SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF KINGS
_____X

KIYA JOHNSON, SUSAN MUTNICK, NOYIELLE SUTHERLAND, JASMINE ROGERS, MARCUS ROBINSON, SHAKIRA JONES, DEWANNA WASHINGTON, and ANIKA FRANCIS individually and on behalf of all others similarly situated,

Plaintiffs,

- vs-

ONE BROOKLYN HEALTH SYSTEM, INC.,

Defendant.
_____X

PLAINTIFFS' FIRST AMENDED CLASS ACTION COMPLAINT

Index No.: 512485/2023

JURY TRIAL DEMANDED

Plaintiffs Kiya Johnson, Susan Mutnick, Noyielle Sutherland, Jasmine Rogers, Marcus Robinson, Shakira Jones, DeWanna Washington, and Anika Francis (together, "Plaintiffs"), individually and on behalf of all others similarly situated, file this First Amended Class Action Complaint against Defendant One Brooklyn Health System, Inc. ("Defendant" or "OBH"). Plaintiffs seek to obtain damages, restitution, and injunctive relief for the Class, as defined below, from OBH as a result of its failure to adequately safeguard the sensitive data entrusted to it by Plaintiffs and those similarly situated. Plaintiffs make the following allegations upon information and belief, except as to their own actions which are based upon the investigation of their counsel.

NATURE OF THE CASE

1. Healthcare providers that handle sensitive, personally identifying information ("PII") or protected health information ("PHI") owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of PII or PHI to unauthorized

persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private health matters.

2. The harm resulting from a data and privacy breach manifests in a number of ways, including identity theft and financial fraud. The exposure of a person's PII or PHI through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and take a number of additional prophylactic measures.

3. As a comprehensive local healthcare provider, OBH knowingly obtains sensitive patient PII and PHI and has a resulting duty to securely maintain such information in confidence. Indeed, OBH's "Notice of Privacy Practices" acknowledges that it is "required by law to maintain confidentiality of your protected health information" and assures patients that it will "keep[] your information private and confidential."[1] Its Privacy Practices delineate certain limited situations where patient data entrusted to OBH may be shared, such as where necessary to facilitate medical treatment.

4. OBH breached these promises set forth in its own Privacy Practices and as established as a matter of law by failing to implement measures sufficient to adequately safeguard the highly sensitive personal and medical data entrusted to it. This, in turn, allowed the sensitive PII and PHI of Plaintiffs and those similarly situated to be accessed and exposed to unauthorized

[1] *Notice of Privacy Practices*, One Brooklyn Health, https://onebrooklynhealth.org/media/abab33wi/obhs-notice-of-privacy-practices-04112023-4.docx.

third parties during a data breach of OBH's system on or about November 19, 2022, which OBH belatedly announced on or about April 20, 2023 (the "Data Breach").[2]

5. Based on the public statements of OBH to date, a wide variety of PII and PHI was implicated in the breach, including but not limited to: names, dates of birth, Social Security Numbers, driver's license and state ID numbers, financial account and payment card information, medical information, and health insurance information.[3]

6. Plaintiffs and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their health privacy, and similar forms of criminal mischief, risk which may last for the rest of their lives. Consequently, Plaintiffs and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

7. Plaintiffs, on behalf of themselves and the Class as defined herein, bring claims for negligence, negligence *per se*, breach of fiduciary duty, breach of an implied contract, breach of an express contract, unjust enrichment, violations of GEN. BUS. LAW § 349, and the common law of New York, and seek declaratory judgment, actual, treble, and putative damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

8. To recover from OBH for their sustained, ongoing, and future harms, Plaintiffs and the Class seek damages in an amount to be determined at trial, declaratory judgment, and injunctive relief requiring OBH to: 1) disclose, expeditiously, the full nature of the Data Breach and the types of PII and PHI accessed, obtained, or exposed by the hackers; 2) implement improved data security

[2] *Notice of Data Security Event* (April 20, 2023), https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-201.pdf.
[3] *One Brooklyn Health Notice of Data Security Event*, https://onebrooklynhealth.org/media/p4abqfwk/obh-website-notice.pdf. (last visited December 13, 2023).

practices to reasonably guard against future breaches of PII and PHI possessed by Defendant; and 3) provide, at its own expense, all impacted victims with identity theft protection services for an appropriate period of time.

PARTIES

Plaintiffs

9. Plaintiff Kiya Johnson is an adult who is a resident and citizen of the borough of Brooklyn, located in Kings County in the State of New York.

10. Plaintiff Susan Mutnick is an adult who is a resident and citizen of the borough of Brooklyn, located in Kings County in the State of New York.

11. Plaintiff Noyielle Sutherland is an adult who is a resident and citizen of Hudson County in the State of New Jersey.

12. Plaintiff Jasmine Rogers is an adult who is a resident and citizen of Fort Bend County in the State of Texas.

13. Plaintiff Marcus Robinson is an adult who is a resident and citizen of the borough of Brooklyn, located in Kings County in the State of New York.

14. Plaintiff Shakira Jones is an adult who is a resident and citizen of the borough of Brooklyn, located in Kings County in the State of New York.

15. Plaintiff DeWanna Washington is an adult who is a resident and citizen of the borough of Brooklyn, located in Kings County in the State of New York.

16. Plaintiff Anika Francis is an adult who is a resident and citizen of the borough of Brooklyn, located in Kings County in the State of New York.

Defendant

17. Defendant One Brooklyn Health System, Inc. is an entity incorporated in Kings County in the State of New York with a principal place of business located at 1545 Atlantic Avenue, Brooklyn, New York 11213.

18. Defendant OBH provides comprehensive local healthcare at 3 hospitals in Eastern Brooklyn and is comprised of more than 600 providers with over 50 specialties.[4]

JURISDICTION AND VENUE

19. This Court has personal jurisdiction over Defendant One Brooklyn Health System, Inc. because it conducts business and has its principal place of business within the State of New York and this judicial district.

20. Venue is proper in this Court pursuant to CPLR § 503 because Defendant One Brooklyn Health System, Inc. regularly advertises and markets its services and conducts business and because a substantial part of the events or omissions giving rise to the claims occurred in this judicial district.

FACTUAL BACKGROUND

A. OBH and the Services it Provides.

21. OBH is a 501(c)(3) enterprise providing inpatient acute care, community-based ambulatory care and long-term care services throughout East and Central Brooklyn.[5]

22. While administering healthcare services, OBH receives, creates, and handles PII and PHI, which includes, *inter alia*, patients' full name, address, date of birth, Social Security

[4] *See OBH Linked In Page*, https://www.linkedin.com/company/one-brooklyn-health-system-inc/ (last visited Dec. 13, 2023).
[5] *Id.*

Number, driver's license or state ID number, financial account and payment card information, medical information, and health insurance information.

23. Plaintiffs and Class Members entrusted this information to OBH with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

24. As noted above, OBH contains a comprehensive "Notice of Privacy Practices" that acknowledges its obligations to keep Plaintiffs' and Class Members' PII and PHI confidential and secure from unauthorized access.[6] The notice states "OBH is required by law to maintain confidentiality of your protected health information (PHI)."[7] It later acknowledges that the Notice of Privacy Practices "tells [patients] how [their] PHI may be used and how OBH keeps [patients] information private and confidential and applies regardless on which campus or facility in which [patients] receive care."[8]

25. By obtaining, collecting, and storing Plaintiffs' and Class Members' PII and PHI, OBH assumed legal and equitable duties and knew or should have known that OBH was reasonably responsible for protecting Plaintiffs' and Class Members PII and PHI from unauthorized disclosure.

