted to Defendants, which was compromised in and because of the Data Breach. Plaintiffs suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and have anxiety and increased concerns for the loss of their privacy.

62. Plaintiffs have suffered imminent and impending injury arising from the exacerbated of fraud, identity theft, and misuse resulting from their Private Information being placed in the hands of unauthorized third parties and possibly criminals.

63. Plaintiffs have a continuing interest in ensuring that their Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

The Data Breach was Foreseeable.

64. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[3]

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

[3] *See* How to Protect Your Networks from **RANSOMWARE**, at 3, *available at* https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/ransomware (last accessed May 29, 2024).

breach.

66. Considering recent high profile cybersecurity incidents across the country, Defendants knew or should have known that their electronic records would be targeted by cybercriminals.

67. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so that they are aware of, and prepared for, a potential attack.[4]

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

Value of Private Information

69. The Private Information of individuals remains of high value to criminals, as shown by the prices they will pay through the dark web. Many 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.[5] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[6] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[7]

70. For these reasons, the information compromised in the Data Breach is far 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.

71. This data demands a much higher price on the black market. Martin Walter, senior

---

[4] FBI, Secret Service Warn of Targeted, Law360 (Nov.18,2019), *available at* https://www.law360.com/articles/1220974/fbisecret-service-wam-of-targeted-ransomware.

[5] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at:* https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed May 29, 2024).

[6] *Here's How Much Your Personal Information Is Selling for on the Dark Web,* Experian, Dec. 6, 2017, *available at:* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed May 29, 2024).

[7] *In the Dark,* VPNOverview, 2019, *available at:* https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed May 29, 2024).

director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information... [is] worth more than 10x on the black market."[8]

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

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

74. Drug manufacturers, device manufacturers, pharmacies, hospitals, and healthcare service providers often purchase PII and PHI 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 PII and PHI to adjust their insureds' insurance premiums.

75. According to account monitoring company LogDog, private data, such as PII and PHI, sells for $50 and up on the Dark Web.[9]

76. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and between when PII and PHI is stolen and when they are used. According to the U.S. Government Accountability Office ("GAO"), which studied 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.[10]

77. At all relevant times, Defendants knew, or reasonably should have known, of the

---

[8] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers,* IT World, (Feb. 6, 2015), *available at:* https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html last accessed May 29, 2024).

[9] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals,* Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last accessed May 29, 2024).

[10] *Report to Congressional Requesters,* GAO, at 29 (June 2007), *available at: https://www.gao.gov/assets/gao-07-737.pdf* (last accessed May 29, 2024).

importance of safeguarding the PII and PHI of Plaintiffs and Class Members and the foreseeable consequences that would occur if Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members because of a breach.

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

79. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' network, amounting to potentially millions of individuals' detailed, personal information and thus the significant number of individuals who would be harmed by the exposure of the unencrypted data.

80. 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 PII and PHI of Plaintiffs and class Members.

81. As a condition of providing healthcare-related services, processing claims, sending bills, and providing services related to treatment, Defendants require that their customers entrust them with Private Information.

82. By obtaining, collecting, using, and profiting from Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

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

84. Plaintiffs and the Class Members relied on Defendants to implement and follow

adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business purposes, and to prevent the unauthorized disclosures of the Private Information.

Defendants Acquires, Collects, and Stores the Private Information of Plaintiffs and Class Members

85. Defendants acquired, collected, and stored the Private Information of Plaintiffs and Class Members.

86. 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 they were responsible for protecting the PII and PHI from disclosure.

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

Defendants Failed to Properly Protect Plaintiffs' and Class Members' Private Information

88. Defendants could have prevented this Data Breach by properly securing and encrypting the systems containing the Private Information of Plaintiffs and Class Members. Alternatively, Defendants could have destroyed the data, especially for individuals with whom they had not had a relationship for some time.

89. Defendants' negligence in safeguarding the PII and PHI of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendants to protect and secure sensitive data they possess.

90. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII and PHI of Plaintiffs and Class Members from being compromised.

