UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF FLORIDA

ABIGAIL WALECKI, on behalf of herself and all others similarly situated, Plaintiff, vs. NORTH BROWARD HOSPITAL DISTRICT d/b/a BROWARD HEALTH, Defendants.	Case No. _____-Civ-

CLASS ACTION COMPLAINT
JURY TRIAL DEMANDED

Plaintiff Abigail Walecki ("Plaintiff"), by and through her attorneys, upon personal knowledge as to herself and her own acts and experiences, and upon information and belief as to all other matters, alleges as follows:

INTRODUCTION

1. This class action arises out of the recent data breach ("Data Breach") involving Defendant North Broward Hospital District d/b/a Broward Health ("Defendant" or "Broward Health"), one of the largest public health systems in the United States.

2. Broward Health failed to reasonably secure, monitor, and maintain the Protected Health Information ("PHI") and Personally Identifiable Information ("PII") stored on its network. As a result, Plaintiff and approximately 1.35 million other patients ("Class Members") have had the most sensitive details of their lives and identities accessed and exfiltrated by malicious cybercriminals intent on causing harm.

3. The PII and PHI accessed and exfiltrated in the breach includes patients' full names, dates of birth, addresses, phone numbers, financial and bank account information, Social Security numbers, insurance information, account numbers, medical information including history, condition, treatment and diagnoses, medical record numbers, driver's license numbers, and email addresses (collectively, "Sensitive Information").

4. By obtaining, collecting, using, and deriving a benefit from the Sensitive Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that Sensitive Information from unauthorized access and intrusion. Defendant's conduct in breaching these duties amounts to negligence and/or recklessness and violates federal and state statutes.

5. Plaintiff brings this action on behalf of all persons whose Sensitive Information was compromised as a result of Defendant's failure to take reasonable steps to protect the Sensitive Information of Plaintiff and Class Members and warn Plaintiff and Class Members of Defendant's inadequate information security practices. Defendant disregarded the rights of Plaintiff and Class Members by knowingly failing to implement and maintain adequate and reasonable measures to ensure that the PII and PHI of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the use of and access to data for internal and external use.

6. In this era of frequent data security attacks and data breaches, particularly in the healthcare industry, Defendant's failures leading to the Data Breach are particularly egregious.

7. As a direct and proximate result of Defendant's data security failures and the Data Breach, the PII and PHI of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party, and Plaintiff and Class Members have suffered actual, concrete and imminent injury. These injuries include: (i) lost or diminished value of PII and PHI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (iii) lost 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 certainly increased risk to their PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI; (iv) the invasion of privacy; (v) the compromise, disclosure, theft, and unauthorized use of

Plaintiff's and the Class Member's PII and PHI; and (vi) emotional distress, fear, anxiety, nuisance and annoyance related to the theft and compromise of their PII and PHI.

8. Plaintiff has already experienced attempted health insurance fraud as a direct and proximate result of the Data Breach and Defendant's failure to adequately secure and maintain the Sensitive Information on its network.

9. Plaintiff seeks to remedy these harms, and prevent any future data compromise on behalf of herself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and remains at risk due to Defendant's inadequate data security.

10. Plaintiff 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.

11. Accordingly, Plaintiff, on behalf of herself and other Class Members, asserts claims for negligence, negligence *per se*, breach of contract, breach of implied contract, breach of confidence, unjust enrichment, and declaratory judgment. Plaintiff seeks injunctive relief, declaratory relief, monetary damages, and all other relief as authorized in equity or by law.

THE PARTIES

Defendant Broward Health

12. Defendant Broward Health is a public, non-profit hospital system governed by the North Broward Hospital District Board of Commissioners, a seven-member district board appointed by the Governor and confirmed by the Florida Senate.

Plaintiff Abigail Walecki

13. Plaintiff Abigail Walecki is a natural person domiciled in the State of Virginia. Her permanent residence is located in the State of Virginia.

14. Plaintiff Walecki was a patient of Broward Health in 2019 and provided her Sensitive Information to Defendant in the course of receiving treatment.

15. Plaintiff received a letter dated January 1, 2022 from Defendant concerning the Data Breach. The letter stated that "[o]n October 15, 2021, an intruder … gained unauthorized access to the Broward Health network …." It further stated that Broward Health's investigation "confirmed" that Plaintiff's "personal medical information was included in data accessed by the intruder."

16. The letter received by Plaintiff goes on to state that Plaintiff's "name, address, date of birth, phone number, financial or bank account information, Social Security number, insurance information and account number, medical information including history, condition, treatment and diagnosis, medical record number, driver's license number, and email address" were all "exfiltrated" or "removed" by the "intruder."

17. In November 2021, Plaintiff was the victim of attempted fraud when an unknown individual submitted a false medical claim for payment under Plaintiff's name to Plaintiff's health insurance company.

18. Plaintiff learned of this after receiving an email from her health insurance company indicating that a doctor reached out to determine if he was in Plaintiff's insurance network. Upon receiving this email, Ms. Walecki researched the doctor's name and discovered that he was a doctor from a different state and not associated with any care that she had received. Ms. Walecki responded to her insurance company via email that she did not recognize the name of the doctor and that this was not care that she requested.

19. Plaintiff spent a significant amount of time researching the details of the Data Breach and learning how to monitor her information following a breach involving PII and PHI.

This was time she otherwise would have spent performing other activities, such as her job and/or leisure activities for the enjoyment of life.

20. Knowing that a hacker stole her Sensitive Information, and that her Sensitive Information may be available for sale on the dark web, has caused Ms. Walecki great concern. She is now very concerned about medical identity theft, and identity theft in general.