26. Despite OBH purporting that it "prioritizes its responsibility to safeguard the information it collects in providing services,"[9] OBH nevertheless employed inadequate data security measures to protect and secure the PII and PHI patients entrusted to it, resulting in the Data Breach and compromise of Plaintiffs' and Class Members' PII and PHI.

---

[6] *Notice of Privacy Practices, supra* note 1.
[7] *Id.*
[8] *Id.*
[9] *One Brooklyn Health Notice of Data Security Event, supra* note 5.

B. OBH Knew the Risks of Storing Valuable PII and PHI and the Foreseeable Harm to its Patients.

27. At all relevant times, OBH knew it was storing sensitive PII and PHI and that, as a result, its systems would be an attractive target for cybercriminals.

28. OBH also knew that a breach of its systems—and the exposure of the information stored therein—would result in the increased risk of identity theft and fraud against the individuals whose PII and PHI was compromised, as well as intrusion into their highly private health information.

29. These risks are not theoretical. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[10]

30. "Hospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily—making the industry a growing target."[11]

31. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July 2022. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[12]

[10] *The healthcare industry is at risk*, SwivelSecure, https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited Dec. 13, 2023).
[11] *Id.*
[12] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year.

32. Further, a 2022 report released by IBM Security stated that for 12 consecutive years the healthcare industry has had the highest average cost of a data breach and as of 2022 healthcare data breach costs have hit a new record high.[13]

33. Indeed, cyberattacks against the healthcare industry have been common over the past ten years with the Federal Bureau of Investigation ("FBI") warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." [14] The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[15]

34. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[16]

35. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[17]

---

[13] *Cost of a Data Breach Report 2022*, IBM Security, https://www.ibm.com/downloads/cas/3R8N1DZJ (last visited Dec. 13, 2023).
[14] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.
[15] *Id*.
[16] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.
[17] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-

36. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's patients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

37. PII and PHI is a valuable property right.[18] The value of PII and PHI as a commodity is measurable.[19] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[20] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[21] It is so valuable to identity thieves that once PII and PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years after the breach.

38. As a result of their real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, PII and PHI, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information

---

cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited Dec. 13, 2023).

[18] *See* Marc Van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION & COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . . ").

[19] Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle. /824192.

[20] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[21] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

exposed in the Data Breach, can be aggregated and becomes more valuable to thieves and more damaging to victims.

39. PHI is particularly valuable and has been referred to as a "treasure trove for criminals." [22] As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[23] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[24]

40. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.

---

[22] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[23] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, IDX (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[24] *Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security® Survey 2015*, PriceWaterhouseCoopers, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last visited Dec. 13, 2023).

> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[25]

41. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

42. Consumers place a high value on the privacy of their data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites." [26]

43. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII and PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

---

[25] Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, Experian (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

[26] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) Information Systems Research 254 (June 2011), https://www.guanotronic.com/~serge/papers/weis07.pdf.

44. Based on the value of its patients' PII and PHI to cybercriminals and cybercriminals' propensity to target healthcare providers, OBH certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

C. OBH Breached its Duty to Protect its Patients' PII and PHI.

45. As noted above, OBH announced on April 20, 2023 that it experienced a security incident disrupting access to its systems.[27]

46. According to OBH, it engaged external specialists to commence an investigation into the nature and scope of the Data Breach.[28]

47. The investigation confirmed that data containing PII and PHI may have been accessed or acquired by an unauthorized third party.[29]

48. After the investigation revealed that PII and PHI may have been accessed or acquired by an unauthorized third party, OBH then conducted a review process to confirm what it already knew—that PII and PHI of current and former patients had been compromised.[30] This review process took an additional four months and was completed on March 21, 2023.[31]

49. The patient PII and PHI compromised in the Data Breach includes patient names, dates of birth, Social Security Numbers, driver's license or state ID numbers, financial account and/or payment information, medical information, and health insurance information.[32]

[27] *One Brooklyn Health Notice of Data Security Event*, *supra* note 5.
[28] *Id.*
[29] *Id.*
[30] *Id.*
[31] *Id.*
[32] *Id.*

50. Despite OBH discovering the cybersecurity incident on November 19, 2022, OBH did not report the Data Breach to the Attorney General of Montana ("AG MT") until April 20, 2023.[33]

51. On or about the same date that OBH reported the Data Breach to AG MT, OBH provided notice to Plaintiffs indicating that her PII and PHI may have been compromised or accessed during the Data Breach, approximately six months after OBH first discovered the Data Breach.

52. Like Plaintiffs, the Class Members received similar notices informing them that their PII and/or PHI was exposed in the Data Breach.

53. All in all, approximately 235,251 people who had entrusted their PII and PHI to OBH had their sensitive information breached.[34]

54. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures in order to protect its patients' PII and PHI.

D. Plaintiffs' Experiences

Plaintiff Kiya Johnson

55. Plaintiff Kiya Johnson was required to provide her PII and PHI to OBH in connection with receiving healthcare or other services from OBH.

56. Based on representations made by OBH, Plaintiff Johnson believed that OBH had implemented and maintained reasonable security and practices to protect her PII and PHI. With

[33]*Reported Data Breach Incidents,* Montana Attorney General, https://dojmt.gov/consumer/databreach/ (last visited Dec. 13, 2023).
[34]*Notice of Data Security Event,* Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/73e780c9-ea42-4b82-9d46-41bc962aceb5.shtml (last visited Dec. 13, 2023).

this belief in mind, Plaintiff Johnson provided her PII and PHI to OBH in connection with or in exchange for healthcare or other related services or products provided by OBH.

57. In connection with services provided to Plaintiff Johnson, OBH stores and maintains Plaintiff Johnson's PII and PHI on its systems, including the system involved in the Data Breach.

58. Had Plaintiff Johnson known that OBH does not adequately protect the PII and PHI in its possession, she would not have agreed to provide OBH with her PII and PHI or used OBH's services.

59. Plaintiff Johnson received a letter from OBH notifying her that her PII and PHI was exposed in the Data Breach.

60. As a direct result of the Data Breach, Plaintiff Johnson has suffered injury and damages including, *inter alia*: a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII and PHI; deprivation of the value of her PII and PHI; and overpayment for services that did not include adequate data security. Plaintiff Johnson estimates that she has spent at least two hours dealing with the ramifications of the Data Breach.

Plaintiff Susan Mutnick

61. Plaintiff Susan Mutnick was required to provide her PII and PHI to OBH in connection with receiving healthcare or other services from OBH.

62. Based on representations made by OBH, Plaintiff Mutnick believed that OBH had implemented and maintained reasonable security and practices to protect her PII and PHI. With this belief in mind, Plaintiff Mutnick provided her PII and PHI to OBH in connection with or in exchange for healthcare or other related services or products provided by OBH.

63. In connection with services provided to Plaintiff Mutnick, OBH stores and maintains Plaintiff's PII and PHI on its systems, including the system involved in the Data Breach.

