UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO.:

DANIEL ESTERLY, individually and on behalf of all others similarly situated,

Plaintiff,

v.

NORTH BROWARD HOSPITAL DISTRICT d/b/a BROWARD HEALTH,

Defendant.

CLASS ACTION COMPLAINT

Plaintiff Daniel Esterly ("Plaintiff"), by and through the undersigned counsel, brings this class action complaint against Defendant North Broward Hospital District d/b/a Broward Health ("Defendant" or "Broward Health"), on behalf of himself and all others similarly situated. Plaintiff makes the following allegations based upon personal knowledge as to his own actions and upon information and belief as to all other matters:

NATURE OF THE CASE

1. On January 1, 2022, Broward Health, a Florida-based healthcare system that operates more than 30 healthcare locations in Broward County, Florida, disclosed that it was the subject of a massive data breach whereby hackers gained unauthorized access to its networks between October 15 and October 19, 2021 (the "Data Breach").

2. The hackers were able to access and exfiltrate highly-sensitive information stored on Broward Health's servers, including 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 ("PII").

3. The Data Breach occurred because Broward Health failed to implement reasonable security procedures and practices, failed to disclose material facts surrounding its deficient data security protocols, and failed to timely notify the victims of the Data Breach.

4. As a result of Broward Health's failure to protect the sensitive information it was entrusted to safeguard, Plaintiff and class members did not receive the benefit of their bargain with Broward Health and now face a significant risk of medical-related identity theft and fraud, financial fraud, and other identity-related fraud now and into the indefinite future.

PARTIES

5. Plaintiff Daniel Esterly is a resident of Pittsburgh, Pennsylvania and healthcare patient of Broward Health.

6. Defendant Broward Health is a healthcare system that operates several hospitals and dozens healthcare facilities in the South Florida region.

JURISDICTION AND VENUE

7. 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 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.

8. 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.

9. 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

Broward Health's Privacy Practices

10. 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. Broward Health is overseen by a board of seven commissioners who are appointed by the Governor of Florida and confirmed by the Florida Senate.

11. In the course of providing healthcare services, Broward Health requires patients to provide personal information, including their full names, home addresses, dates of birth, email addresses, and Social Security numbers, financial information such as bank account and payment card numbers, and medical information including medical histories, past treatment records, prescription information, health provider information, and health insurance coverage. As a result, when patients are treated by a Broward Health healthcare facility, their highly sensitive personal identifiable information ("PII") and protected health information ("PHI") is stored on centralized servers maintained by Broward Health.

12. Given the amount and sensitive nature of the data it collects, 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."

13. 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."

14. 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 maintains that it will "maintain[] the confidentiality of patient and other information in accordance with legal and ethical standards, and breaches will not be tolerated."

15. 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.

16. 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."

17. 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

18. Contrary to its representations, on October 15, 2021, hackers infiltrated Broward Health's networks and accessed highly sensitive patient information stored on its servers. Broward Health disclosed that it discovered the intrusion on October 19, 2021, and "promptly contained the

incident upon discovery, notified the FBI and the Department of Justice (DOJ), required all employees to update their passwords and engaged an independent cybersecurity firm to conduct an extensive investigation into the incident."

19. 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."

20. The investigation confirmed that extensive personal medical information was accessed, including 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.

21. Broward Health acknowledged this information was not only accessed, but also "exfiltrated, or removed, from Broward Health's systems." A disclosure by Broward Health to the office of the Maine attorney general revealed that the breach impacted 1,357,879 individuals.

22. Broward Health did not disclose the existence of the Data Breach until January 1, 2022, when it began mailing individual notification letters. Broward Health attributed the delayed notification to a request from the DOJ to "briefly delay this notification to ensure that the notification does not compromise the ongoing law enforcement investigation."

The Data Breach was Preventable

23. Following the Data Breach, Broward Health stated that it "takes the protection of [patient] personal and medical information very seriously" and "is taking steps to prevent recurrence of similar incidents, which include the ongoing investigation, a password reset with

enhanced security measures across the enterprise, and the implementation of multifactor authentication for all users of its systems."

24. Broward Health also stated it has "begun implementation of additional minimum-security requirements for devices that are not managed by Broward Health Information Technology that access our network, which will become effective in January 2022."

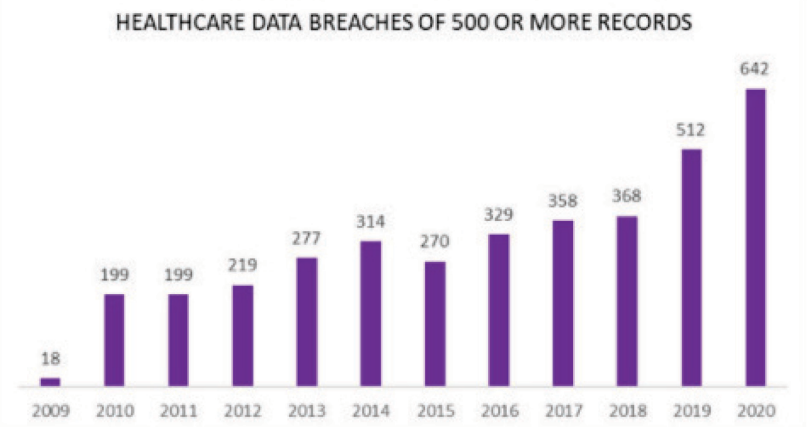
25. But these "steps" are industry-standard measures that should have been implemented long before the Data Breach occurred. This is especially true given that the healthcare industry is frequently one of the most targeted sectors for cyberattacks and attacks using stolen credentials have increased precipitously over the last several years.

26. Healthcare providers like Broward Health are prime targets because of the information they collect and store, including financial information of patients, login credentials, insurance information, medical records and diagnoses, and personal information of employees and patients—all extremely valuable on underground markets.