21. Now, due to Defendants' misconduct and the resulting Data Breach, hackers obtained her Sensitive Information at no compensation to Ms. Walecki whatsoever. That is money gained for the hackers – who could sell her Sensitive Information on the dark web.

22. Moreover, Ms. Walecki suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Sensitive Information being placed in the hands of criminals.

23. Ms. Walecki has a continuing interest in ensuring her Sensitive Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

24. To the best of her knowledge, prior to the activity described above during the period in which the Data Breach occurred, Ms. Walecki's PHI and PII had never been stolen or compromised.

25. Additionally, Ms. Walecki never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

26. Ms. Walecki stores any and all electronic and paper documents containing her PHI PII in a safe and secure location.

JURISDICTION & VENUE

27. 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. There are more than 100 putative class members and at least some members of the proposed Class, including Plaintiff, have a different citizenship from Broward Health. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. §1367 because all claims alleged herein form part of the same case or controversy.

28. This Court has jurisdiction over Broward Health because it maintains and operates healthcare facilities in this District. Defendant is authorized to and conducts business in this District and is subject to general personal jurisdiction in this state.

29. Venue is proper in this Court pursuant to 28 U.S.C. §1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District, Broward Health operates healthcare facilities within this District, and Broward Health has caused harm to Class Members residing in this District.

FACTUAL ALLEGATIONS

Background

30. Broward Health operates four hospitals and more than 30 healthcare facilities in the South Florida region, including Broward Health Medical Center, Broward Health North, Broward Health Imperial Point, Broward Health Coral Springs, Salah Foundation Broward Health Children's Hospital, and Broward Health Weston.

31. In the course of providing healthcare services, Broward Health requires patients to provide their Sensitive Information. As a result, when patients are treated by a Broward Health healthcare facility, their highly sensitive PII and PHI is stored on centralized servers maintained by Broward Health.

32. Upon information and belief, Broward Health obtains and stores the PII and PHI of hundreds of thousands, if not millions, of individuals every year. For example, in the year 2020

alone, Broward Health handled 252,576 physician practice visits, 246,031 emergency department visits, 163,402 outpatient medical center visits, 79,040 children's diagnostics and treatment center visits, 77,223 primary care visits, 52,244 hospital admissions, 17,662 Broward Health Weston visits, 14,656 home health and hospice visits, 13,714 outpatient surgeries, 11,834 inpatient surgeries, and 4,798 newborn admissions.

33. Broward Health maintains a "Notice of Privacy Practices for Protected Health Information" which describes how confidential patient information is used and disclosed. Broward Health represents that it: "will abide by the most stringent of the regulations as they pertain to Protected Health Information, including obtaining your prior written authorization, as required, before any such information is disclosed to a third party."

34. The Notice of Privacy Practices states that Broward Health is required by law to satisfy the following duties:

- Maintain the privacy of Protected Health Information
- Provide you with a notice of our legal duties and privacy practices with respect to Protected Health Information
- In the event of a breach of your unsecured Protected Health Information, Broward Health will provide written or other notification in accordance with federal and state law.

35. Broward Health also maintains a "Code of Conduct" intended to demonstrate its "commitment to maintaining a culture of compliance." As part of its Code, Broward Health states that it will "maintain[] the confidentiality of patient and other information in accordance with legal and ethical standards, and breaches will not be tolerated."

36. In order to fulfill its commitment to "protect patient and property information," Broward Health states that it will:

- Establish confidentiality and privacy policies and procedures that adhere to the Health Insurance Portability and Accountability Act (HIPAA).
- Respect and protect patients' health and personal information in all forms, including paper, electronic, verbal, telephonic, social media, etc.
- Only access a patient's chart when involved in that patient's care or for a legitimate work-related reason such as billing, administrative, teaching or research requirements. Access is limited to only the minimum amount necessary to complete the related work.
- Refrain from revealing information unless it is supported by a legitimate clinical or business purpose need, in compliance with our policies and procedures and applicable laws, rules and regulations.
- Refrain from discussing patient information in public, including, but not limited to, elevators, hallways or dining areas.
- Maintain computer workstations responsibly and refrain from sharing computer identification information and passwords. Carefully manage and maintain confidential and proprietary information to protect its value.
- Refrain from disclosing other Broward Health financial information, including the healthcare system's financial performance and contract pricing for goods and services, without prior, appropriate approval.
- Refrain from using or sharing "insider information," which is not otherwise available to the general public.

37. Broward Health also permits third-party providers, contractors, volunteers, physicians, and other individuals who perform services on behalf of Broward Health to access its systems and networks for various purposes. Broward Health requires these parties execute a "Confidentiality and Data Security Agreement" whereby they acknowledge that "Broward Health has a legal and ethical responsibility to safeguard the privacy of all patients" and agree to "protect the confidentiality of all information that [they] use, originate, discover, or develop in the performance of [their] duties at Broward Health."

38. Among other requirements, the Confidentiality and Data Security Agreement provides that "Broward Health maintains audit trails of access to information and system activity and that the audit trail may be reviewed at any time."

The Data Breach

39. According to Broward Health, on October 15, 2021, a malicious actor gained unauthorized access to the Broward Health network. This network contained the sensitive personal, medical, and financial information of its current and former patients.

40. According to Broward Health, it did not detect the intrusion to its network until October 19, 2021. Upon information and belief, during this time, malicious actors maintained unfettered access to Broward Health's network and exfiltrated copious amounts of Sensitive Information.

41. According to Broward Health, the investigation revealed that "the intrusion occurred through the office of a third-party medical provider who is permitted access to the system to provide healthcare services."

42. Defendant did not disclose the existence of the Data Breach until January 1, 2022, when it began mailing notice letters to victims.