64. Had Plaintiff Mutnick known that OBH does not adequately protect the PII and PHI in its possession, she would not have agreed to provide OBH with her PII and PHI or used OBH's services.

65. Plaintiff Mutnick received a letter from OBH notifying her that her PII and PHI was exposed in the Data Breach.

66. As a direct result of the Data Breach, Plaintiff Mutnick has suffered injury and damages including, *inter alia*: a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII and PHI; deprivation of the value of her PII and PHI; and overpayment for services that did not include adequate data security. Plaintiff Mutnick also spends about two hours per month ensuring that no unusual activity happens on her financial accounts.

Plaintiff Noyielle Sutherland

67. Plaintiff Noyielle Sutherland was required to provide her PII and PHI to OBH in connection with receiving healthcare or other services from OBH.

68. Based on representations made by OBH, Plaintiff Sutherland believed that OBH had implemented and maintained reasonable security and practices to protect her PII and PHI. With this belief in mind, Plaintiff Sutherland provided her PII and PHI to OBH in connection with or in exchange for healthcare or other related services or products provided by OBH.

69. In connection with services provided to Plaintiff Sutherland, OBH stores and maintains Plaintiff's PII and PHI on its systems, including the system involved in the Data Breach.

70. Had Plaintiff Sutherland known that OBH does not adequately protect the PII and PHI in its possession, she would not have agreed to provide OBH with her PII and PHI or used OBH's services.

71. Plaintiff Sutherland received a letter from OBH notifying her that her PII and PHI was exposed in the Data Breach.

72. As a direct result of the Data Breach, Plaintiff Sutherland has suffered injury and damages including, *inter alia*: a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII and PHI; deprivation of the value of her PII and PHI; and overpayment for services that did not include adequate data security. In total, Plaintiff Sutherland estimates she has spent approximately 20 hours dealing with the ramifications of the Data Breach.

73. In addition, Plaintiff Sutherland has also experienced actual fraud as a result of the Data Breach. Shortly after the Data Breach occurred, Plaintiff Sutherland received a denial letter for an Amazon Credit Card, which she had not applied for herself. After this happened, Plaintiff Sutherland contacted Amazon regarding the fraudulent application and spent time changing her passwords. She estimates that she spent approximately five (5) hours dealing with the incident.

Plaintiff Jasmine Rogers

74. Plaintiff Jasmine Rogers was required to provide her PII and PHI to OBH in connection with receiving healthcare or other services from OBH.

75. Based on representations made by OBH, Plaintiff Rogers believed that OBH had implemented and maintained reasonable security and practices to protect her PII and PHI. With this belief in mind, Plaintiff Rogers provided her PII and PHI to OBH in connection with or in exchange for healthcare or other related services or products provided by OBH.

76. In connection with services provided to Plaintiff Rogers, OBH stores and maintains Plaintiff Rogers' PII and PHI on its systems, including the system involved in the Data Breach.

77. Had Plaintiff Rogers known that OBH does not adequately protect the PII and PHI in its possession, she would not have agreed to provide OBH with her PII and PHI or used OBH's services.

78. Plaintiff Rogers received a letter from OBH notifying her that her PII and PHI was exposed in the Data Breach.

79. As a direct result of the Data Breach, Plaintiff Rogers has suffered injury and damages including, *inter alia*: a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII and PHI; deprivation of the value of her PII and PHI; and overpayment for services that did not include adequate data security. In total, Plaintiff Rogers estimates she has spent approximately 10 to 12 hours dealing with the ramifications of the Data Breach.

80. In addition, Plaintiff Rogers has experienced actual fraud as a result of the Data Breach. In June of 2023, someone attempted to charge $200 on her Chase Bank Debit Card. As a result, she had to shut down her online banking. She was eventually reimbursed for the fraudulent charge by Chase and had to get a new Debit Card. Plaintiff Rogers estimates that she spent approximately 10 to 12 hours dealing with the fraudulent charges.

Plaintiff Marcus Robinson

81. Plaintiff Marcus Robinson was required to provide his PII and PHI to OBH in connection with receiving healthcare or other services from OBH.

82. Based on representations made by OBH, Plaintiff Robinson believed that OBH had implemented and maintained reasonable security and practices to protect his PII and PHI. With

this belief in mind, Plaintiff Robinson provided his PII and PHI to OBH in connection with or in exchange for healthcare or other related services or products provided by OBH.

83. In connection with services provided to Plaintiff Robinson, OBH stores and maintains Plaintiff Robinson's PII and PHI on its systems, including the system involved in the Data Breach.

84. Had Plaintiff Robinson known that OBH does not adequately protect the PII and PHI in its possession, he would not have agreed to provide OBH with his PII and PHI or used OBH's services.

85. Plaintiff Robinson received a letter from OBH notifying him that his PII and PHI was exposed in the Data Breach.

86. As a direct result of the Data Breach, Plaintiff Robinson has suffered injury and damages including, *inter alia*: a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive PII and PHI; deprivation of the value of his PII and PHI; and overpayment for services that did not include adequate data security. In total, Plaintiff Robinson estimates he has spent several hours dealing with the ramifications of the Data Breach.

87. In addition, Plaintiff Robinson has experienced actual fraud as a result of the Data Breach. Plaintiff Robinson had a bank account opened in his name at KeyBank in Pennsylvania. He learned of the account when he was sent a letter about a PIN. Plaintiff Robinson called the bank to inform them that he did not open the account. Plaintiff Robinson spent hours attempting to deal with the fraudulent account.

Plaintiff Shakira Jones

88. Plaintiff Shakira Jones was required to provide her PII and PHI to OBH in connection with receiving healthcare or other services from OBH.

89. Based on representations made by OBH, Plaintiff Jones believed that OBH had implemented and maintained reasonable security and practices to protect her PII and PHI. With this belief in mind, Plaintiff Jones provided her PII and PHI to OBH in connection with or in exchange for healthcare or other related services or products provided by OBH.

90. In connection with services provided to Plaintiff Jones, OBH stores and maintains Plaintiff Jones' PII and PHI on its systems, including the system involved in the Data Breach.

91. Had Plaintiff Jones known that OBH does not adequately protect the PII and PHI in its possession, she would not have agreed to provide OBH with her PII and PHI or used OBH's services.

92. Plaintiff Jones received a letter from OBH notifying her that her PII and PHI was exposed in the Data Breach.

93. As a direct result of the Data Breach, Plaintiff Jones has suffered injury and damages including, *inter alia*: a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII and PHI; deprivation of the value of her PII and PHI; and overpayment for services that did not include adequate data security. In total, Plaintiff Jones estimates she has spent approximately 10 to 12 hours dealing with the ramifications of the Data Breach.

94. In addition, Plaintiff Jones has experienced actual fraud as a result of the Data Breach. Since the Data Breach, she has had hard inquiries for credit cards made in her name and had incorrect addresses listed on her credit report. It took approximately 90 days for the incorrect

addresses to be removed. She also has seen an increase in spam calls, which she receives approximately 4 to 5 of per day, which started around November of 2022.

Plaintiff DeWanna Washington

95. Plaintiff DeWanna Washington was required to provide her PII and PHI to OBH in connection with receiving healthcare or other services from OBH.