27. This was known and obvious to Broward Health as it observed frequent public announcements of data breaches affecting healthcare providers and knew that information of the type it collected, maintained, and stored is highly coveted and a frequent target of hackers.

28. According to a report by the HIPAA Journal, "data breach statistics clearly show there has been an upward trend in data breaches over the past 10 years, with 2020 seeing more data breaches reported than any other year since records first started being published."[1] In fact, healthcare data breaches were up 55% in 2020 from the prior year alone.[2]

[1] https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited January 7, 2022).
[2] https://www.cpomagazine.com/cyber-security/healthcare-cyber-attacks-rise-by-55-over-26-million-in-the-u-s-impacted/ (last visited January 7, 2022).



29. It is well known that use of stolen credentials through long been the most popular and effective method of gaining authorized access to a company's internal networks and that companies should activate defenses to prevent such attacks.

30. According to the Federal Bureau of Investigation (FBI), phishing schemes designed to induce individuals to reveal personal information were the most common type of cybercrime in 2020, with such incidents nearly doubling in frequency between 2019 and 2020.[3] According to Verizon's 2021 Data Breach Investigations Report, 43% of breaches stemmed from phishing and/or pretexting schemes.[4]

31. The risk is so prevalent for healthcare providers that on October 28, 2020, the FBI and two federal agencies issued a "Joint Cybersecurity Advisory" warning that they have "credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."[5] The Cybersecurity and Infrastructure Security Agency (CISA), the Department of

[3] https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (last visited January 7, 2022).
[4] https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/ (subscription required) (last visited January 7, 2022).
[5] https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf (last visited January 7, 2022).

Health and Human Services (HHS), and the FBI issued the advisory to warn healthcare providers to take "timely and reasonable precautions to protect their networks from these threats."[6]

32. There are two primary ways to mitigate the risk of stolen credentials: user education and technical security barriers. User education is the process of making employees or others users of a network aware of common disclosure schemes and implementing company-wide policies requiring the request or transfer of sensitive personal or financial information only through secure sources to known recipients. For example, a common phishing e-mail is an "urgent" request from a company "executive" requesting confidential information in an accelerated timeframe. The request may come from an e-mail address that appears official but contains only one different number or letter. Other phishing methods include baiting a user to click a malicious link that redirects them to a nefarious website or to download an attachment containing malware.

33. User education provides the easiest method to assist in properly identifying fraudulent "spoofing" e-mails and prevent unauthorized access of sensitive internal information. According to September 2020 guidance from CISA, organizations housing sensitive data should "[i]mplement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity" and conduct "organization-wide phishing tests to gauge user awareness and reinforce the importance of identifying potentially malicious emails."[7]

34. From a technical perspective, companies can also greatly reduce the flow of fraudulent e-mails by installing software that scans all incoming messages for harmful attachments or malicious content and implementing certain security measures governing e-mail transmissions, including Sender Policy Framework (SPF) (e-mail authentication method used to prevent

[6] *Id*.
[7] https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf (last visited January 7, 2022).

spammers from sending messages on behalf of a company's domain), DomainKeys Identified Mail (DKIM) (e-mail authentication method used to ensure messages are not altered in transit between the sending and recipient servers), and Domain-based Message Authentication, Reporting and Conformance (DMARC), which "builds on the widely deployed [SPF] and [DKIM] protocols, adding a reporting function that allows senders and receivers to improve and monitor protection of the domain from fraudulent email."[8]

35. Additionally, because the goal of these schemes is to gain an employee's login credentials in order to access a company's network, there are industry-standard measures that companies can implement to greatly reduce unauthorized access, even if an individual's login credentials are disclosed. For example, multi-factor authentication is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login. This could include entering a code from the user's smartphone, answering a security question, or providing a biometric indicator such as a fingerprint or facial recognition—in addition to entering a username and password. Thus, even if hackers obtain an employee's username and password, access to the company's system is thwarted because they do not have access to the additional authentication methods.

36. Similarly, companies housing sensitive data must implement adequate "network segmentation," which is the practice of dividing a larger network into several smaller subnetworks that are each isolated from one another to provide enhanced security. For example, hackers that gain access to an unsegmented network (commonly through phishing) can move laterally across the network to access databases containing valuable assets such as sensitive personal information or financial records. Malicious lateral movement can be difficult to detect because it oftentimes

[8] *Id.*

appears as normal network traffic. By implementing adequate network segmentation, companies can prevent even those hackers who already gained a foothold in their network from moving across databases to access their most sensitive data.

37. Network segmentation is commonly used in conjunction with the principle of least privilege (POLP), which is a security practice that limits employees' privileges to the minimum necessary to perform the job or task. In an IT environment, adhering to POLP reduces the risk of hackers gaining access to critical systems or sensitive data by compromising a low-level user account, device, or application.[9] In an example given by security software provider Digital Guardian:

> [A]n employee whose job is to enter info into a database only needs the ability to add records to that database. If malware infects that employee's computer or if the employee clicks a link in a phishing email, the malicious attack is limited to making database entries. If that employee has root access privileges, however, the infection can spread system-wide.[10]

This is precisely why approximately 67% of targeted malware and stolen credential schemes are directed at individual contributors and lower-level management personnel.[11]

38. In addition to mitigating the risk of stolen credentials, the CISA guidance encourages organizations to prevent unauthorized access by:

- Conducting regular vulnerability scanning to identify and address vulnerabilities, particularly on internet-facing devices;
- Regularly patching and updating software to latest available versions, prioritizing timely patching of internet-facing servers and software processing internet data;
- Ensuring devices are properly configured and that security features are enabled;

[9] https://digitalguardian.com/blog/what-principle-least-privilege-polp-best-practice-information-security-and-compliance (last visited January 7, 2022).
[10] *Id.*
[11] https://healthitsecurity.com/news/pharmaceutical-companies-most-targeted-industry-by-cybercriminals (last visited January 7, 2022).