43. A disclosure by Broward Health to the office of the Maine attorney general revealed that the breach impacted 1,357,879 individuals.

44. In letters to victims of the Data Breach, Defendant states that it will take steps to prevent recurrence of similar incidents, including "enhanced security measures" and the "implementation of multifactor authentication for all users of its systems." Defendant also states that it has "begun implementation of minimum-security requirements" for all devices accessing its

network. However, these are industry-standard measures that should have been taken *before* the Data Breach. The failure to do so is inexcusable.

45. The notification letters provided to Plaintiff and Class Members recommend several time-consuming steps that victims of the Data Breach can take to try to mitigate the risk of future fraud and identity theft, such as fraud alerts and credit freezes.

46. Acknowledging the risk of identity theft and fraud caused by the Data Breach, Defendant offered Plaintiff and Class Members a two-year subscription to credit monitoring and identity protection services. Upon information and belief, Defendant has not offered to extend this credit monitoring longer than two years despite Plaintiff and Class Members facing a substantial risk of fraud and identity theft both now and for years to come.

47. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

(a) Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

(b) 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 DomainKeys Identified Mail (DKIM) to prevent email spoofing.

(c) Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

(d) Configure firewalls to block access to known malicious IP addresses.

(e) Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

(f) Set anti-virus and anti-malware programs to conduct regular scans automatically.

(g) 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.

(h) 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.

(i) 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.

(j) 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.

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

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

(m) Execute operating system environments or specific programs in a virtualized environment.

(n) Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

48. To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

(a) **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….

(b) **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). Pay attention to 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)….

(c) **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.

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

(e) **Verify email senders**. If you are unsure whether or not 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.

(f) **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.

(g) **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[1]

49. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

(a) **Secure internet-facing assets**

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

(b) **Thoroughly investigate and remediate alerts**

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

(c) **Include IT Pros in security discussions**

[1] *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 visited Jan. 11, 2021).

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

(d) **Build credential hygiene**

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

(e) **Apply principle of least-privilege**

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

(f) **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].[2]

50. Given that Defendant was storing the PII and PHI of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

51. The occurrence of the Data Breach and information disclosed to date by Defendant indicates that Defendant failed to adequately implement one or more of the above measures to

[2] *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 visited Jan. 11, 2021).

prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII and PHI of Plaintiff and approximately 1.35 million Class Members.

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

Defendant Knew or Should Have Known of the Risk Because the Healthcare Sector is Particularly Susceptible to Cyber Attacks

53. The seriousness with which Defendant should have taken its data security is shown by the number of data breaches perpetrated in the healthcare industry over the past few years.

54. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[3] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that victims were often forced to pay out of pocket costs for healthcare they did not receive in order to restore coverage.[4] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to

[3] *See* Identity Theft Resource Center, *2018 End -of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-end-of-year-data-breach-report/ (last visited Nov. 11, 2021).

[4] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited Jan. 11, 2021).

resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impacts the economy as a whole.[5]

55. Healthcare related data breaches continue to rapidly increase. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported having a significant security incident within the previous 12 months, and most of these known incidents being caused by "bad actors," such as cybercriminals.[6] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[7]

56. Over 41 million patient records were breached in 2019, with a single hacking incident affecting close to 21 million records.[8] Healthcare breaches in 2019 almost tripled those

---

[5] *See id*.

[6] *See 2019 HIMSS Cybersecurity Survey, available at*: https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last visited Jan. 11, 2021).

[7] *See* Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited Jan. 11, 2021).

[8] Heather Landi, *Number of patient records breached nearly triples in 2019*, FIERCE HEATLHCARE (Feb. 20, 2020), https://www.fiercehealthcare.com/tech/number-patient-records-breached-2019-almost-tripled-from-2018-as-healthcare-faces-new-threats#:~:text=Over%2041%20million%20patient%20records,close%20to%2021%20million%20records (last visited Jan. 11, 2021).

the healthcare industry experienced in 2018, when 15 million patient records were affected by data breach incidents, according to a report from Protenus and DataBreaches.net.[9]

57. Protenus, a healthcare compliance analytics firm, analyzed data breach incidents disclosed to the U.S. Department of Health and Human Services or the media during 2019, finding that there has been an alarming increase in the number of data breaches of patient privacy since 2016, when there were 450 security incidents involving patient data.[10] In 2019 that number jumped to 572 incidents, which is likely an underestimate, as two of the incidents for which there were no data affected 500 dental practices and clinics and could affect significant volumes of patient records. There continues to be on average at least one health data breach every day.[11]

58. One recent report found that in 2020, healthcare was one of the industries most affected by tracked ransomware incidents.[12]

59. As a healthcare provider, Defendant knew or should have known the importance of safeguarding PII and PHI entrusted to it, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Defendant failed, however, to take reasonable cybersecurity measures to prevent the Data Breach.

---

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] Kat Jerich, *Healthcare hackers demanded an average ransom of $4.6 last year, says BakerHostetler*, HEALTHCARE IT NEWS (May 4, 2021), https://www.healthcareitnews.com/news/healthcare-hackers-demanded-average-ransom-46m-last-year-says-bakerhostetler (last visited Dec. 23, 2021).

60. Defendant had the resources to invest in the necessary data security and protection measures. Yet, Defendant failed to exercise reasonable care in the hiring and/or supervision of its employees and agents and failed to undertake adequate analyses and testing of its own systems, adequate personnel training, and other data security measures to avoid the failures that resulted in the Data Breach.

PII & PHI are Very Valuable

61. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[13] 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."[14]

62. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[15]

---

[13] 17 C.F.R. § 248.201 (2013).