91. 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."

92. The ramifications of Defendants' failure to keep secure the PII and PHI of Plaintiffs and Class Members are long-lasting and severe. Once PII or PII is stolen, fraudulent use of that information and damage to victims may continue for years.

93. To prevent and detect unauthorized cyber-attacks, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should know about the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and Domain Keys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set antivirus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls-including file, directory, and network share permissions-

with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[11]

94. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks . . ..

- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Monitor the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) . . ..

- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

[11] *Id.* at 3-4.

- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it . . ..

- **Verify email senders.** If you are unsure whether an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters-and keep them updated-to reduce malicious network traffic.[12]

95. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in **security discussions**

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

[12] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last accessed May 24, 2024).

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[13]

96. Given that Defendants were storing the PII and PHI of Plaintiffs and Class Members, Defendants could and should have implemented all the above measures to prevent and detect cyberattacks.

97. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII and PHI of Plaintiffs and Class Members.

98. As the result of computer systems needing security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendants negligently and unlawfully failed to safeguard Plaintiff' and Class Members' Private Information.

99. Because Defendants failed to properly protect safeguard Plaintiffs' and Class Members' Private Information, an unauthorized third party was able to access Defendants' network, and access Defendants' database and system configuration files.

100. Specifically, Defendants admits that on or around February 12, 2024, an unauthorized party accessed Defendants' network and deleted databases and system configuration files.

[13] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last accessed May 29, 2024).

101. Given that Defendants were storing the PII and PHI of Plaintiffs and Class Members, Defendants could and should have implemented all the above measures to prevent and detect cyberattacks.

102. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII and PHI of Plaintiffs and Class Members.

103. As the result of computer systems needing security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendants negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

Defendants' Conduct Violates HIPAA and Evidences their Insufficient Data Security

104. HIPAA requires covered entities such as Defendants to protect against reasonably anticipated threats to the security of sensitive patient health information.

105. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

106. 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 PII like the data Defendants left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a) (1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

107. A Data Breach such as the one Defendants experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

A breach under the HIPAA Rules is defined as, "...the acquisition,

> access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40.

108. Defendants' Data Breach resulted from a combination of insufficiencies that demonstrate they failed to meet mandated by HIPAA regulations.

Defendants violated FTC Guidelines

109. The Federal Trade Commission ("FTC") has promulgated many guides for businesses which show how important it is to implement reasonable data security practices. According to the FTC, the need for data security should influence all business decision-making.

110. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[14]

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

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

[14] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

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

114. Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' PII and PHI constitutes an unfair act or practice prohibited by Section *5* of the FTC Act, 15 U.S.C. § 45.

115. Defendants were always fully aware of their obligation to protect the PII and PHI of Plaintiffs and Class members. Defendants were also aware of the significant repercussions that would result from their failure to do so.

Defendants failed to meet Industry Standards

116. As shown above, experts studying cyber security routinely identify the healthcare industry as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which is collected and maintained.

117. Several best practices have been identified that at a minimum should be implemented by healthcare service providers like Defendants, including, but not limited to, educating all employees; strong passwords; multi-layer security, including firewalls, antivirus, and antimalware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

118. Other best cybersecurity practices that are standard in the healthcare services industry 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; and training staff regarding critical points.

119. 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-I, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-I, PR.DS-1, PR.DS-5, PR.PT-I, PR.PT-3, DE.CM-I, 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.

120. The foregoing frameworks are existing and applicable industry standards in the healthcare services industry, and Defendants failed to meet accepted standards, thereby opening the door to and causing the Data Breach.