- Employing best practices for use of Remote Desktop Protocol (RDP) as threat actors often gain initial access to a network through exposed and poorly secured remote services; and

- Disabling operating system network file sharing protocol known as Server Message Block (SMB) which is used by threat actors to travel through a network to spread malware or access sensitive data.[12]

39. The CISA guidance further recommends use of a centrally managed antivirus software utilizing automatic updates that will protect all devices connected to a network (as opposed to requiring separate software on each individual device), as well as implementing a real-time intrusion detection system that will detect potentially malicious network activity that occurs prior to ransomware deployment.[13]

40. Despite holding the PII and PHI of thousands of patients, Broward Health failed to adhere these recommended best practices. Indeed, had Broward Health implemented common sense security measures like network segmentation and POLP, the hackers never could have accessed millions of patient files using the credentials of a third-party provider and the breach would have been prevented or much smaller in scope. Broward Health also lacked the necessary safeguards to detect and prevent phishing attacks and failed to implement adequate monitoring or control systems to detect the unauthorized infiltration after it occurred.

41. Broward Health, like any healthcare provider its size storing valuable data, should have had robust protections in place to detect and terminate a successful intrusion long before access and exfiltration could expand to millions of patient files. Broward Health's implementation of enhanced security measures only after the fact is inexcusable given its knowledge that it was a prime target for cyberattacks.

[12] CISA Guide at 4.
[13] *Id*. at 5.

Broward Heath has a Troubling History of Governance Issues

42. Broward Health is a taxpayer-supported district that runs hospitals and clinics in the northern two-thirds of Broward County. With an annual budget approaching $2 billion, Broward Health is one of the country's ten largest public health systems. The system operates four hospitals, with a total of 1,579 beds, 8,300 employees, and more than 1,700 doctors.

43. Despite its prominent stature, Broward Health has been charged with numerous acts of corruption that calls into questions its commitment to and investment in patient care. For example, in 2015 Broward Health entered into a $69.5 million with the state of Florida and the DOJ amid whistleblower allegations that it engaged in illegal kickbacks based on the number of patient referrals to the Broward Health system. Six months later, the State of Florida demanded the healthcare system pay $5.3 million to settle related Medicaid fraud charges.[14]

44. In March of 2016, Broward Health's CEO, Nabil El Sanadi, M.D. committed suicide. In the year before he killed himself, Dr. El Sanadi brought in a corporate private investigator to probe wrongdoing at the public hospital system, meeting with him in restaurants and at his home because he feared his office was bugged.[15]

45. In December 2016, the Broward Health board fired CEO Pauline Grant after an investigation revealed probable violations of the anti-kickback statute. The following year, several current and former Broward Health board members were indicted for violations of the Florida Sunshine Law after four commissioners held de facto meetings at a hotel, restaurant, and by

[14] https://www.sun-sentinel.com/local/broward/fl-broward-health-ag-demand-20160318-story.html (last visited January 7, 2022).
[15] https://www.sun-sentinel.com/local/broward/fl-broward-health-investigation-20160202-story.html (last visited January 7, 2022).

telephone to discuss the allegations against Grant.[16] Broward Health's board of directors later approved a $975,000 settlement with Ms. Grant after she sued for wrongful termination.[17]

46. In May 2017, the Broward Health directors voted to approve board member Beverly Capasso as interim CEO, with an annual salary of $650,000. Controversy arose when it was discovered Ms. Capasso voted for herself at a special board meeting despite having a clear conflict of interest.[18] Following her appointment, it was reported that Ms. Capasso held a master's degree in health administration from Kennedy-Western University, a defunct university identified by federal investigators as a diploma mill.[19]

47. At the time of her appointment, the Florida Sun Sentinel questioned why Capasso was never fully vetted for the job. "Board members engaged in virtually no questioning of her background, her work experience or her likely approach to the job. No one asked whether anyone at Broward Health had talked with her previous health care industry employers about the quality of her work."[20] Nevertheless, in February 2018, the board of Broward Health rejected four finalists for the CEO position and voted to elevate Capasso to permanent CEO, along with up to $1.125 million in compensation, despite her being under indictment.[21]

---

[16] https://www.sun-sentinel.com/local/broward/fl-sb-broward-health-charges-20171212-story.html (last visited January 7, 2022).
[17] https://www.fiercehealthcare.com/hospitals-health-systems/broward-health-settles-ex-ceo-for-975-000 (last visited January 7, 2022).
[18] https://www.local10.com/news/2017/05/12/new-broward-health-interim-ceo-voted-for-herself-for-job/ (last visited January 7, 2022).
[19] https://www.sun-sentinel.com/health/fl-sb-capasso-degree-20170629-story.html (last visited January 7, 2022).
[20] https://www.sun-sentinel.com/local/broward/fl-sb-broward-health-new-ceo-20170508-story.html (last visited January 7, 2022).
[21] https://www.sun-sentinel.com/local/broward/fl-sb-broward-health-ceo-meeting-20180130-story.html (last visited January 7, 2022).

48. In October 2018, Capasso resigned after allegations of infighting between Broward Health's general counsel's office, the executive team, and an independent law firm appointed to ensure the Broward Health is abiding by the terms of its DOJ settlement.[22]

49. In July 2019, Broward Health paid a $690,000 fine for violating the terms of the DOJ settlement after it was alleged Broward Health failed to take certain required steps to ensure compliance with anti-kickback laws and breached five provisions of the settlement agreement, leading to individual penalties of up to $2,500 a day.[23]

50. In June 2021, Broward Health's former procurement Brian Bravo pleaded guilty to a federal conspiracy for accepting over $400,000 in kickbacks in exchange for awarding vendors lucrative government contracts.[24]

51. These are just a subset of the allegations of corruption and misconduct plaguing taxpayer-funded Broward Health. Thus, while it is clear Broward Health had the knowledge and resources to prevent a breach—and in fact made significant expenditures to pay settlements and fines—the organization neglected to make corresponding investments in data security to ensure the millions of patient files in its possession were securely stored.