[14] *Id.*

[15] *The Information Marketplace: Merging and Exchanging Consumer Data*, FTC (Mar. 13, 2001), *transcript available* at http://www.ftc.gov/news-events/events-calendar/2001/03/information-marketplace-merging-exchanging-consumer-data (last visited Dec. 23, 2021).

63. Consumers rightfully place a high value not only on their PII and PHI, but also on the privacy of that data. Researchers have already begun to shed light on how much consumers value their data privacy – and the amount is considerable. Notably, one study on website privacy determined that U.S. consumers valued the restriction of improper access to their personal information – the very injury at issue here – between $11.33 and $16.58 per website. The study also determined that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49 – 44.62."[16] This study was done in 2002, almost twenty years ago. The sea-change in how pervasive the Internet is in everyday lives since then indicates that these values—when associated with the loss of PII and PHI to bad actors—would be exponentially higher today.

64. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[17] Experian reports that a stolen credit or debit card number can

[16] Il-Horn Hann, Kai-Lung Hui, *et al*, *The Value of Online Information Privacy: Evidence from the USA and Singapore*, at 17. Marshall Sch. Bus., Univ. So. Cal. (Oct. 2002), https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited Dec. 23, 2021).

[17] *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 visited Jan. 11, 2021).

sell for $5 to $110 on the dark web.[18] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[19]

The PII and PHI at Issue Here is Particularly Valuable to Hackers

65. Credit card and bank account numbers are tempting targets for hackers, but credit and debit cards can be cancelled, quickly mitigating the hackers' ability to cause further harm. Instead, PHI and types of PII that cannot be easily changed (such as names, dates of birth, and Social Security numbers) are the most valuable to hackers.[20]

66. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[21]

67. The Social Security Administration ("SSA") stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards

---

[18] *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 visited Jan. 11, 2021).

[19] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Jan. 11, 2021).

[20] *Calculating the Value of a Data Breach – What Are the Most Valuable Files to a Hacker?* Donnellon McCarthy Enters., https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/ (last visited Dec. 23, 2021).

[21] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Jan. 11, 2021).

> and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[22]

68. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns.[23] Victims of the Data Breach will spend, and already have spent, time contacting various agencies, such as the Internal Revenue Service and the SSA. They also now face a real and imminent substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

69. Social Security numbers cannot easily be replaced. In order to obtain a new Social Security number a person must prove, among other things, that he or she continues to be disadvantaged by the misuse. Thus, no new Social Security number can be obtained until the damage has been done.

70. Furthermore, as the SSA warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.

---

[22] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 11, 2021).

[23] When fraudulent tax returns are filed, the requirements for a legitimate taxpayer to file their tax returns with the IRS increase, including the necessity to obtain and utilize unique PIN numbers just to be able to file a tax return.

> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[24]

71. PHI is just as, if not more, valuable than Social Security numbers. According to a report by the Federal Bureau of Investigation's ("FBI") Cyber Division, healthcare records can be sold by criminals for 50 times the price of stolen Social Security numbers or credit card numbers.[25] A file containing private health insurance information can be bought for between $1,200 and $1,300 ***each*** on the black market.[26]

72. Similarly, the most recent edition of the annual Baker Hostetler Data Security Incident Response Report found that in 2020, hackers in ransomware attacks made an average initial ransomware demand of $4,583,090 after obtaining PHI. In 2020, final payouts to hackers committing ransomware attacks involving PHI averaged $910,335.[27]

73. Companies recognize that PII and PHI are valuable assets. Indeed, PII and PHI are valuable commodities. A "cyber black-market" exists in which criminals openly post stolen PII

---

[24] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Dec. 23, 2021).

[25] *FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI (April 8, 2014), https://publicintelligence.net/fbi-health-care-cyber-intrusions/ (last visited Dec. 23, 2021).

[26] Elizabeth Clarke, *Hackers Sell Health Insurance Credentials, Bank Accounts, SSNs and Counterfeit Documents*, SecureWorks (July 15, 2013), https://www.secureworks.com/blog/general-hackers-sell-health-insurance-credentials-bank-accounts-ssns-and-counterfeit-documents (last visited Dec. 23, 2021).

[27] Jerich, *supra* n.12.

and PHI on a number of Internet websites. Plaintiff's and Class Members' compromised PII has a high value on both legitimate and black markets.

74. Some companies recognize PII, and especially PHI, as a close equivalent to personal property. Software has been created by companies to value a person's identity on the black market. The commoditization of this information is thus felt by consumers as theft of personal property in addition to an invasion of privacy.

75. Moreover, compromised health information can lead to falsified information in medical records and fraud that can persist for years as it "is also more difficult to detect, taking twice as long as normal identity theft."[28]

76. Because much of the Sensitive Information exposed in the Data Breach is of a permanent and continuing nature, there may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[29]

77. Plaintiff 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.

---

[28] *See* FBI, *supra* n.25.

[29] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Jan. 11, 2021).

78. The physical, emotional, and social toll suffered (in addition to the financial toll) by identity theft victims also cannot be understated.[30] A 2016 Identity Theft Resource Center survey of identity theft victims sheds light on the prevalence of this emotional suffering caused by identity theft: 74 percent of respondents reported feeling stressed, 69 percent reported feelings of fear related to personal financial safety, 60 percent reported anxiety, 42 percent reported fearing for the financial security of family members, and 8 percent reported feeling suicidal.[31]

Defendant's Conduct Violates HIPAA

79. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of PHI. Covered entities, including Defendant, must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[32]

80. 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 PHI—the type of data Defendant failed to safeguard. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

---

[30] https://www.lifelock.com/learn/identity-theft-resources/lasting-effects-of-identity-theft (last visited Jan. 11, 2021).