96. Based on representations made by OBH, Plaintiff Washington believed that OBH had implemented and maintained reasonable security and practices to protect her PII and PHI. With this belief in mind, Plaintiff Washington provided her PII and PHI to OBH in connection with or in exchange for healthcare or other related services or products provided by OBH.

97. In connection with services provided to Plaintiff Washington, OBH stores and maintains Plaintiff Washington's PII and PHI on its systems, including the system involved in the Data Breach.

98. Had Plaintiff Washington known that OBH does not adequately protect the PII and PHI in its possession, she would not have agreed to provide OBH with her PII and PHI or used OBH's services.

99. Plaintiff Washington received a letter from OBH notifying her that her PII and PHI was exposed in the Data Breach.

100. As a direct result of the Data Breach, Plaintiff Washington has suffered injury and damages including, *inter alia*: a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII and PHI; deprivation of the value of her PII and PHI; and overpayment for services that did not include adequate data security. In total, Plaintiff Washington estimates she has spent approximately 3 to 4 hours dealing with the ramifications of the Data Breach.

Plaintiff Anika Francis

101. Plaintiff Anika Francis was required to provide her PII and PHI to OBH in connection with receiving healthcare or other services from OBH.

102. Based on representations made by OBH, Plaintiff Francis believed that OBH had implemented and maintained reasonable security and practices to protect her PII and PHI. With this belief in mind, Plaintiff Francis provided her PII and PHI to OBH in connection with or in exchange for healthcare or other related services or products provided by OBH.

103. In connection with services provided to Plaintiff Francis, OBH stores and maintains Plaintiff Francis's PII and PHI on its systems, including the system involved in the Data Breach.

104. Had Plaintiff Francis known that OBH does not adequately protect the PII and PHI in its possession, she would not have agreed to provide OBH with her PII and PHI or used OBH's services.

105. Plaintiff Francis received a letter from OBH notifying her that her PII and PHI was exposed in the Data Breach.

106. As a direct result of the Data Breach, Plaintiff Francis has suffered injury and damages including, *inter alia*: a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII and PHI; deprivation of the value of her PII and PHI; and overpayment for services that did not include adequate data security. In total, Plaintiff Francis estimates she has spent approximately 25 hours dealing with the ramifications of the Data Breach.

107. In addition, Plaintiff Francis has suffered actual identity fraud as a result of the Data Breach. After the Data Breach occurred, someone attempted to open a Discover Card in her name. She spent time informing the bank that she did not make the application and the bank cancelled

the application. Plaintiff Francis' debit card was also separately compromised, requiring her to obtain a new debit card.

E. OBH is Obligated Under HIPAA to Safeguard Personal Information

108. OBH is required by the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1302d, *et seq*. ("HIPAA") to safeguard patient PHI. Under HIPAA health insurance providers have an affirmative duty to keep patients' PHI private.

109. OBH is an entity covered under HIPAA, which sets minimum federal standards for privacy and security of PHI. As a covered entity, Defendant has a statutory duty under HIPAA to safeguard Plaintiffs' and Class Members' PHI.

110. HIPAA establishes national standards for the protection of PHI. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302. This includes compliance with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E (Standards for Privacy of Individually Identifiable Health Information"), and the 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.

111. Under 45 C.F.R. § 160.103, HIPAA defines "protected health information" or PHI as "individually identifiable health information" that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."

112. Under C.F.R. § 160.103, HIPAA defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2)"[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an

individual;" and (3) either (a) identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual."

113. HIPAA requires OBH to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 CFR § 164.102, *et. seq*.

114. HIPAA also requires OBH to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under C.F.R. § 164.306(e), and to "[i]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 rules." 45 C.F.R. § 164.312(a)(1).

115. Further, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[35]

116. While HIPAA permits healthcare providers to disclose PHI to third parties under certain circumstances, HIPAA does not permit healthcare providers to disclose PHI to cybercriminals nor did Plaintiffs or the Class Members consent to the disclosure of their PHI to cybercriminals.

[35] *Breach Notification Rule*, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

117. As such, OBH is required under HIPAA to maintain the strictest confidentiality of Plaintiffs' and Class Members' PHI that it requires, receives, and collects, and Defendant is further required to maintain sufficient safeguards to protect that information from being accessed by unauthorized third parties.

118. Given the application of HIPAA to OBH and that Plaintiffs and Class Members entrusted their PHI to Defendant in order to receive healthcare services, Plaintiffs and Class Members reasonably expected that Defendant would safeguard their highly sensitive information and keep their PHI confidential.

F. FTC Guidelines Prohibit OBH from Engaging in Unfair or Deceptive Acts or Practices.

119. OBH is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

120. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[36]

121. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no

[36] *Start with Security – A Guide for Business*, United States Federal Trade Comm'n (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[37]

122. The FTC further recommends that companies only maintain PII as long as needed for authorization of a transaction; limit access to private 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.[38]

123. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

124. OBH failed to properly implement basic data security practices. OBH's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

125. OBH was at all times fully aware of its obligations to protect the PII and PHI of patients because of its position as a healthcare provider, which gave it direct access to reams of patient PII and PHI. Defendant was also aware of the significant repercussions that would result from its failure to do so.

[37] *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformationpdf.
[38] *Id.*

G. Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft.

126. Cyberattacks and data breaches at healthcare companies like OBH are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

127. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[39]

128. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[40]

129. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[41]

130. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims and to take over victims'

[39] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour /science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.

[40] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 HEALTH SERVICES RESEARCH 971, 971-980 (2019), https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

[41] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007), https://www.gao.gov/new.items/d07737.pdf.

identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

131. Criminals can use stolen PII and PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[42] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "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."[43]

132. Theft of PII and PHI is serious. The FTC warns consumers that identity thieves use PII and PHI to exhaust financial accounts, receive medical treatment, open new utility accounts, and incur charges and credit in a person's name.

133. The FTC recommends that identity theft victims take several steps to protect their

[42]. *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon ("*What Happens to Stolen Healthcare Data*") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing freezes on their credit, and correcting their credit reports.[44]

134. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.

135. Identity thieves can also use the victim's name and Social Security number to obtain government benefits or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, and/or rent a house or receive medical services in the victim's name.

136. Moreover, theft of PII and PHI is also gravely serious because PII and PHI is an extremely valuable property right.[45]

137. Theft of PHI, in particular, is gravely serious. Data breaches involving medical

[44] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last accessed Feb. 24, 2023).

[45] *See, e.g.*, John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years." [46] It "is also more difficult to detect, taking almost twice as long as normal identity theft." [47] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [48] The FTC also warns, "If the thief's health information is mixed with yours it could affect the medical care you're able to get or the health insurance benefits you're able to use." [49]

138. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

139. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States. For example, with the PII and PHI stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government

[46] Pam Dixon & John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.
[47] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.
[48] *See What to Know About Medical Identity Theft*, FED. TRADE COMM'N CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Dec. 11, 2023).
[49] *Id.*

benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft. These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class Members.

140. As discussed above, PII and PHI is a valuable commodity to identity thieves. Once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

141. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number:** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refund, employment—even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your lift in so many ways. [50]

142. For instance, with a stolen Social Security number, which is only one subset of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[51]

143. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[52] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[53] Each of these fraudulent

[50] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number* (Nov. 2, 2017), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (emphasis added).
[51] *Id.*
[52] *Id.*
[53] *Id.* at 4.

activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

144. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[54]

145. This was a financially motivated Data Breach, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against companies like OBH is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. This data demands a much higher price on the black market.

146. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[55] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[56]

[54] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.
[55] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.
[56] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

147. The medical information, PHI, which was exposed is also highly valuable. PHI can sell for as much as $363 according to the Infosec Institute.[57]

148. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to PII, they will use it.[58]

149. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum.[59] "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[60]

150. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[61] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[62] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[63] The FTC also warns, "If the thief's health

---

[57] Center for Internet Security, *Data Breaches: In the Healthcare Sector*, https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last visited Dec. 13, 2023).
[58] *Id.*
[59] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, Kaiser Health News, (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/.
[60] *Id.*
[61] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, WORLD PRIVACY FORUM 6 (Dec. 12, 2017), https://www.worldprivacyforum.org/2017/12/new-report-the-geography-of-medical-identity-theft/.
[62] *FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions* (May 6, 2014), https://publicintelligence.net/fbi-health-care-cyber-intrusions.
[63] *What to Know About Medical Identity Theft*, Federal Trade Commission, https://consumer.ftc.gov/sites/default/files/articles/pdf/973a-medical-idtheft-what-to-know-what-to-do-508_0.pdf.

information is mixed with yours, it could affect the medical care you're able to get or the health insurance benefits you're able to use. It could also hurt your credit."[64]

151. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services not sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[65]

152. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even

[64] *Id.*

[65] *FTC Informational Injury Workshop*, (October 2018), https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf.

years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

153. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[66]

154. Cybercriminals can post stolen PII and PHI on the cyber black-market for years following a data breach, thereby making such information publicly available.

155. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened. [67] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[68]

156. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[69]

---

[66] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

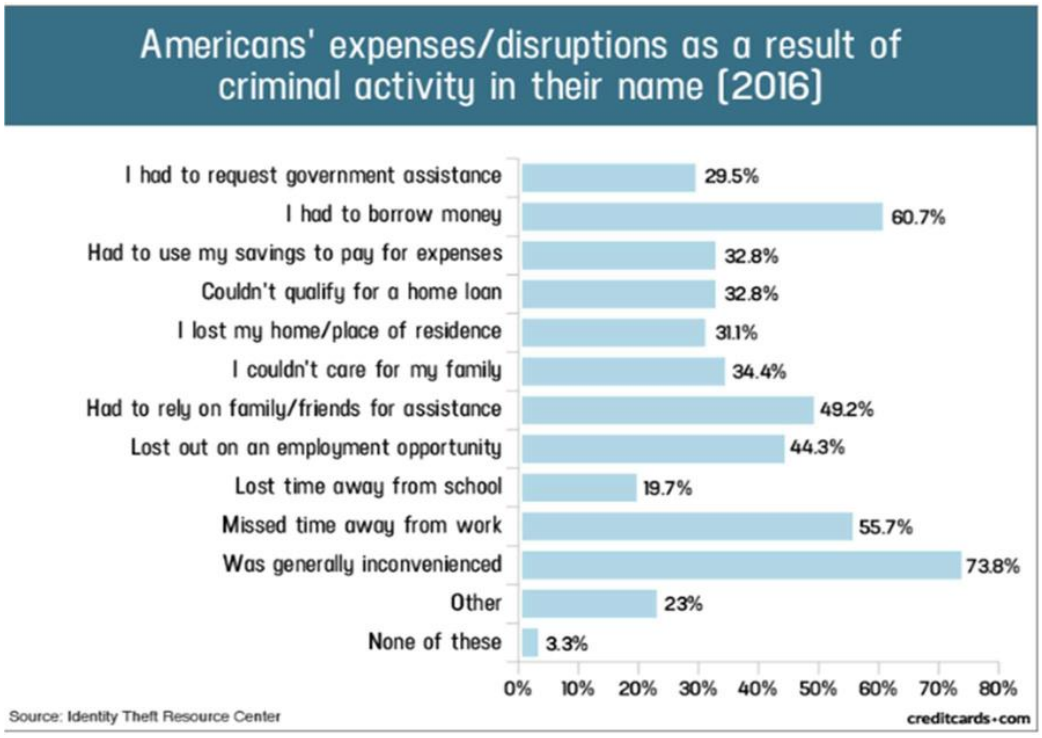
[67] *See* Medical ID Theft Checklist, https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last visited Dec. 13, 2023).

[68] Experian, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages*"), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited Dec. 13, 2023).

[69] *Guide for Assisting Identity Theft Victims*, Fed. Trade Comm'n, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

157. It is within this context that Plaintiffs and all other Class Members must now live with the knowledge that their PII and PHI is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

158. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information.



159. Victims of the Data Breach, like Plaintiffs and Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[70]

160. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have had their PII and PHI exposed; have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

[70] *Id.*

Plaintiffs and Class Members must now take the time and effort (and spend money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

161. Moreover, Plaintiffs and Class Members have an interest in ensuring that their PII and PHI, which remains in the possession of OBH, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. OBH has shown itself to be wholly incapable of protecting Plaintiffs' and Class Members' PII and PHI.

162. Plaintiffs and Class Members also have an interest in ensuring that their personal information that was provided to OBH is removed from OBH's unencrypted files.

163. OBH acknowledged, in its letter to Plaintiffs and Class Members, that, in response to the Data Breach, OBH has "implemented enhanced security measures and additional monitoring tools to reduce any risk associated with this incident and to better prevent similar incidents in the future."[71]

164. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. For this reason, OBH knew or should have known about these dangers and strengthened its data security

[71] *See Notice of Data Security Event*, *supra* note 2.

accordingly. OBH was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

H. Plaintiffs and Class Members Suffered Damages

165. OBH received Plaintiffs' PII and PHI in connection with providing certain medical services to them. In requesting and maintaining Plaintiffs' PII and PHI for business purposes, OBH expressly and implicitly promised and undertook a duty, to act reasonably in its handling of Plaintiffs' PII and PHI. OBH did not, however, take proper care of Plaintiffs' PII and PHI, leading to its exposure to and exfiltration by cybercriminals as a direct result of OBH's inadequate security measures.

166. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiffs and Class Members significant injuries and harm in several ways. Plaintiffs and members of the Class must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services and pay to procure them. Plaintiffs have taken or will be forced to take these measures in order to mitigate their potential damages as a result of the Data Breach.

167. The Data Breach also impacted the physical health of Plaintiffs because it caused many of OBH's "critical services" to remain offline for weeks, which led to delays in obtaining lab results and diagnostic imaging.

168. Once PII and PHI is exposed, there is little that can be done to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason,

Plaintiffs and Class Members will need to maintain these heightened measures for years and possibly their entire lives as a result of Defendant's conduct.

169. Further, the value of Plaintiffs' and Class Members' PII and PHI has been diminished by its exposure in the Data Breach. Plaintiffs and Class Members did not receive the full benefit of their bargain when paying for medical services and instead received services that were of a diminished value to those described in their agreements with OBH for the benefit and protection of Plaintiffs and Class Members and their respective PII and PHI. Plaintiffs and Class Members were damaged in an amount at least equal to the difference in the value between the services they thought they paid for (which would have included adequate data security protection) and the services they actually received.