Allegations Relating to Plaintiff Daniel Esterly

52. Plaintiff Daniel Esterly lives and resides in Pittsburgh, Pennsylvania and is a former healthcare patient of a Broward Health healthcare facility.

53. For purposes of receiving medical treatment, Mr. Esterly was required to provide Broward Health with his sensitive personal information, including, among other information, his

[22] https://www.miamiherald.com/news/health-care/article219429370.html (last visited January 7, 2022).
[23] https://www.politico.com/states/florida/story/2019/07/16/broward-paid-fine-for-breaching-2015-fraud-settlement-with-feds-1098093 (last visited January 7, 2022).
[24] https://www.local10.com/news/local/2021/06/02/ex-broward-health-exec-pleads-guilty-to-400k-bribery-scheme/ (last visited January 7, 2022).

full name, home address, date of birth, e-mail address, Social Security number, health insurance ID card, and driver's license.

54. Broward Health also maintained Mr. Esterly's patient account numbers, health insurance plan member ID numbers, medical record numbers, dates of service, provider names, and medical and clinical treatment information.

55. In January 2022, Mr. Esterly received a notification letter from Broward Health stating that he was a victim of the Data Breach. The letter stated that: "We are alerting you to this situation now that the involvement of your personal information has been confirmed."

56. The letter recommended that Mr. Esterly take certain actions like monitoring his financial accounts and "placing a 'fraud alert' and/or a 'security freeze' on your credit report to further detect any possible misuse of your personal information." The letter further stated that "[w]e recommend that you consider steps to protect yourself from medical identity theft. Medical identity theft occurs when someone uses an individual's name, and sometimes other identifying information, without the individual's knowledge to obtain medical services or products, or to fraudulently bill for medical services that have not been provided. We suggest that you regularly review the explanation of benefits statements that you receive from your health plan. If you see any service that you did not receive, contact the health plan at the number on the statement."

57. Despite making these recommendations, Broward Health also attempted to downplay the risk of harm by stating three times in the letter that "we have no evidence that your personal information has been misused." This statement is facially dubious as the objective of almost every data breach is to access information that can be misused for financial gain and in any event Broward Health would not receive reports of misuse until *after* victims are affirmatively notified they were subject to the Data Breach.

58. As a result of the Data Breach, Mr. Esterly has spent time and effort researching the breach and reviewing his financial and medical account statements for evidence of unauthorized activity, which he will continue to do indefinitely. Mr. Esterly also suffered emotional distress knowing that his highly personal medical and treatment information is no longer confidential and can be used for blackmail, extortion, medical-related identity theft or fraud, and any number of additional harms against him for the rest of his life.

Broward Health Failed to Comply with Federal Law and Regulatory Guidance

59. Broward Health is a healthcare provider covered by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (*see* 45 C.F.R. § 160.102) and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

60. These rules establish national standards for the protection of patient information, including PHI, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. 45 C.F.R. § 160.103.

61. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."[25]

62. HIPAA requires that Broward Health implement appropriate safeguards for this information.[26]

[25] 45 C.F.R. § 164.502.
[26] 45 C.F.R. § 164.530(c)(1).

63. HIPAA requires that Broward Health provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons—*i.e.* non-encrypted data.[27]

64. Despite these requirements, Broward Health failed to comply with its duties under HIPAA and its own Notice of Privacy Practices. Indeed, Broward Health failed to:

a. Maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;

b. Adequately protect the PII and PHI of its patients and employees;

c. Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. Implement technical policies and procedures for electronic information systems that maintain electronically 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);

e. Implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. Implement adequate 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)(1)(ii)(D);

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

h. Ensure compliance with the electronically protected health information security standard rules by their workforces, in violation of 45 C.F.R. § 164.306(a)(4); and/or

i. Train all members of their workforces effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

[27] 45 C.F.R. § 164.404; 45 C.F.R. § 164.402.

65. Additionally, federal agencies have issued recommendations and guidelines to help minimize the risks of a data breach for businesses holding sensitive data. For example, the Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices, which should be factored into all business-related decision making.[28]

66. The FTC's publication *Protecting Personal Information: A Guide for Business* sets forth fundamental data security principles and practices for businesses to implement and follow as a means to protect sensitive data.[29] Among other things, the guidelines note that businesses should (a) protect the personal customer information that they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems. The FTC guidelines further recommend that businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.[30]

67. Additionally, the FTC recommends that companies 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.[31] This is consistent with guidance provided by the FBI, HHS, and the principles set forth in the CISA 2020 guidance.

---

[28] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited January 7, 2022).
[29] https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited January 7, 2022).
[30] *Id*.
[31] FTC, *Start With Security*, *supra* note 41.

68. The FTC has brought enforcement actions against businesses for failing to reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[32]

69. Broward Health was fully aware of its obligation to implement and use reasonable measures to protect the PII and PHI of its patients but failed to comply with these basic recommendations and guidelines that would have prevented this breach from occurring. Broward Health's failure to employ reasonable measures to protect against unauthorized access to patient information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

The Impact of the Data Breach on Victims

70. The PII and PHI exposed in the Data Breach is highly coveted and valuable on underground markets as it can be used to commit medical-related identity theft and fraud, one of the most dangerous and costly forms of identity theft.