[31] *Id.*

[32] *See* HIPAA Journal, *What is Considered Protected Health Information Under HIPAA?, available at:* https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/ (last visited Jan. 11, 2021).

81. Defendant's Data Breach resulted from a combination of insufficiencies demonstrating Defendant failed to comply with safeguards mandated by HIPAA regulations. Defendant's security failures include, but are not limited to:

(a) Failing to ensure the confidentiality and integrity of electronic protected health information that Defendant creates, receives, maintains, and transmits, in violation of 45 C.F.R. §164.306(a)(1);

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

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

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

(e) Failing to protect against any reasonably–anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 C.F.R. §164.306(a)(2);

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

(g) Failing to ensure compliance with HIPAA security standard rules by its workforce, in violation of 45 C.F.R. §164.306(a)(94);

(h) Impermissibly and improperly using and disclosing protected health information that is, and remains, accessible to unauthorized persons, in violation of 45 C.F.R. §164.502, *et seq.*; and

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

Defendant's Post-Breach Activity Was (and Remains) Inadequate

82. Immediate notice of a security breach is essential to protect victims such as Plaintiff and Class Members. Defendant failed to provide such immediate notice, thus further exacerbating the harm to Plaintiff and Class Members resulting from the Data Breach.

83. Such failure to protect Plaintiff's and Class Members' PII and PHI, and timely notify them of the Data Breach, has significant ramifications. The information stolen allows criminals to commit theft, identity theft, and other types of fraud. Moreover, because the data points stolen are persistent—for example, names, dates of birth, Social Security numbers, and health information—as opposed to transitory, criminals who access, stole, or purchase the PII and PHI belonging to Plaintiff and the Class Members, do not need to use the information to commit fraud immediately. The PII and PHI can be used or sold for use years later, and often is.

84. Plaintiff and Class Members are now at a significant risk of imminent and future fraud, misuse of their PII and PHI, and identity theft for many years in the future as a result of the Defendant's actions and the Data Breach. The theft of their PHI is particularly impactful, as many banks or credit card providers have substantial fraud detection systems with quick freeze or cancellation programs in place, whereas the breadth and usability of PHI allows criminals to get away with misuse for years before healthcare-related fraud is spotted.

85. Plaintiff and Class Members have suffered real and tangible losses, including but not limited to the loss in the inherent value of their PII and PHI, the loss of their time as they have had to spend additional time monitoring accounts and activity, and additional economic loss to mitigate the costs of injuries realized as a result of discovery in this case, but until recently, kept silent by Defendant.

86. Despite Defendant's egregious failure to protect Plaintiff's and Class Members' Sensitive Information, it has only offered to provide Plaintiff and Class Members with trivial compensation or remedy, such as two-years of credit monitoring or identity protection services.

CLASS ACTION ALLEGATIONS

87. Pursuant to the provisions of Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), and 23(c)(4), Plaintiff seeks to bring this class action on behalf of herself and a nationwide class (the "Class") defined as:

> **All persons who reside in the United States whose Sensitive Information was compromised by the Data Breach.**

88. Excluded from the Class are Defendant; officers, directors, and employees of Defendant; any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the Judges and Court personnel in this case and any members of their immediate families.

89. Plaintiff reserves the right to modify and/or amend the Class definition, including but not limited to creating additional subclasses, as necessary.

90. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

91. All Class Members are readily ascertainable in that Defendant has access to addresses and other contact information for all Class Members, which can be used for providing notice to Class Members.

92. ***Numerosity***. The Class is so numerous that joinder of all members is impracticable. The Class includes roughly 1.35 million individuals whose Sensitive Information was compromised by the Data Breach.

93. ***Commonality and Predominance***. There are numerous questions of law and fact common to Plaintiff and the Class that predominate over any questions that may affect only individual Class Members, including the following:

- whether Defendant engaged in the wrongful conduct alleged in this Complaint;
- whether Defendant's conduct was unlawful;
- whether Defendant failed to implement and maintain reasonable systems and security procedures and practices to protect customers' personal data;
- whether Defendant failed to exercise reasonable care in the hiring of its employees and agents;
- whether Defendant failed to exercise reasonable care in the supervision of its employees and agents;
- whether Defendant unreasonably delayed in notifying affected customers of the Data Breach;
- whether Defendant owed a duty to Plaintiff and Class Members to adequately protect their personal data and to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;
- whether Defendant breached its duties to protect the personal data of Plaintiff and Class Members by failing to provide adequate data security and failing to provide timely and adequate notice of the Data Breach to Plaintiff and the Class;
- whether Defendant's conduct was negligent;
- whether Defendant knew or should have known that its computer systems were vulnerable to attack;

- whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach of its systems, resulting in the loss of Class Members' personal data;
- whether Defendant wrongfully or unlawfully failed to inform Plaintiff and Class Members that it did not maintain computers and security practices adequate to reasonably safeguard customers' personal data;
- whether Defendant should have notified the public, Plaintiff, and Class Members immediately after it learned of the Data Breach;
- whether Plaintiff and Class Members suffered injury, including ascertainable losses, as a result of Defendant's conduct (or failure to act);
- whether Plaintiff and Class Members are entitled to recover damages; and
- whether Plaintiff and Class Members are entitled to declaratory relief and equitable relief, including injunctive relief, restitution, disgorgement, and/or other equitable relief.

94. ***Typicality***. Plaintiff's claims are typical of the claims of the Class in that Plaintiff, like all Class Members, had their personal data compromised, breached, and stolen in the Data Breach. Plaintiff and all Class Members were injured through the uniform misconduct of Defendant, described in this Complaint, and assert the same claims for relief.