Defendants' Negligent Acts and Breaches

121. Defendants breached their obligations to Plaintiffs and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

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

b. Failing to adequately protect the Personal and Private Health Information of Plaintiffs and the Class;

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

d. Failing to train employees in the proper handling of emails containing links cyber-attackers used to first access Defendants' networks, and to and maintain adequate email security practices;

e. Failing to put into place proper procedures, software settings, and data security software protections to adequately protect against a blunt force intrusion;

f. Failing to ensure the confidentiality and integrity of electronic PHI they created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(l);

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

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(l)(ii)(D);

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

k. Failing to comply with FTC guidelines for cybersecurity, in violation of Section *5* of the FTC Act; Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

l. Failing to train all members of Defendant's workforce effectively on the policies and procedures about PHI as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); and/or

m. Failing to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as they had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 C.F.R. § 164.304, definition of "encryption"); and

n. Failing to adhere to industry standards for cybersecurity.

122. As the result of antivirus and malware protection software needing security updating, inadequate procedures for handling phishing emails or emails containing viruses or other malignant computer code, and other failures to maintain their networks in configuration that would protect against cyberattacks like the one here, Defendants negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Personal and Private Health Information by allowing/providing unsecured and unencrypted Personal and Private Health Information to Defendants which in tum allowed cyberthieves to access their IT systems.

123. Accordingly, as outlined below, Plaintiffs and Class Members now face an increased risk of fraud and identity theft.

Because Defendants Failed to Safeguard Private Information, Plaintiffs and the Class Members have Experienced Substantial Harm and Will Face Significant Risk of Continued Identity Theft.

124. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their PII and PHI that can be directly traced to Defendants.

125. The ramifications of Defendants' failure to keep Plaintiffs' and the Class's PII and PHI secure are severe. Identity theft occurs when someone uses another's Personal and Private Health Information such as that person's name, financial account number(s), Social Security number, driver's license number, date of birth, PHI, and/or other information, without permission, to commit fraud or other crimes. According to experts, one out of four data breach notification recipients become a victim of identity fraud.

126. As a result of Defendants' failures to prevent-and to timely detect-the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII and PHI is used;

b. The diminution in value of their PII and PHI;

c. The compromise and continuing publication of their PII and PHI;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

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

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII and PHI; and

h. The continued risk to their PII and PHI, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fails to undertake the

appropriate measures to protect the PII and PHI in their possession.

127. Stolen PII and PHI is one of the most valuable commodities on the criminal information black market According to Experian, a credit-monitoring service, stolen PII and PHI can be worth up to $1,000.00 depending on the type of information obtained.

128. The value of Plaintiffs' and the proposed Class's PII and PHI on the black market is considerable. Stolen PII and PHI trades on the black market for years, and criminals often post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

129. It can take victims years to spot identity or PII/PHI theft, giving criminals plenty of time to milk that information for cash.

130. One such example of criminals using PII and PHI for profit is the development of "Fullz" packages.

131. Cyber-criminals can cross-reference two sources of PII and PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

132. The development of "Fullz" packages means that stolen PII and PHI from the Data Breach can easily be used to link and identify it to Plaintiffs' and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII and PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that

Plaintiffs' and other members of the proposed Class's stolen PII and PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

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

134. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good" Defendants did not rapidly report to Plaintiffs and the Class that their PII and PHI had been stolen.

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

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

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

138. The Federal Trade Commission ("FTC'') has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data

is currency."[15]

139. The FTC has also issued many guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.

140. According to the FTC, unauthorized PHI disclosures ravage consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout.[16] The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

141. Defendants' failure to properly notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs' and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

Plaintiffs' and Class Members' Damages

[15] Statement of FTC Commissioner Pamela Jones Harbour-Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009), https://www.ftc.gov/news-events/news/speeches/remarks-ftc-exploring-privacy-roundtable (last visited May 29, 2024).

[16] *See* Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen (last visited May 29, 2024)

142. To date, Defendants have done little to provide Plaintiffs and Class Members with relief for the damages they have suffered because of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach. Defendants have only offered 24 months of inadequate identity monitoring services, despite Plaintiffs and Class Members being at risk of identity theft and fraud for the remainder of their lifetimes.

143. The 24 months of credit monitoring offered to persons whose Private Information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face ongoing identity theft and financial fraud for the rest of their lives. What's more, Defendants places the burden squarely on Plaintiffs and Class Members by requiring them to expend time signing up for that service rather than automatically enrolling all victims of this Data Breach.

144. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

145. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

146. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, financial or medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

147. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members.

148. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs

directly or indirectly related to the Data Breach.

149. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

150. Defendants provided no compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' Private Information.

151. Plaintiffs and Class Members have been damaged by the compromise of their Personal and Private Health Information in the cyber-attack. Moreover, Defendants' delay in noticing affected persons of the theft of their Private Information prevented early mitigation efforts and compounded the harm.

152. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out- of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

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

f. Closely reviewing and monitoring financial, medical, and bank accounts; and credit reports for unauthorized activity for years to come.

153. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Personal and Private Health Information, which is believed to remain in the possession of Defendants, is protected from further breaches by implementing security measures and safeguards, including, but

not limited to, making sure that the storage of data or documents containing Personal and Private Health Information is inaccessible online and that access to such data is password protected.

CLASS ALLEGATIONS

154. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of others similarly situated under Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

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

> All persons whose Private Information was actually or potentially accessed or acquired during the Data Breach (the "Class").

156. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; 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.

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

158. Numerosity, Fed R. Civ. P. 23(a)(l): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are an excess of 10,000 individuals whose Private Information may have been improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendants' records.

159. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members.

These include:

- Whether and to what extent Defendants had a duty to protect the Private Information of Plaintiffs and Class Members;
- Whether Defendants had duties not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;
- Whether Defendants had duties not to use the Private Information of Plaintiffs and Class Members for non-business purposes;
- Whether Defendants failed to adequately safeguard the Private Information of Plaintiffs and Class Members;
- When Defendants learned of the Data Breach;
- Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII and PHI had been compromised;
- Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class Members that their PII and PHI had been compromised;
- 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;

1. 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 Defendants violated the consumer protection statutes invoked herein;

l. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages from Defendants' wrongful conduct;

m. Whether Plaintiffs and Class Members are entitled to restitution because of Defendants' wrongful conduct; and

n. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced because of the Data Breach.

160. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their PII and PHI compromised because of the Data Breach, based

on Defendants' misfeasance.

161. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged here apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendants' conduct toward the Class as a whole, not on facts or law applicable only to Plaintiff.

162. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

163. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged here; it will permit many Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the

courts.

164. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

165. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

166. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

167. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the Private Information of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

168. Defendants have acted or refused to act on grounds generally applicable to the Classes and thus final injunctive or corresponding declaratory relief for the Class Members is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

169. Likewise, issues under Rule 23(c)(4) are appropriate for certification because such

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

- Whether Defendants owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- Whether Defendants breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- Whether Defendants violated their own policies and applicable laws, regulations, and industry standards relating to data security;
- Whether an implied contract existed between Defendants on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;
- Whether Defendants breached the implied contract;
- Whether Defendants adequately and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;
- 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;
- Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members; and
- Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief because of Defendants' wrongful conduct.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Putative Rule 23 Class)

170. Plaintiffs and the Class repeat and re-allege every allegation as if fully set forth herein.

171. Plaintiffs and the Class entrusted Defendants with their Private Information.

172. Plaintiffs and the Class entrusted their Private Information to Defendants on the premise and with the understanding that Defendants would safeguard their information, use their PII and PHI for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

173. Defendants know about 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.

174. 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.

175. Defendants had a duty to exercise reasonable care in 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 Members in Defendants' possession was adequately secured and protected.

176. Defendants also had a duty to exercise appropriate clearinghouse practices to remove Private Information they were no longer required to retain under regulations.

177. Defendants also had a duty to have procedures in place to detect and prevent the improper access and misuse of the Private Information of Plaintiffs and the Class.

178. Defendants' duty to use reasonable security measures arose because of the special relationship that existed between 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 obtaining services from Defendants.

179. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs or the Class.

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

181. 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 importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendants' systems.

182. 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 asset 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.

183. Plaintiffs and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendants' possession.

184. Defendants could protect against the harm suffered by Plaintiffs and the Class because of the Data Breach.

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

186. Defendants had a duty to employ proper procedures to prevent the unauthorized dissemination of the Private Information of Plaintiffs and the Class.