71. According to a *Reuters* investigation that included interviews with nearly a dozen healthcare executives, cybersecurity investigators, and fraud experts, medical data for sale on underground markets "includes names, birth dates, policy numbers, diagnosis codes and billing information" which fraudsters commonly use "to create fake IDs to buy medical equipment or

[32] https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited January 7, 2022).

drugs that can be resold, or they combine a patient number with a false provider number and file made-up claims with insurers."[33]

72. According to Tom Kellermann, chief cybersecurity officer of cybersecurity firm Carbon Black, "Health information is a treasure trove for criminals [because] by compromising it, by stealing it, by having it sold, you have seven to 10 personal identifying characteristics of an individual."[34] For this reason, a patient's full medical records can sell for up to $1,000 on the dark web, while credit card numbers and Social Security numbers may cost $5 or less.[35]

73. As noted by Paul Nadrag, a software developer for medical device integration and data technology company Capsule Technologies: "The reason for this price discrepancy—like any other good or service—is perceived value. While a credit card number is easily canceled, medical records contain a treasure trove of unalterable data points, such as a patient's medical and behavioral health history and demographics, as well as their health insurance and contact information. Once records are stolen, cybercriminals often tap into members of a criminal network on the dark web experienced in drug trafficking and money laundering who are eager to buy medical records to support their criminal activities, such as illegally obtaining prescription medications, filing bogus medical claims or simply stealing the patient's identity to open credit cards and fraudulent loans."[36]

74. Indeed, while federal law generally limits an individual's liability for fraudulent credit card charges to $50, there are no such protections for a stolen medical identity. According

[33] https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924 (last visited January 7, 2022).
[34] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited January 7, 2022).
[35] https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited January 7, 2022).
[36] https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web (last visited January 7, 2022).

to a 2015 survey on medical identity theft conducted by the Ponemon Institute, victims of medical identity theft spent an average of $13,500 in out-of-pocket costs to resolve the crime.[37] Frequently, this information was used to obtain medical services or treatments (59%), obtain prescription drugs (56%), or receive Medicare and Medicaid benefits (52%). Only 14% of respondents said that the identity thieves used the information to obtain fraudulent credit accounts, indicating that medical information is a much more profitable market.[38]

75. According to the Ponemon study, "[t]hose who have resolved the crime spent, on average, more than 200 hours on such activities as working with their insurer or healthcare provider to make sure their personal medical credentials are secured and can no longer be used by an imposter and verifying their personal health information, medical invoices and claims and electronic health records are accurate."[39]

76. Additionally, the study found that medical identity theft can have a negative impact on reputation as 45% of respondents said that medical identity theft affected their reputation mainly because of embarrassment due to disclosure of sensitive personal health conditions, with 19% responding that they missed out on employment opportunities as a result.[40]

77. Exacerbating the problem, victims of medical identity theft oftentimes struggle to resolve the issue because HIPAA regulations require the victim to be personally involved in the resolution of the crime.[41] In some cases, victims may not even be able to access medical records using their personal information because they include a false name or data points taken from

[37] https://static.nationwide.com/static/2014_Medical_ID_Theft_Study.pdf?r=65 ("Ponemon Study") (last visited January 7, 2022).
[38] *Id*. at 9.
[39] *Id*. at 2.
[40] *Id*. at 14.
[41] *Id*. at 1.

another person's records. Consequently, only 10% of medical identity theft victims responded that they "achiev[ed] a completely satisfactory conclusion of the incident."[42]

78. Moreover, it can take months or years for victims to even discover they are the victim of medical-related identity theft or fraud given the difficulties associated with accessing medical records and healthcare statements. For example, the FTC notes that victims may only discover their identity has been compromised after they:

- Receive a bill for medical services they did not receive;
- Get contacted by a debt collector about medical debt they do not owe;
- See medical collection notices on their credit report that they do not recognize;
- Find erroneous listings of office visits or treatments on their explanation of benefits (EOB);
- Receive information from their health plan that they have reached their limit on benefits; or
- Be denied insurance because their medical records show a condition they do not have.[43]

79. Perhaps most dangerous, however, is the potential for misdiagnoses or treatment. According to Ann Patterson, a senior vice president of the Medical Identity Fraud Alliance, "About 20 percent of victims have told us that they got the wrong diagnosis or treatment, or that their care was delayed because there was confusion about what was true in their records due to the identity theft."[44] This echoes the Ponemon study, which notes that "many respondents are at risk for further theft or errors in healthcare records that could jeopardize medical treatments and diagnosis."[45]

---

[42] *Id.*
[43] https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf (last visited January 7, 2022).
[44] https://www.consumerreports.org/medical-identity-theft/medical-identity-theft/ (last visited January 7, 2022).
[45] Ponemon Study at 1.

80. According to a Consumer Reports article entitled *The Rise of Medical Identity Theft*, this outcome "isn't a hypothetical problem" as the "long tail on medical identity theft can create havoc in victims' lives."[46] As one example, a pregnant woman reportedly used a victim's medical identity to pay for maternity care at a nearby hospital. When the infant was born with drugs in her system, the state threatened to take the *victim's* four children away—not realizing her identity had been stolen. The victim ultimately had to submit to a DNA test to remove her name from the infant's birth certificate, but it took years to get her medical records corrected.[47]

81. Other types of medical fraud include "leveraging details specific to a disease or terminal illness, and long-term identity theft."[48] According to Tom Kellermann, "Traditional criminals understand the power of coercion and extortion. By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[49] Long-term identity theft occurs when fraudsters combine a victim's data points, including publicly-available information or data points exposed in other data breaches, to create new identities, open false lines of credit, or commit tax fraud that can take years to remedy.

82. Given the confirmed exfiltration of PII and PHI from Broward Health's systems, many victims of the Data Breach have likely already experienced significant harms as the result of the Data Breach, including, but not limited to, medical-related identity theft and fraud. Plaintiff and class members have also spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit monitoring services, reviewing financial and healthcare

[46] https://www.consumerreports.org/medical-identity-theft/medical-identity-theft/ (last visited January 7, 2022).
[47] *Id.*
[48] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited January 7, 2022).
[49] *Id.*

statements, checking credit reports, and spending time and effort searching for unauthorized activity.