170. Plaintiffs and Class Members would not have obtained medical services from OBH, or paid the amount they did to receive such, had they known that OBH would negligently fail to adequately protect their PII and PHI. Indeed, Plaintiffs paid for medical services with the expectation that OBH would keep their PII and PHI secure and inaccessible from unauthorized parties. Plaintiffs and Class Members would not have obtained services from OBH had they known that Defendant failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their PII and PHI from criminal theft and misuse.

171. As a result of Defendant's failures, Plaintiffs and Class Members are also at substantial and certainly impending increased risk of suffering identity theft and fraud or misuse of their PII and PHI.

172. Further, because Defendant was nearly six months delayed in notifying Plaintiffs and the Class about the Data Breach, Plaintiffs were unable to take affirmative steps during that time period to attempt to mitigate any harm or take preventative steps to protect against injury.

173. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[72]

174. With respect to health care breaches, another study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[73] Indeed, in 2013 alone, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States," which is more than identity thefts involving banking, finance, the government and the military, or education.[74]

175. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[75]

[72] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KnowBe4, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last visited Dec. 13, 2023).
[73] Jessica David, *70% of Data Involved in Healthcare Breaches Increases Risk of Fraud*, HealthITSecurity (Sept. 25, 2019) https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud.
[74] Michael Ollove, *supra* note 68.
[75] David, *supra* n. 73.

176. The reality is that cybercriminals seek nefarious outcomes from a data breach, and "stolen health data can be used to carry out a variety of crimes."[76]

177. Health information in particular is likely to be used in detrimental ways—by leveraging sensitive personal health details and diagnoses to extort or coerce someone or through serious and long-term identity theft.[77] This is especially true here, as the medical information at issue involves patients' drug and alcohol abuse treatments, and this information has already been leaked on the dark web.

178. A study by Experian found that the average total cost of medical identity theft is "about $20,000" per incident and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[78] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and forty percent were never able to resolve their identity theft at all.[79]

179. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[80]

---

[76] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HealthTech (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.
[77] *Id.*
[78] Elinor Mills, *Study: Medical Identity Theft is Costly for Victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.
[79] *Id.*; *see also* Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, Experian (Mar. 31, 2023), /www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.
[80] *The Potential Damages and Consequences of Medical Identity theft and Healthcare Data Breaches*, Experian (Apr. 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

180. Plaintiffs and Class Members are also at a continued risk because their information remains in Defendant's computer systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its patients' PII and PHI.

181. In addition, Plaintiffs and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers.

CLASS ALLEGATIONS

182. Plaintiffs sue on their own behalf and on behalf of a Class for damages and injunctive relief under CPLR § 901, *et seq*.

183. Plaintiffs seek to represent a class of persons to be defined as follows:

> All persons whose PII or PHI was compromised in the OBH Data Breach which was announced on or about April 20, 2023, including all persons who received a data breach notification letter from OBH.

184. Plaintiffs additionally seek to represent the following state subclasses:

> **New Jersey Subclass:** All New Jersey citizens whose PII or PHI was compromised in the OBH Data Breach which was announced on or about April 20, 2023, including all New Jersey citizens who received a data breach notification letter from OBH.
>
> **New York Subclass:** All New York citizens whose PII or PHI was compromised in the OBH Data Breach which was announced on or about April 20, 2023, including all New York citizens who received a data breach notification letter from OBH.
>
> **Texas Subclass:** All Texas citizens whose PII or PHI was compromised in the OBH Data Breach which was announced on or about April 20, 2023, including all Texas citizens who received a data breach notification letter from OBH.

185. Excluded from the Class are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assignees of any such excluded party, the judicial officers to whom this action is assigned, and the members of their immediate families.

186. This proposed class definition is based on the information available to Plaintiffs at this time. Plaintiffs may modify the class definition in an amended pleading or when they move for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

187. **Numerosity – CPLR § 901(a)(1).** Plaintiffs are informed and believe, and thereon allege, that there are at minimum, thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through OBH's records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes approximately 235,251 individuals.

188. **Commonality – CPLR § 901(a)(2).** This action involves questions of law and fact common to the Class. Such common questions include but are not limited to:

a. Whether OBH failed to timely notify Plaintiffs and Class Members of the Data Breach;

b. Whether OBH had a duty to protect the PII and PHI of Plaintiffs and Class Members;

c. Whether OBH was negligent in collecting and storing Plaintiffs' and Class Members' PII and PHI and breached its duties thereby;

d. Whether OBH breached its fiduciary duty to Plaintiffs and the Class;

e. Whether OBH breached its duty of confidence to Plaintiffs and the Class;

f. Whether OBH entered into an implied contract with Plaintiffs and the Class;

g. Whether OBH breached any express or implied contractual duties by failing to adequately safeguard Plaintiffs' and Class Members' PII and PHI;

h. Whether OBH was unjustly enriched;

i. Whether Plaintiffs and Class Members are entitled to damages as a result of OBH's wrongful conduct; and

j. Whether Plaintiffs and Class Members are entitled to restitution as a result of OBH's wrongful conduct.

189. **Typicality – CPLR § 901(a)(3).** Plaintiffs' claims are typical of the claims of the members of the Class. The claims of the Plaintiffs and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiffs and members of the Class were all patients of OBH, each having their PII and PHI exposed and/or accessed by an unauthorized third party.

190. **Adequacy of Representation – CPLR § 901(a)(4).** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other Class Members Plaintiffs seek to represent; Plaintiffs have retained counsel competent and experienced in complex class action litigation; Plaintiffs intend to prosecute this action vigorously; and Plaintiffs' counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiffs and Plaintiffs' counsel.

191. **Superiority – CPLR § 901(a)(5)**. A class action is superior to any other available method for adjudicating this controversy. The proposed Class is the surest way (i) to fairly and expeditiously compensate so large a number of injured persons that constitute the Class, (ii) to keep the courts from being inundated by dozens or hundreds of repetitive cases, and (iii) to reduce transactions costs so that the injured class members can obtain the most compensation possible. Accordingly, class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious wasteful litigation

FIRST CAUSE OF ACTION
NEGLIGENCE
(by Plaintiffs on behalf of themselves and the Class)

192. Plaintiffs incorporate by reference the preceding allegations as if fully set forth herein.

193. OBH owed a duty to Plaintiffs and Class Members to exercise reasonable care in safeguarding and protecting their PII and PHI in its possession, custody, and control.

194. OBH's duty to use reasonable care arose from several sources, including but not limited to those described below.

195. As discussed above, OBH had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of the OBH. By collecting and storing valuable PII and PHI that is routinely targeted by criminals for unauthorized access, OBH was obligated to act with reasonable care to protect against these foreseeable threats.

196. OBH's duty also arose from its position as a healthcare provider. OBH holds itself out as a trusted provider of healthcare, and thereby assumes a duty to reasonably protect its patients' information. Indeed, OBH was in a unique and superior position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

197. OBH breached the duties owed to Plaintiffs and Class Members and thus was negligent. As a result of a successful attack directed towards OBH that compromised Plaintiffs' and Class Members' PII and PHI, Defendant breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the

unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its patients; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII or PHI.

198. But for OBH's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their PII and PHI would not have been compromised.