187. Defendants have admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

188. 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.

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

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

191. 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 and prevent dissemination of Private Information.

192. Defendants breached their duty to exercise appropriate clearinghouse practices by failing to remove Private Information they were no longer required to retain under regulations.

193. 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.

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

195. 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 Plaintiffs and the Nationwide Class. The Private Information of Plaintiffs and Class Members was lost and 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.

196. Defendants' duty of care to use reasonable security measures arose because of the special relationship that existed between Defendants and its patients, including Plaintiffs, which is recognized by laws and regulations including, but not limited to, HIPAA, as well as common law. Defendants could ensure that their systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs and Class Members from the Data Breach or a data breach.

197. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all the healthcare, dental, and/or medical information at issue constitutes "protected health information" within the meaning of HIPAA.

198. Additionally, 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.

199. 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. Defendants' conduct was particularly unreasonable given the nature and amount of PII and PHI they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

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

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

202. The harm attributable to 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.

203. As a direct and proximate result of Defendants' negligence and 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 present and continuing 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 is 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) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the effect of the Private Information compromised because of the Data Breach for the rest of the lives of Plaintiffs and the Class.

204. As a direct and proximate result of Defendants' negligence and negligence *per se,* Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

205. Additionally, as a direct and proximate result of Defendants' negligence and negligence *per se,* Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain 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.

206. As a direct and proximate result of Defendants' negligence and negligence *per se,* Plaintiffs and the Class have a right to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Putative Rule 23 Class)

207. Plaintiffs and the Class repeat and re-allege every allegation as if fully set forth herein.

208. Plaintiffs and the Class entrusted their Private Information to Defendants. In so doing, Plaintiffs and the Class entered implied contracts with Defendants by which Defendants 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.

209. In entering such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations, including HIPAA, and adhered to industry standards.

210. In their privacy policies, Defendants represented that they would not disclose Plaintiffs and Class Members' Private Information to unauthorized third parties.

20S. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendants.

206. Defendants breached the implied contracts they made with Plaintiffs and the Class by failing to safeguard and protect their personal information, by failing to delete the information of

Plaintiffs and the Class once the relationship ended, and by failing to provide timely and accurate notice to them that personal information was compromised because of the Data Breach.

207. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiffs and the Class have suffered (and will continue to suffer) 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 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.

208. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiffs and the Class have a right to recover actual, consequential, and nominal damages.

COUNT III
NEGLIGENCE PER SE
(On behalf of Plaintiffs and the Putative Rule 23 Class)

209. Plaintiffs and the Class repeat and re-allege every allegation as if fully set forth herein.

210. Pursuant to Federal Trade Commission, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

211. Under HIPAA, 42 U.S.C. § 1302d, et seq., Defendants had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information.

212. Under HIPAA, Defendants had a duty to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a

low probability of assigning meaning without use of a confidential process or key." *See* definition of encryption at 45 C.F.R. § 164.304.

213. Defendants breached their duties to Plaintiffs and Class Members under the Federal Trade Commission Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

214. Defendants breached their duties to Plaintiffs and Class Members under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

215. Defendants' failure to comply with applicable laws and regulations constitutes negligence per se.

216. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

217. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties, and that Defendants' breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

218. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered an injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT IV
BREACH OF FIDUCIARY DUY
(On behalf of Plaintiffs and the Putative Rule 23 Class)

219. Plaintiffs and the Class repeat and re-allege every allegation as if fully set forth herein.

220. In light of the special relationship between Defendants and Plaintiffs and Class

Members, under which Defendants became guardian of Plaintiffs and Class Members' Private Information, Defendants became a fiduciary by their undertaking and guardianship of the Private Information, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendants did and does store.

221. Defendants have a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of Defendants' relationship with their patients, in particular, to keep secure their Private Information.

222. Defendants breached their fiduciary duties to Plaintiffs and Class Members by failing to diligently discovery, investigate, and give notice of the Data Breach in a reasonab1e and practicable period.