83. It is no wonder then that identity theft exacts a severe emotional toll on its victims. The 2017 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed
- 67% reported anxiety
- 66% reported feelings of fear related to personal financial safety
- 37% reported fearing for the financial safety of family members
- 24% reported fear for their physical safety
- 15.2% reported a relationship ended or was severely and negatively impacted by the identity theft; and
- 7% reported feeling suicidal.[50]

84. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances
- 37.1% reported an inability to concentrate / lack of focus
- 28.7% reported they were unable to go to work because of physical symptoms
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[51]

[50] https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited January 7, 2022).
[51] *Id.*

85. The unauthorized disclosure of the sensitive PII and PHI to data thieves also reduces its inherent value to its owner, which has been recognized by courts as an independent form of harm.[52]

86. Consumers are injured every time their data is stolen and traded on underground markets, even if they have been victims of previous data breaches. Indeed, the dark web is comprised of multiple discrete repositories of stolen information that can be aggregated together or accessed by different criminal actors who intend to use it for different fraudulent purposes. Each data breach increases the likelihood that a victim's personal information will be exposed to more individuals who are seeking to misuse it at the victim's expense.

87. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiff and class members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. the unconsented disclosure of confidential information to a third party;

b. losing the inherent value of their PII and PHI;

c. losing the value of the explicit and implicit promises of data security;

d. identity theft and fraud resulting from the theft of their PII and PHI;

e. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

f. anxiety, emotional distress, and loss of privacy;

g. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

h. unauthorized charges and loss of use of and access to their financial and investment account funds and costs associated with inability to obtain money from their accounts

[52] *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

i. lowered credit scores resulting from credit inquiries following fraudulent activities;

j. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including searching for fraudulent activity, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and

k. the continued, imminent, and certainly impending injury flowing from potential fraud and identify theft posed by their PII and PHI being in the possession of one or many unauthorized third parties.

88. Even in instances where an individual is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement.

89. There may also be a significant time lag between when personal information is stolen and when it is misused for fraudulent purposes. According to the Government Accountability Office, which conducted a study regarding data breaches: "law 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."[53]

90. Plaintiff and class members place significant value in data security. According to a survey conducted by cyber-security company FireEye Mandiant, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a

[53] http://www.gao.gov/new.items/d07737.pdf (last visited January 7, 2022).

provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[54]

91. Because of the value consumers place on data privacy and security, healthcare providers with robust data security practices are viewed more favorably by patients and can command higher prices than those who do not. Consequently, had Broward Health's patients known the truth about its data security practices—that it did not adequately protect and store their PII and PHI —they would not have sought medical care from Broward Health or would have paid significantly less. As such, Plaintiff and class members did not receive the benefit of their bargain with Broward Health because they paid for the value of services they did not receive.

92. Plaintiff and class members have a direct interest in Broward Health's promises and duties to protect their PII and PHI, *i.e.*, that Broward Health *not increase* their risk of identity theft and fraud. Because Broward Health failed to live up to its promises and duties in this respect, Plaintiff and class members seek the present value of identity protection services to compensate them for the present harm and present and continuing increased risk of harm caused by Broward Health's wrongful conduct. Through this remedy, Plaintiff and class members seek to restore themselves and class members as close to the same position as they would have occupied but for Broward Health's wrongful conduct, namely its failure to adequately protect Plaintiff's and class members' PII and PHI.

93. Plaintiff and class members further seek to recover the value of the unauthorized access to their PII and PHI permitted through Broward Health's wrongful conduct. This measure of damages is analogous to the remedies for unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's PII or PHI is non-

[54] https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited January 7, 2022).

rivalrous—the unauthorized use by another does not diminish the rights-holder's ability to practice the patented invention or use the trade-secret protected technology. Nevertheless, a plaintiff may generally recover the reasonable use value of the IP—*i.e.*, a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a non-practicing patentee) and even though the owner would not have otherwise licensed such IP to the infringer. A similar royalty or license measure of damages is appropriate here under common law damages principles authorizing recovery of rental or use value. This measure is appropriate because (a) Plaintiff and class members have a protectible property interest in their PII and PHI; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; and (c) rental value is established with reference to market value, *i.e.*, evidence regarding the value of similar transactions.

94. Broward Health's deficient notice letter also caused Plaintiff and class members harm. For example, Broward Health provided no context for its repeated unsubstantiated statement that there was "no evidence that your personal information has been misused" as the objective of almost every data breach is to gain access to an organization's sensitive data so that the data can be misused for financial gain. Furthermore, the letter did not explain the precise nature of the attack, the identity of the hackers, or the number of individuals affected. Broward Health's decision to withhold these key facts is significant because affected individuals may take different precautions depending on the severity and imminence of the perceived risk. By waiting months to disclose the Data Breach and by downplaying the risk of misuse, Broward Health prevented victims from taking meaningful, proactive, and targeted mitigation measures that could help protect them from harm.

95. Because Broward Health continues to hold the PII and PHI of its patients, Plaintiff and class members have an interest in ensuring that their PII and PHI is secured and not subject to further theft.

CLASS ACTION ALLEGATIONS

96. Plaintiff seeks relief in his individual capacity and as a representative of all others who are similarly situated. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff brings this action on behalf of himself and the Class defined as: All individuals whose personal information was compromised in the Data Breach (the "Class").

97. Specifically excluded from the Class are Defendant; its officers, directors, or employees; any entity in which Defendant has a controlling interest; and any affiliate, legal representative, heir, or assign of Defendant. Also excluded from the Class are any federal, state, or local governmental entities, any judicial officer presiding over this action and the members of their immediate family and judicial staff, and any juror assigned to this action.