95. ***Adequacy***. Plaintiff and counsel will fairly and adequately protect the interests of the Class. Plaintiff retained counsel who are experienced in Class action and complex litigation. Plaintiff has no interests that are antagonistic to, or in conflict with, the interests of other Class Members.

96. ***Superiority***. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class Members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendant's

violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiff and Class Members have been harmed by Defendant's wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to Defendant's conduct and/or inaction. Plaintiff knows of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action. Class certification is appropriate under Fed. R. Civ. P. 23(b)(1)(A), in that the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action conserves judicial resources and the parties' resources and protects the rights of each Class member. Specifically, injunctive relief could be entered in multiple cases, but the ordered relief may vary, causing Defendant to have to choose between differing means of upgrading its data security infrastructure and choosing the court order with which to comply. Class action status is also warranted because prosecution of separate actions by the Class Members would create the risk of adjudications with respect to individual Class Members that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

97. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3), because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

98. Particular issues are also appropriate for certification under Fed. R. Civ. P. 23(c)(4) because the claims present particular, common issues, the resolution of which would materially

advance the resolution of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

(a) Whether Plaintiff's and Class Members' PII and PHI were accessed, compromised, or stolen in the Data Breach;

(b) Whether (and when) Defendant knew about the Data Breach before it notified Plaintiff and Class Members and whether Defendant failed to timely notify Plaintiff and Class Members of the Data Breach;

(c) Whether Defendant owed a legal duty to Plaintiff and the Class;

(d) Whether Defendant failed to take reasonable steps to safeguard the PII and PHI of Plaintiff and Class Members;

(e) Whether Defendant failed to adequately monitor its data security systems;

(f) Whether Defendant failed to comply with its applicable laws, regulations, and industry standards relating to data security;

(g) Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiff's and Class Members' PII or PHI secure;

(h) Whether Defendant's adherence to HIPAA regulations, FTC data security obligations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach.

99. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Defendant, through its uniform conduct, acted or failed and refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole. Moreover, Defendant continues to maintain its inadequate security practices, retains possession of Plaintiff's and Class Members' PII and PHI, and has not been forced to change its practices or to

relinquish PII and PHI by nature of other civil suits or government enforcement actions, thus making injunctive and declaratory relief a live issue and appropriate to the Class as a whole.

COUNT I
Negligence

100. Plaintiff incorporates paragraphs 1-99 of the Complaint as if fully set forth herein.

101. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Sensitive Information, and 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.

102. Defendant had a common law duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' Sensitive Information.

103. Defendant systematically failed to provide adequate security for data in its possession.

104. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Sensitive Information within Defendant's possession.

105. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' Sensitive Information.

106. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the Sensitive Information within Defendant's possession might have been compromised and precisely the type of information compromised.

107. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Sensitive Information to be compromised.

108. As a result of Defendant's ongoing failure to notify Plaintiff and Class Members regarding what type of Sensitive Information has been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

109. Defendant's breaches of duty caused Plaintiff and Class Members to suffer injuries, including ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of value of the compromised PII and PHI; illegal sale of the compromised PII and PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach, reviewing bank statements, payment card, statements, insurance statements, and credit reports; expenses and time spent initiating fraud alerts, decreased credit scores and ratings; lost time; other economic harm; and emotional distress.

COUNT II
Negligence *Per Se*

110. Plaintiff incorporates paragraphs 1-99 of the Complaint as if fully set forth herein.

111. Plaintiff and Class Members were required to provide non-public PII and PHI in order to obtain medical services.

112. As a healthcare provider, Defendant is covered by HIPAA, 45 C.F.R. § 160.102, and is therefore obligated to comply with all rules and regulations under 45 C.F.R. Parts 160 and 164.

113. 45 C.F.R. Part 164 governs "Security and Privacy," with Subpart A providing "General Provisions," Subpart B regulating "Security Standards for the Protection of Electronic Protected Health Information," Subpart C providing requirements for "Notification in the Case of

Breach of Unsecured Protected Health Information," and Subpart E governing "Privacy of Individually Identifiable Health Information."

114. 45 C.F.R. § 164.104 states that the "standards, requirements, and implementation specifications adopted under this part" apply to covered entities and their business associates, such as Defendant.

115. Defendant is obligated under HIPAA to, among other things, "ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits" and "protect against any reasonably anticipated threats or hazards to the security or integrity of such information." 45 C.F.R. § 164.306.

116. 45 C.F.R. Sections 164.308 (Administrative safeguards), 164.310 (Physical safeguards), 164.312 (Technical safeguards), 164.314 (Organizational requirements), and 164.316 (Policies and procedures and documentation requirements) provide mandatory standards that all covered entities must adhere to.

117. Defendant violated HIPAA by failing to adhere to and meet the required standards as set forth in 45 C.F.R. §§164.308, 164.310, 164.312, 164.314, and 164.316.

118. Likewise, HIPAA regulations require covered entities "without unreasonable delay and in no case later than 60 calendar days after discovery of the breach" to "notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of" a data breach. 45 C.F.R. §164.404. The notice must also contain a minimum amount of information regarding the breach (including the dates of the breach and its discovery), the types of protected health information that were involved, steps individuals should take to protect themselves from harm resulting from the

breach, a description of what the entity is doing to investigate the breach and mitigate harm, and contact information to obtain further information. *Id.*

119. Defendant breached its notification obligations under HIPAA by failing to give timely and complete notice of the breach to Plaintiff and Class Members.