199. As a direct and proximate result of OBH's negligence, Plaintiffs and Class Members have suffered injuries, including, but not limited to:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII and PHI;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent

charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

200. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(by Plaintiffs on behalf of themselves and the Class)

201. Plaintiffs incorporate by reference the preceding allegations as if fully set forth herein.

202. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as OBH for failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of Defendant's duty.

203. OBH violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored and the foreseeable consequences of a data breach involving PII and PHI of its patients.

204. Plaintiffs and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

205. OBH's violation of Section 5 of the FTC Act constitutes negligence *per se*.

206. OBH is an entity covered under HIPAA, which sets minimum federal standards for privacy and security of PHI.

207. Pursuant to HIPAA, 42 U.S.C. § 1302d, *et. seq.*, and its implementing regulations, Defendant had a duty to implement and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect Plaintiffs' and the Class Members' electronic PHI.

208. Specifically, HIPAA required OBH to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c)

protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by their workforce to satisfy HIPAA's security requirements. 45 C.F.R. § 164.102, *et. seq*.

209. OBH violated HIPAA by actively disclosing Plaintiffs' and the Class Members' electronic PHI and by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PHI.

210. Plaintiffs and the Class Members are patients within the class of persons HIPAA was intended to protect.

211. OBH's violation of HIPAA constitutes negligence *per se*.

212. OBH violated Part 2 by actively disclosing Plaintiffs' and the Class Members' electronic PHI to unknown cyber criminals.

213. Plaintiffs and the Class Members are patients within the class of persons Part 2 was intended to protect.

214. OBH's violation of Part 2 constitutes negligence *per se*.

215. The harm that has occurred as a result of OBH's conduct is the type of harm that the FTC Act, HIPAA, and Part 2 was intended to guard against.

216. As a direct and proximate result of OBH's negligence, Plaintiffs and Class Members have been injured as described herein and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
VIOLATION OF GENERAL BUSINESS LAW § 349
(by Plaintiffs on behalf of themselves and the Class)

217. Plaintiffs incorporate by reference the preceding allegations as if fully set forth herein.

218. Gen. Bus. Law § 349 prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state."

219. The acts of OBH described herein are consumer-oriented in that they are directed at members of the consuming public.

220. The misrepresentations and material omissions of OBH with respect to its privacy practices and failure to adequately safeguard the information entrusted to it violate the General Business Law.

221. The aforementioned acts are willful, unfair, unconscionable, deceptive, and contrary to the public policy of New York, which aims to protect consumers.

222. As a direct and proximate result of Defendant's unlawful deceptive acts and practices, Plaintiffs and the Class have suffered injury and monetary damages in an amount to be determined at the trial of this action. Plaintiffs do not seek to recover on their own behalf or on behalf of the members of the Class any penalties or minimum measures of recovery provided by Gen. Bus. Law § 349.

223. Plaintiffs and the other members of the Class further seek equitable relief against OPH.

FOURTH CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(by Plaintiffs on behalf of themselves and the Class)

224. Plaintiffs incorporate by reference the preceding allegations as if fully set forth herein.

225. Plaintiffs and Class Members have an interest, both equitable and legal, in the PII and PHI about them that was conveyed to, collected by, and maintained by OBH and that was ultimately accessed or compromised in the Data Breach.

226. As a healthcare provider, and recipient of patients' PII and PHI, OBH has a fiduciary relationship to its patients, including Plaintiffs and the Class Members.

227. Because of that fiduciary relationship, OBH was provided with and stored private and valuable PHI and PII related to Plaintiff and the Class. Plaintiffs and the Class were entitled to expect their information would remain confidential while in Defendant's possession.

228. OBH owed a fiduciary duty under common law to Plaintiffs and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

229. As a result of the parties' fiduciary relationship, OBH had an obligation to maintain the confidentiality of the information within Plaintiffs' and the Class Members' medical records.

230. OBH's patients, including Plaintiffs and Class Members, have a privacy interest in personal medical matters, and OBH had a fiduciary duty not to disclose medical data concerning its patients.

231. As a result of the parties' relationship, OBH had possession and knowledge of confidential PII and PHI of Plaintiffs and Class Members, information not generally known.

232. Plaintiffs and Class Members did not consent to nor authorize OBH to release or disclose their PII and PHI to unknown criminal actors.

233. OBH breached its fiduciary duties owed to Plaintiffs and Class Members by, among other things:

a. mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of

customer information that resulted in the unauthorized access and compromise of PII and PHI;

b. mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks;

c. failing to design and implement information safeguards to control these risks;

d. failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures;

e. failing to evaluate and adjust its information security program in light of the circumstances alleged herein;

f. failing to detect the breach at the time it began or within a reasonable time thereafter;

g. failing to follow its own privacy policies and practices published to its patients; and

h. failing to adequately train and supervise employees and third-party vendors with access or credentials to systems and databases containing sensitive PII or PHI.

234. But for OBH's wrongful breach of its fiduciary duties owed to Plaintiffs and Class Members, their PII and PHI would not have been compromised.

235. As a direct and proximate result of OBH's negligence, Plaintiffs and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII and PHI;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

236. As a direct and proximate result of OBH's breach of its fiduciary duties, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

FIFTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(by Plaintiffs on behalf of themselves and the Class)

237. Plaintiffs incorporate by reference the preceding allegations as if fully set forth herein.

238. When Plaintiffs and members of the Class provided their PII and PHI to OBH in exchange for healthcare services, they entered into implied contracts with Defendant, under which OBH agreed to take reasonable steps to protect Plaintiffs' and Class Members' PII and PHI, comply with it statutory and common law duties to protect Plaintiffs' and Class Members' PII and PHI, and to timely notify them in the event of a data breach.

239. OBH solicited and invited Plaintiffs and Class Members to provide their PII and PHI as part of Defendant's provision of healthcare services. Plaintiffs and Class Members accepted Defendant's offers and provided their PII and PHI to Defendant.

240. When entering into implied contracts, Plaintiffs and Class Members reasonably believed and expected that OBH's data security practices complied with its statutory and common law duties to adequately protect Plaintiffs' and Class Members' PII and PHI and to timely notify them in the event of a data breach.

241. OBH's implied promise to safeguard patient PII and PHI is evidence by, *e.g.*, the representations in Defendant's Notice of Privacy Practices set forth above.

242. Plaintiffs and Class Members paid money to Defendant in order to receive healthcare services. Plaintiffs and Class Members reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. OBH failed to do so.

243. Plaintiffs and Class Members would not have provided their PII and PHI to OBH had they known that Defendant would not safeguard their PII and PHI, as promised, or provide timely notice of a data breach.

244. Plaintiffs and Class Members fully performed their obligations under their implied contracts with OBH.

245. OBH breached its implied contracts with Plaintiffs and Class Members by failing to safeguard Plaintiffs' and Class Members' PII and PHI and by failing to provide them with timely notice of the Data Breach.

246. As a direct and proximate result of OBH's breach of contract, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SIXTH CAUSE OF ACTION
BREACH OF EXPRESS CONTRACT
(by Plaintiffs on behalf of themselves and the Class)

247. Plaintiffs incorporate by reference the preceding allegations as if fully set forth herein.

248. When Plaintiffs and members of the Class provided their PII and PHI to OBH in exchange for healthcare services, OBH expressly agreed, in its "Notice of Privacy Practices" and elsewhere, that it would take reasonable steps to protect Plaintiffs' and Class Members' PII and

PHI, comply with it statutory and common law duties to protect Plaintiffs' and Class Members' PII and PHI, and to timely notify them in the event of a data breach.