98. Class Identity: The members of the Class are readily identifiable and ascertainable. Defendant and/or its affiliates, among others, possess the information to identify and contact class members.

99. Numerosity: The members of the Class are so numerous that joinder of all of them is impracticable. Broward Health's disclosures reveal that the Class contains more than 1.3 million individuals whose PII was compromised in the Data Breach.

100. Typicality: Plaintiff's claims are typical of the claims of the members of the Class because all class members had their PII compromised in the Data Breach and were harmed as a result.

101. Adequacy: Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has no known interest antagonistic to those of the Class and his interests are aligned with Class members' interests. Plaintiff was subject to the same Data Breach as class members, suffered similar harms, and faces similar threats due to the Data Breach. Plaintiff has also retained competent counsel with significant experience litigating complex class actions, including Data Breach cases involving multiple classes and data breach claims.

102. Commonality and Predominance: There are questions of law and fact common to the Class such that there is a well-defined community of interest in this litigation. These common questions predominate over any questions affecting only individual class members. The common questions of law and fact include, without limitation:

a. Whether Defendant owed Plaintiff and class members a duty to implement and maintain reasonable security procedures and practices to protect their PII and PHI;

b. Whether Defendant breached an express or implied contract with Plaintiff and class members, including whether Defendant breached an agreement with Plaintiff and class members to keep their PII and PHI confidential;

c. Whether Defendant received a benefit without proper restitution making it unjust for Defendant to retain the benefit without commensurate compensation;

d. Whether Defendant acted negligently in connection with the monitoring and/or protection of Plaintiff's and class members' PII and PHI;

e. Whether Defendant violated its duty to implement reasonable security systems to protect Plaintiff's and class members' PII and PHI;

f. Whether Defendant's breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiff and class members;

g. Whether Defendant adequately addressed and fixed the vulnerabilities that enabled the Data Breach;

h. Whether Plaintiff and class members are entitled to credit monitoring and other injunctive relief;

i. Whether Defendant provided timely notice of the Data Breach to Plaintiff and class members; and

j. Whether class members are entitled to compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the Data Breach.

103. Defendant has engaged in a common course of conduct and Plaintiff and class members have been similarly impacted by Defendant's failure to maintain reasonable security procedures and practices to protect patients' PII and PHI, as well as Defendant's failure to timely alert affected customers to the Data Breach.

104. 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. Absent a class action, most if not all class members would find the cost of litigating their individual claims prohibitively high and have no effective remedy. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members and risk inconsistent treatment of claims arising from the same set of facts and occurrences. Plaintiff knows of no difficulty likely to be encountered in the maintenance of this action as a class action under the applicable rules.

CLAIMS FOR RELIEF

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

105. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

106. Defendant required Plaintiff and class members to provide their PII and PHI as a condition of receiving healthcare services. Defendant collected and stored the data for purposes of providing medical treatment as well as for commercial gain.

107. Defendant owed Plaintiff and class members a duty to exercise reasonable care in protecting their PII and PHI from unauthorized disclosure or access. Defendant acknowledged this duty in its Notice of Privacy Policy, where it promised not to disclose PII and PHI without authorization.

108. Defendant owed a duty of care to Plaintiff and class members to provide adequate data security, consistent with industry standards, to ensure that Defendant's systems and networks adequately protected the PII and PHI.

109. As a healthcare provider, Defendant had a special relationship with Plaintiff and class members who entrusted Defendant to adequately their confidential personal, financial, and medical information.

110. Defendant's duty to use reasonable care in protecting PII and PHI arises as a result of the parties' relationship, as well as common law and federal law, including the HIPAA regulations described above and Defendant's own policies and promises regarding privacy and data security.

111. Defendant knew, or should have known, of the risks inherent in collecting and storing PII and PHI in a centralized location, Defendant's vulnerability to network attacks, and the importance of adequate security.

112. Defendant breached its duty to Plaintiff and class members in numerous ways, as described herein, including by:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the PII and PHI of Plaintiff and class members;

b. Failing to comply with industry standard data security measures for the healthcare industry leading up to the Data Breach;

c. Failing to comply with its own privacy policies;

d. Failing to comply with regulations protecting the PII and PHI at issue during the period of the Data Breach;

e. Failing to adequately monitor, evaluate, and ensure the security of Defendant's network and systems;

f. Failing to recognize in a timely manner that PII and PHI had been compromised; and

g. Failing to timely and adequately disclose the Data Breach.

113. Plaintiff's and class members' PII and PHI would not have been compromised but for Defendant's wrongful and negligent breach of their duties.

114. Defendant's failure to take proper security measures to protect the sensitive PII and PHI of Plaintiff and class members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access and exfiltration of PII and PHI by unauthorized third parties. Given that healthcare providers are prime targets for hackers, Plaintiff and class members are part of a foreseeable, discernible group that was at high risk of having their PII and PHI misused or disclosed if not adequately protected by Defendant.

115. It was also foreseeable that Defendant's failure to provide timely and forthright notice of the Data Breach would result in injury to Plaintiff and class members.

116. As a direct and proximate result of Defendant's conduct, Plaintiff and class members have and will suffer damages including: (i) the loss of rental or use value of their PII and PHI; (ii) the unconsented disclosure of their PII and PHI to unauthorized third parties; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PII and PHI; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on

credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII and PHI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect it; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives; and (ix) any nominal damages that may be awarded.

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

117. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

118. 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.

119. 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."

120. 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.

121. 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.

122. 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.

123. 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.

124. 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*.

125. Defendant breached its notification obligations under HIPAA by failing to give timely and complete notice of the breach to Plaintiff and class members.

126. 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.

127. 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.

128. 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.

129. Defendant's violations of HIPAA constitute negligence *per se*.

130. Plaintiff and class members are within the class of persons that HIPAA and its implementing regulations were intended to protect.