120. HIPAA requires Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. §164.530(c)(1). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

121. HIPAA further requires Defendant to disclose the unauthorized access and theft of the PII and PHI to Plaintiff and Class Members "without unreasonable delay" so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and detect misuse of their PII and PHI. *See* 45 C.F.R. §164.404.

122. Defendant violated HIPAA by failing to reasonably protect Plaintiff's and Class Members' PII and PHI and by failing to give timely and complete notice, as described herein.

123. Additionally, Section 5 of the Federal Trade Commission Act ("FTC Act") prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII and PHI. 15 U.S.C. §45(a)(1).

124. Pursuant to the Fair Credit Reporting Act ("FCRA"), Defendant had a duty to adopt, implement, and maintain adequate procedures to protect the security and confidentiality of Plaintiff's and Class Members' PII. *See* 15 U.S.C. §1681(b).

125. Defendant violated the state and federal statutes identified above by failing to use reasonable measures to protect PII and PHI of Plaintiff and Class Members and not complying with applicable industry standards, as described herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

126. Defendant's violation of state and federal statutes constitutes negligence *per se*.

127. Plaintiff and the Class Members are within the class of persons the state and federal statutes identified above were designed to protect.

128. The harm that occurred as a result of the breach is the type of harm the state and federal statutes were intended to guard against.

129. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members have suffered, and continue to suffer, damages arising from the breach as described herein and are entitled to compensatory, consequential, and nominal damages in an amount to be proven at trial.

130. Such injuries include those described above, including: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of value of the compromised PII and PHI; illegal sale of the compromised PII and PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach, reviewing bank statements, payment card, statements, insurance statements, and credit reports; expenses and time spent initiating fraud alerts, decreased credit scores and ratings; lost time; other economic harm; and emotional distress.

COUNT III
Breach of Contract

131. Plaintiff incorporates paragraphs 1-99 of the Complaint as if fully set forth herein.

132. Defendant disseminated a "Notice of Privacy Practices" to its patients which constitutes an agreement between Defendant and persons who provided their Sensitive Information to Defendant, including Plaintiff and Class Members.

133. Plaintiff and Class Members formed a contract with Defendant and complied with all obligations under such contract when they provided Sensitive Information to Defendant subject to the Notice of Privacy Practices.

134. Defendant promised in the Notice of Privacy Practices that it would "abide by the most stringent of the regulations as they pertain to Protected Health Information, including obtaining your prior written authorization, as required, before any such information is disclosed to a third party" and to not disclose information unless as authorized. Defendant further promised it would "[m]aintain the privacy of Protected Health Information."

135. Defendant breached its agreements with Plaintiff and Class Members when Defendant allowed for the disclose of Plaintiff's and Class Members' Sensitive Information without their authorization and in a manner that was inconsistent with the permissible authorizations set forth in the Notice of Privacy Practices, as well as when it failed to maintain the confidentiality of Plaintiff's and Class Members' medical and treatment information.

136. As a direct and proximate result of these breaches, Plaintiff and Class Members sustained actual losses and damages as alleged herein, including that they did not receive the benefits of the bargains for which they paid. Plaintiff and Class Members alternatively seek an award of nominal damages.

COUNT IV
Breach of Implied Contract

137. Plaintiff incorporates paragraphs 1-99 of the Complaint as if fully set forth herein.

138. Plaintiff and Class Members were required to provide their Sensitive Information to Defendant in order to receive healthcare services and treatment.

139. As part of these transactions, Defendant agreed to safeguard and protect the Sensitive Information of Plaintiff and Class Members. Implicit in these transactions between Defendant and Class Members was the obligation that Defendant would use the Sensitive Information for approved business purposes only and would not make unauthorized disclosures of the information or allow unauthorized access to the information.

140. Additionally, Defendant implicitly promised to retain this Sensitive Information only under conditions that kept such information secure and confidential and therefore had a duty to reasonably safeguard and protect the Sensitive Information of Plaintiff and Class Members from unauthorized disclosure or access.

141. Plaintiff and Class Members entered into implied contracts with the reasonable expectation that Defendant's data security practices and policies were reasonable and consistent with industry standards. Plaintiff and Class Members believed that Defendant would use part of the monies paid to Defendant under the implied contracts to fund adequate and reasonable data security practices to protect their Sensitive Information.

142. Plaintiff and Class Members would not have provided and entrusted their Sensitive Information to Defendant or would have paid less for Defendant's services in the absence of the implied contract between them and Defendant. The safeguarding of Plaintiff's and Class Members' Sensitive Information was critical to realizing the intent of the parties.

143. The nature of Defendant's implied promise itself—the subject matter of the contractual provision at issue—was to protect Plaintiff's and Class Members' Sensitive Information in order to prevent harm and prevent present and continuing increased risk.

144. Defendant breached their implied contract with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff's and Class Members' Sensitive Information, which was compromised as a result of the Data Breach.

145. As a direct and proximate result of Defendant's breaches, Plaintiff and Class Members sustained actual losses and damages as alleged herein, including that they did not receive the benefits of the bargains for which they paid. Plaintiff and Class Members alternatively seek an award of nominal damages.

COUNT V
Breach of Confidence

146. Plaintiff incorporates paragraphs 1-99 of the Complaint as if fully set forth herein.

147. Plaintiff and Class Members maintained a confidential relationship with Defendant wherein Defendant undertook a duty not to disclose PII and PHI provided by Plaintiff and Class Members to unauthorized third parties. Such PII and PHI was confidential and novel, highly personal and sensitive, and not generally known.

148. Defendant knew Plaintiff's and Class Members' PII and PHI was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreed to protect the confidentiality and security of the PII and PHI it collected, stored, and maintained.