223. Defendants breached their fiduciary duties to Plaintiffs and Class Members by failing to encrypt or otherwise protect the integrity of the systems containing Plaintiffs and Class Members' Private Information.

224. Defendants breached their fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

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

226. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with

effort expended and the loss of productivity addressing and attempting to mitigate the actual and consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the rest of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendants' services they received

227. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Putative Rule 23 Class)

228. Plaintiffs and the Class repeat and re-allege every allegation as if fully set forth herein.

229. Plaintiffs and Class Members conferred a monetary benefit on Defendants, by providing Defendants with their valuable Private Information.

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

231. Rather than provide a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to avoid their data security obligations at the expense of Plaintiffs and Class Members by using cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

232. Under the principles of equity and good conscience, Defendants should not be

permitted to retain the monetary value of the benefit belonging to Plaintiffs and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

233. Defendants acquired the monetary benefit and PII and PHI through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

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

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

236. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, 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 consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect Private Information in their continued possession and (vii) future costs in terms of time, effort, and money to be expended to prevent, detect, contest, and repair the effect of the Private Information compromised because of the Data Breach for the rest of the lives of Plaintiffs and Class Members.

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

238. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them.

COUNT VI
DECLARATORY AND INJUNCTIVE RELIEF
(On behalf of Plaintiffs and the Putative Rule 23 Class)

239. Plaintiffs and the Class repeat and re-allege every allegation as if fully set forth herein.

240. Plaintiffs pursue this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

241. Defendants owe a duty of care to Plaintiffs and Class Members that require them to adequately secure Plaintiffs' and Class members' Private Information.

242. Defendants failed to fulfill their duty of care to safeguard Plaintiffs' and Class Members' Private Information.

243. As described above, actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual obligations and duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class members are at risk of additional or further harm. due to the exposure of their Private Information and Defendants' failure to address the security failings that led to such exposure.

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

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

a. Defendant owes a legal duty to secure its clients' patients' Private Information and to

timely notify them of a data breach under the common law, HIPAA, and the FTCA;

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

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

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

e. Ordering that Defendants purge, delete, and destroy, in a reasonably secure manner, any Private Information unnecessary for their provision of services;

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

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

PRAYER FOR RELIEF

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

A. For an Order certifying the Class, and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein relating to the misuse and/or disclosure of the PII and PHI of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any 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. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. 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;

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

v. prohibiting Defendants from maintaining the PII and PHI of Plaintiffs and Class Members on a cloud-based database;

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 their 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' systems;

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 their respective employees' knowledge of the education programs discussed in the preceding

subparagraphs, as well as randomly and periodically testing employee's 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, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

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

F. For prejudgment interest on all amounts awarded; and

G. Any other relief that this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand that this matter be tried before a jury.

Date: May 29, 2024,

Respectfully submitted,

/s/ Ethen Ostroff

ETHEN OSTROFF LAW
Ethen Ostroff
Pennsylvania Bar: 326660
eo@ethenostrofflaw.com
21 East 5th Ave, STE 102
Conshohocken, PA 19428
Phone: 215-767-9477

ELLZEY & ASSOCIATES, PLLC
Jarrett L. Ellzey (*pro hac vice* forthcoming)
Texas Bar No. 24040864
jarrett@ellzeylaw.com
Leigh S. Montgomery (*pro hac vice* forthcoming)
Texas Bar No. 24052214
leigh@ellzeylaw.com
Alexander G. Kykta (*pro hac vice* forthcoming)
Texas Bar No. 24107841
alex@ellzeylaw.com
1105 Milford Street
Houston, Texas 77006
Phone: (888) 350-3931
Fax: (888) 276-3455

ATTORNEY TOM & ASSOCIATES
Tom Kherkher (*pro hac vice* forthcoming)
Texas Bar No. 24113389
tom@attorneytom.com
5909 West Loop South Suite 525
Houston, Texas 77401
Phone: (855) 866-9467

ATTORNEYS FOR PLAINTIFF