131. The harm that occurred as a result of the Data Breach is the type of harm HIPAA was intended to guard against.

132. 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).

133. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

134. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and failing to comply with applicable industry standards. Defendant's conduct was unreasonable given the nature and amount of PII and PHI they obtained, stored, and disseminated in the regular course of their business, and the foreseeable consequences of a data

breach, including, specifically, the significant damage that would result to Plaintiff and class members.

135. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

136. Plaintiff and class members are within the class of persons that the FTC Act was intended to protect.

137. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and class members.

138. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and class members sustained actual losses and damages as alleged herein.

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

139. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

140. Defendant disseminated a "Notice of Privacy Practices" to its patients which constitutes an agreement between Defendant and persons who provided their PII and PHI to Defendant, including Plaintiff and class members.

141. Plaintiff and class members formed a contract with Defendant and complied with all obligations under such contract when they provided PII to Defendant subject to the Notice of Privacy Practices.

142. 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."

143. Defendant breached its agreements with Plaintiff and class members when Defendant allowed for the disclose of Plaintiff's and class members' PII and PHI 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.

144. 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
(On Behalf of Plaintiff and the Class)

145. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs and assert this claim in the alternative to his breach of contract claim to the extent necessary.

146. Plaintiff and class members were required to provide their PII to Defendant in order to receive healthcare services and treatment.

147. As part of these transactions, Defendant agreed to safeguard and protect the PII and PHI of Plaintiff and class members. Implicit in these transactions between Defendant and class members was the obligation that Defendant would use the PII and PHI for approved business purposes only and would not make unauthorized disclosures of the information or allow unauthorized access to the information.

148. Additionally, Defendant implicitly promised to retain this PII and PHI only under conditions that kept such information secure and confidential and therefore had a duty to reasonably safeguard and protect the PII and PHI of Plaintiff and class members from unauthorized disclosure or access.

149. 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 PII and PHI.

150. Plaintiff and class members would not have provided and entrusted their PII and PHI 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' PII and PHI was critical to realizing the intent of the parties.

151. 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' PII and PHI in order to prevent harm and prevent present and continuing increased risk.

152. Defendant breached their implied contract with Plaintiff and class members by failing to reasonably safeguard and protect Plaintiff's and class members' PII and PHI, which was compromised as a result of the Data Breach.

153. 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
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

154. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs and assert this claim in the alternative to their breach of contract claims to the extent necessary.

155. Plaintiff and class members have an interest, both equitable and legal, in their PII and PHI that was conferred upon, collected by, and maintained by the Defendant and which was stolen in the Data Breach. This information has independent value.

156. 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.

157. Defendant appreciated and had knowledge of the benefits conferred upon it by Plaintiff and class members.

158. 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.

159. 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.

160. 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 VI
Breach of Confidence
(On Behalf of Plaintiff and the Class)

161. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

162. 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.

163. 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.

164. 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.

165. Plaintiff and class members suffered harm the moment the unconsented disclosure of the confidential information to an unauthorized third party took place.

166. 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 VII
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

167. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

168. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and 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 statutes described in this Complaint.

169. 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 PII and PHI and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and class members from further cyberattacks and data breaches that could compromise their PII and PHI.

170. Defendant still possesses PII and PHI pertaining to Plaintiff and class members, which means their PII remains at risk of further breaches because Defendant's data security measures remain inadequate. Plaintiff and class members continue to suffer injuries as a result of the compromise of their PII and PHI and remain at an imminent risk that additional compromises of their PII and PHI will occur in the future.

171. Pursuant to the Declaratory Judgment Act, Plaintiff seeks a declaration that: (a) Defendant's existing data security measures do not comply with its obligations and duties of care; and (b) in order to comply with their obligations and duties of care, (1) Defendant must have

policies and procedures in place to ensure the parties with whom it shares sensitive personal information maintain reasonable, industry-standard security measures, including, but not limited to, those listed at (ii), (a)-(i), *infra*, and must comply with those policies and procedures; (2) Defendant must: (i) purge, delete, or destroy in a reasonably secure manner Plaintiff's and class members' PII and PHI if it is no longer necessary to perform essential business functions so that it is not subject to further theft; and (ii) implement and maintain reasonable, industry-standard security measures, including, but not limited to:

a. Engaging 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;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Encrypting PII and PHI and segmenting PII and PHI by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of its systems;

e. Purging, deleting, and destroying in a reasonable and secure manner PII and PHI not necessary to perform essential business functions;

f. Conducting regular database scanning and security checks;

g. Conducting regular employee education regarding best security practices;

h. Implementing multi-factor authentication and POLP to combat system-wide cyberattacks; and

i. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and the Class set forth herein, respectfully requests the following relief:

A. That the Court certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, appoint Plaintiff as class representatives and Plaintiff's counsel as Class Counsel;

B. That the Court grant permanent injunctive relief to prohibit and prevent Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiff and class members compensatory, consequential, and general damages, including nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

D. That the Court award statutory damages, trebled, and/or punitive or exemplary damages, to the extent permitted by law;

E. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of their unlawful acts, omissions, and practices;

F. That Plaintiff be granted the declaratory and injunctive relief sought herein;

G. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses; and

H. That the Court award pre-and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial in the instant action.

Dated: January 8, 2022

/s/ *Julie Braman Kane*
Julie Braman Kane
(Florida Bar No.: 980277)
julie@colson.com
COLSON HICKS EIDSON
255 Alhambra Circle – Penthouse
Coral Gables, Florida 33134
Telephone: (305) 476-7400
Facsimile: (305) 476-7444

Norman E. Siegel*
J. Austin Moore*
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: (816) 714-7100
siegel@stuevesiegel.com
moore@stuevesiegel.com
**Pro Hac Vice Forthcoming*

Counsel for Plaintiff and the Class