149. There was disclosure of Plaintiff's and Class Members' PII and PHI as a result of the Data Breach in violation of this understanding. The disclosure occurred because Defendant

failed to implement and maintain reasonable safeguards to protect its patients' PII and PHI and failed to comply with industry-standard data security practices.

150. Plaintiff and Class Members suffered harm the moment the unconsented disclosure of the confidential information to an unauthorized third party took place.

151. As a direct and proximate result of Defendant's breach of confidence, Plaintiff and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiff and Class Members alternatively seek an award of nominal damages.

COUNT VI
Unjust Enrichment

152. Plaintiff incorporates paragraphs 1-99 of the Complaint as if fully set forth herein.

153. To the extent necessary, Plaintiff asserts this claim in the alternative to her breach of contract claims.

154. Plaintiff and Class Members have an interest, both equitable and legal, in their Sensitive Information that was conferred upon, collected by, and maintained by the Defendant and which was stolen in the Data Breach. This information has independent value.

155. Plaintiff and Class Members conferred a monetary benefit on Defendant in the form of payments for medical and healthcare services, including those paid indirectly by Plaintiff and Class Members to Defendant.

156. Defendant appreciated and had knowledge of the benefits conferred upon it by Plaintiff and Class Members.

157. The price for medical and healthcare services that Plaintiff and Class Members paid (directly or indirectly) to Defendant should have been used by Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

158. Likewise, in exchange for receiving Plaintiff's and Class Members' valuable PII and PHI, which Defendant was able to use for their own business purposes and which provided actual value to Defendant, Defendant was obligated to devote sufficient resources to reasonable data privacy and security practices and procedures.

159. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual damages as described herein. Under principals of equity and good conscience, Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds they received from Plaintiff and Class Members, including damages equaling the difference in value between medical and healthcare services that included implementation of reasonable data privacy and security practices that Plaintiff and Class Members paid for and the services without reasonable data privacy and security practices that they actually received.

COUNT VII
Declaratory Judgment

160. Plaintiff incorporates paragraphs 1-99 of the Complaint as if fully set forth herein.

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

162. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard its users' PII, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII and PHI. Plaintiff and Class Members remain at imminent risk that further compromises of their PII and

PHI will occur in the future. This is true even if they (or their healthcare providers) are not actively using Defendant's products or services.

163. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

(a) Defendant continues to owe a legal duty to secure users' PII and PHI and to timely notify consumers of a data breach under the common law;

(b) Defendant continues to owe a legal duty to secure users' PII and PHI and to timely notify consumers of a data breach under HIPAA;

(c) Defendant continues to owe a legal duty to secure users' PII and PHI and to timely notify consumers of a data breach under the FTC Act, 15 U.S.C. §45(a)(1);

(d) Defendant continues to owe a legal duty to secure users' PII and PHI and to timely notify consumers of a data breach under the FCRA, 15 U.S.C. §1681(b);

(e) Defendant continues to breach this legal duty by failing to employ reasonable measures to secure Plaintiff's and Class Members' PII and PHI.

164. The Court also should issue corresponding prospective injunctive relief pursuant to 28 U.S.C. §2202, requiring Defendant to employ adequate security practices consistent with law and industry standards to protect its users' PII and PHI.

165. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of Defendant. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

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

167. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating additional injuries that would result to Plaintiff, Class Members, and the millions of other Defendant customers whose PII and PHI would be further compromised.

RELIEF REQUESTED

Plaintiff, individually and on behalf of the proposed Class, requests that the Court:

A. Certify this case as a class action on behalf of the Class, defined above, appoint Plaintiff as Class representative, and appoint the undersigned counsel as class counsel;

B. Award declaratory, injunctive, and other equitable relief as is necessary to protect the interests of Plaintiff and other Class Members, including but not limited to an order:

- prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
- requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
- requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

- requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII and PHI of Plaintiff and Class Members;

- prohibiting Defendant from maintaining the PII and PHI of Plaintiff and Class Members on a cloud-based database;

- requiring Defendant 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 Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

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

- requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

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

- requiring Defendant to conduct regular database scanning and securing checks;

- requiring Defendant 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 Plaintiff and Class Members;

- requiring Defendant 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;

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

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

- requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves; and

- requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

C. Award restitution; compensatory, consequential, and general damages, including nominal damages as allowed by law in an amount to be determined at trial or by this Court;

D. Award Plaintiff and Class Members their reasonable litigation expenses and attorneys' fees to the extent allowed by law;

E. Award Plaintiff and Class Members pre- and post-judgment interest, to the extent allowable; and

F. Award such other and further relief as equity and justice may require.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any and all issues in this action so triable as of right.

DATED: January 12, 2022

ROBBINS GELLER RUDMAN
& DOWD LLP

/s/ Dorothy P. Antullis
DOROTHY P. ANTULLIS

DOROTHY P. ANTULLIS
STUART A. DAVIDSON
MAXWELL H. SAWYER
120 East Palmetto Park Road, Suite 500
Boca Raton, FL 33432
Phone: 561/750.3000
561/750.3364 (fax)
sdavidson@rgrdlaw.com
dantullis@rgrdlaw.com
msawyer@rgrdlaw.com

Local Counsel

THE LYON FIRM
Joseph M. Lyon (*pro hac vice* forthcoming)
2754 Erie Avenue
Cincinnati, OH 45208
Phone: 513/381.2333
513/721.1178 (fax)
jlyon@thelyonfirm.com

MARKOVITS, STOCK & DEMARCO, LLC
Terence R. Coates (*pro hac vice* forthcoming)
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Phone: 513/651-3700
513/665.0219 (fax)
tcoates@msdlegal.com

Counsel for Plaintiff and the Class