249. Plaintiffs and Class Members paid money to Defendant in order to receive healthcare services. Plaintiffs and Class Members reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. OBH failed to do so.

250. Plaintiffs and Class Members would not have provided their PII and PHI to OBH had they known that Defendant would not safeguard their PII and PHI, as promised, or provide timely notice of a data breach.

251. Plaintiffs and Class Members fully performed their obligations under their contracts with OBH.

252. OBH breached its express contractual obligations to Plaintiffs and Class Members by failing to safeguard Plaintiffs' and Class Members' PII and PHI and by failing to provide them with timely notice of the Data Breach.

253. As a direct and proximate result of OBH's breach of contract, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SEVENTH CAUSE OF ACTION
UNJUST ENRICHMENT
(by Plaintiffs on behalf of themselves and the Class)

254. Plaintiffs incorporate by reference the preceding allegations as if fully set forth herein.

255. Plaintiffs bring this claim individually and on behalf of the Class in the alternative to their contract-based claims.

256. Upon information and belief, OBH funds its data security measures from its general revenue, including payments made by or on behalf of Plaintiffs and the Class Members.

257. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

258. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased healthcare services from Defendant and/or its agents and in so doing provided Defendant with their PII and PHI. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and services that were the subject of the transaction and should have had their PII and PHI protected with adequate data security.

259. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII and PHI of Plaintiffs and Class Members for business purposes.

260. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII and PHI. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

261. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed

to implement appropriate data management and security measures that are mandated by its common law and statutory duties.

262. Defendant failed to secure Plaintiffs' and Class Members' PII and PHI and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

263. Defendant acquired the PII and PHI through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

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

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

266. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

EIGHTH CAUSE OF ACTION
VIOLATIONS OF THE NEW JERSEY CONSUMER FRAUD ACT
N.J. Stat. §§ 56:8-1 *et seq*. ("NJCFA")
(by Plaintiff Rogers on behalf of herself and the New Jersey Subclass)

267. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

268. This claim is brought by Plaintiff Jasmine Rogers individually and on behalf of the New Jersey Subclass.

269. The NJCFA states:

> The act, use or employment by any person of any commercial practice that is unconscionable or abusive, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any

> material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby, is declared to be an unlawful practice.

N.J. Stat. § 56:8-2.

270. Plaintiff Rogers, New Jersey Subclass members, and OBH are "persons" under the NJCFA. N.J. Stat. § 56:8-1(d).

271. The services that OBH provided are "merchandise" pursuant to the NJCFA. N.J. Stat. § 56:8-1(c).

272. OBH made uniform representations to Plaintiff Rogers and New Jersey Subclass members that their PII/PHI will remain private, as evidenced by, *inter alia*, its Privacy Policy. They committed deceptive omissions in violation of the NJCFA by failing to inform Plaintiff Rogers and Class members that they would not adequately secure Plaintiff Rogers' and New Jersey Subclass members' PII/PHI. Documents that should have contained such disclosures, but did not, include the privacy policies referenced in this Complaint.

273. OBH engaged in unfair acts and practices in violation of the NJCFA by failing to implement and maintain reasonable security measures to protect and secure Plaintiff Rogers' and New Jersey Subclass members' PII/PHI in a manner that complied with applicable laws, regulations, and industry standards. The failure to implement and maintain reasonable data security measures offends established public policy, is immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers.

274. Due to the Data Breach, Plaintiff Rogers and Class members have lost property in the form of their PII/PHI. Further, OBH's failure to adopt reasonable practices in protecting and

safeguarding their patients' PII/PHI will force Plaintiff Rogers and New Jersey Subclass members to spend time or money to protect against identity theft.

275. Plaintiff Rogers and New Jersey Subclass members are now at a substantially higher risk of medical identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for OBH's practice of collecting and storing PII/PHI without appropriate and reasonable safeguards to protect such information.

276. Plaintiff Rogers and all other New Jersey Subclass members were damaged by OBH's violation of the NJCFA because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) they lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) they overpaid for the services that were received without adequate data security.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, pray for relief as follows:

a. For an order certifying the Class defined above, appointing Plaintiffs as Class representatives, and designating their undersigned attorneys as Class Counsel;

b. For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiffs reasonable attorneys' fees, costs, and expenses;

g. Awarding Plaintiffs compensatory, statutory, punitive and treble damages to the extent permitted by law;

h. Awarding pre- and post-judgment interest on any amounts awarded; and

i. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a jury trial on all issues so triable.

Dated: December 15, 2023

Respectfully Submitted:

By: /s/ *Adam Pollock*

Adam Pollock
POLLOCK COHEN LLP
111 Broadway, Suite 1804
New York, NY 10006
(212) 337-5361
adam@pollockcohen.com

Jonathan Shub (NY Bar # 4747739)
Benjamin F. Johns (*pro hac vice*)
Samantha E. Holbrook (*pro hac vice*)
SHUB & JOHNS LLC
Four Tower Bridge
200 Barr Harbor Drive, Suite 400
Conshohocken, PA 19428
(610) 477-8380
jshub@shublawyers.com
bjohns@shublawyers.com
sholbrook@shublawyers.com

Ben Barnow
Anthony L. Parkhill (*pro hac vice pending*)
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Suite 1630
Chicago, IL 60606
(312) 621-2000
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com

Joseph M. Lyon (*pro hac vice pending*)
THE LYON FIRM
2754 Erie Avenue
Cincinnati, OH 45208
(513) 381-2333
jlyon@thelyonfirm.com

Brooke Murphy (*pro hac vice pending*)
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
(405) 389-4989
abm@murphylegalfirm.com

Brian C. Gudmundson (*pro hac vice forthcoming*)
Michael J. Laird (*pro hac vice forthcoming*)
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
(612) 341-0400
bgudmundson@zimmreed.com
michaellaird@zimmreed.com

Kenneth J. Grunfeld (*pro hac vice pending*)
KOPELOWITZ OSTROW FERGUSON WEISELBERG GILBERT
65 Overhill Road
Bala Cynwyd, Pennsylvania 19004
(215) 967-8799
grunfeld@kolawyers.com

Gary F. Lynch
Elizabeth Pollock-Avery (*pro hac vice pending*)

LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
(412) 322-9243
gary@lcllp.com
elizabeth@lcllp.com

Joseph P. Guglielmo
Ethan S. Binder
SCOTT+SCOTT ATTORNEYS AT LAW LLP
230 Park Avenue, 17th Floor
New York, NY 10169
Telephone: (212) 223-6444
jguglielmo@scott-scott.com
ebinder@scott-scott.com

John A. Yanchunis (*pro hac vice forthcoming*)
JYanchunis@forthepeople.com
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 North Franklin Street 7th Floor
Tampa, Florida 33602
(813) 223-5505

J. Burkett McInturff
WITTELS MCINTURFF PALIKOVIC
305 Broadway, 7th Floor
New York, NY 10007
(910) 476-7253
jbm@wittelslaw.com

Counsel for Plaintiffs

ClassAction.org