UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

CHRISTOPHER CICCOZZI, individually and on behalf of all others similarly situated, Plaintiff, v. GATEWAY REHABILITATION CENTER, d/b/a GATEWAY REHAB, Defendant.	Case No. 2:22-cv-1797 **Jury Trial Demanded**

CLASS ACTION COMPLAINT

Plaintiff Christopher Ciccozzi ("Plaintiff"), by and through his attorneys of record, upon personal knowledge as to his own acts and experiences, and upon information and belief as to all other matters, files this complaint against Defendant Gateway Rehabilitation Center d/b/a Gateway Rehab ("Defendant" or "Gateway Rehab") and alleges the following:

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard the private and sensitive information it collected, maintained, stored, analyzed, and used to provide its services. This information includes, but is not limited to, personally identifiable information ("PII") and protected health information ("PHI"), including one or more of the following: name, Social Security number, and records regarding patient care (collectively, "Sensitive Information") of approximately 130,000 individuals.[1]

[1] Exhibit 1, ("Website Notice of Privacy Incident"), available at https://storage.googleapis.com/treatspace-prod-media/pracf/u-2548/Gateway_Rehab_-_Substitute_Notice_-_For_Web_Only.pdf (last accessed Dec. 12, 2022). *See also* U.S. DHHS

2. Defendant Gateway Rehab provides medical services including inpatient and outpatient drug rehab care, extended care, medically monitored withdrawal management, substance abuse support and family programs, adolescent programs, medications for substance abuse disorder, telehealth, and community-based recover specialists.[2] Gateway Rehab has been operating for over 50 years and serves roughly thousands of patients per year at 13 different locations in Western Pennsylvania and Eastern Ohio.[3]

3. To obtain medical treatment and related services, Plaintiff and other patients of Defendant entrust and provide to Defendant an extensive amount of highly sensitive and privileged PII/PHI. Defendant retains this information–even long after the treatment relationship ends. Defendants acknowledge the importance of the protected information.[4]

4. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and members of the proposed Class's PII/PHI, Defendant assumed legal and equitable duties to those individuals.

5. Plaintiff and members of the proposed Class are victims of Defendant's negligent and/or careless acts and omissions and the failure to protect PII and PHI of Defendant's current and former patients.

6. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their PII and PHI. But Defendant betrayed that trust. Defendant failed to use reasonable, up-to-

---

OFFICE FOR CIVIL RIGHTS, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Dec. 12, 2022).

[2] *Services*, Gateway Rehab (last accessed Dec. 12, 2022) available at https://www.gatewayrehab.org/

[3] *Locations,* Gateway Rehab (last accessed Dec. 12, 2022) available at https://www.gatewayrehab.org/

[4] Exhibit 2, ("Notice of Privacy Practices") available at https://www.gatewayrehab.org/resources/about/policies#privacy (last accessed Dec. 12, 2022).

date security practices and protocols to prevent the Data Breach that occurred. Defendant further failed to provide an adequate and accurate notice to Plaintiff and members of the proposed Class.

7. On information and belief, Defendant first became aware of the Breach on June 13, 2022, after the unauthorized party accessed Plaintiff's and Class Members' Sensitive Information from Defendant's systems.[5] Defendant began notifying victims about the Data Breach November 18, 2022.[6]

8. When Defendant announced the Data Breach, it deliberately underplayed the Breach's severity and obfuscated the nature of the Breach. Defendant's notice sent to impacted individuals fails to explain how the breach happened, how many people were impacted, and why the unauthorized party had unfettered access to Plaintiff's and the Class's Sensitive Information.[7]

9. Plaintiff and members of the proposed Class are victims of Defendant's negligent and/or careless acts and omissions and the failure to protect PII and PHI of Plaintiff and members of the Class.

10. On information and belief, cybercriminals were able to breach Defendant's systems because Defendant did not maintain reasonable, up-to-date security practices and protocols to prevent the Data Breach that occurred. Defendant admitted as much in its Notice, stating, "Gateway Rehab takes the security and privacy of patient information very seriously and has taken steps to prevent a similar event from occurring in the future."[8]

11. Prior to notification of the breach, Plaintiff and members of the proposed Class had no idea their PII and PHI had been compromised, and that they were, and continue to be, at

[5] Ex. 1.

[6] Exhibit 3, (Christopher Ciccozzi Notice Letter)

[7] *Id.*

[8] *Id.*

significant risk of identity theft and various other forms of personal, social, and financial harm. This risk will carry on for the duration of their lifetimes.

12. Defendant's failure to timely detect and adequately notify breach victims violates state and federal law and has made Plaintiff and members of the Class (defined *infra*) vulnerable to a present and continuing risk of fraud and identity theft.

13. For example, armed with Sensitive Information acquired in the Data Breach, data thieves are able to commit numerous crimes including opening new financial accounts in members of the proposed Class's names, using members of the proposed Class's names to obtain government benefits, filing fraudulent tax returns, obtaining driver's licenses in members of the proposed Class's names but with another person's photograph, giving false information to police during an arrest, taking out loans in members of the proposed Class's names, and using members of the proposed Class's names to obtain medical services. Accordingly, Plaintiff and members of the proposed Class must now and for the foreseeable future closely monitor their financial and other accounts to guard against identity theft and related harm.

14. As a result of Defendant's conduct, Plaintiff and the Class have and will be required to continue to undertake and incur out-of-pocket, expensive, and time-consuming efforts to mitigate the actual and potential impact of the Data Breach on their lives by, among other things, placing freezes and alerts with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, changing passwords on medical portals, and requesting and maintaining accurate medical records outside of those kept by medical providers.

15. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard the private and sensitive information it collected, maintained, stored, analyzed, and used in its ordinary course of business.

16. Plaintiff and the members of the proposed Class therefore bring this lawsuit seeking remedies including damages, reimbursement of out-of-pocket-costs, and equitable and injunctive relief, including improvements to Defendant's data security systems, future annual audits, and identity protection services funded by Defendant.

PARTIES

17. Plaintiff Christopher Ciccozzi is a resident and citizen of Pennsylvania. Mr. Ciccozzi received a notice informing his that his Sensitive Information was compromised in the Gateway Rehab Data Breach.

18. Defendant Gateway Rehabilitation Center, d/b/a Gateway Rehab, is a Pennsylvania nonprofit corporation and healthcare provider with its principal place of business located at 100 Moffett Run Road, Aliquippa, Pennsylvania 15001 and its principal office address located at 311 Rouser Road, Moon Township, Pennsylvania, 15108.

19. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

20. The Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's Pennsylvania citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs. Thus, minimal diversity exists under 28 U.S.C 1332(d)(2)(A).

21. The Court has personal jurisdiction over Defendant because Defendant's primary place of business is located within this District and Defendant conducts substantial business in this District.

22. Venue is proper in this district under 28 U.S.C. § 1391(b)(1) because Defendant resides in this District pursuant to 28 U.S.C. § 1391(c)(2). In addition, venue is proper in this District because a substantial part of the events giving rise to the cause of action occurred in this District. *Id.* at § 1391(b)(2).

FACTUAL BACKGROUND

A. Gateway Rehab and its Practices

23. Gateway Rehab provides medical services including inpatient and outpatient drug rehab care, extended care, medically monitored withdrawal management, substance abuse support and family programs, adolescent programs, medications for substance abuse disorder, telehealth, and community-based recover specialists.[9] Gateway Rehab has been operating for over 50 years and serves roughly thousands of patients per year at 13 different locations in Western Pennsylvania and Eastern Ohio.[10]

24. To obtain healthcare and related services, patients, like Plaintiff and the Class, must provide Defendant with highly sensitive information, including PHI, PII, or both. Defendant compiles, stores, and maintains the highly sensitive PII and PHI. Defendant serves thousands of individuals per year indicating it has created and maintains a massive repository of Sensitive

[9] *Services*, Gateway Rehab (last accessed Dec. 12, 2022) available at https://www.gatewayrehab.org/

[10] *Locations,* Gateway Rehab (last accessed Dec. 12, 2022) available at https://www.gatewayrehab.org/

Information, acting as a particularly lucrative target for data thieves looking to obtain and misuse or sell patient data.[11]

25. Defendant posts a "Notice of Privacy Practices" on its website.[12] In it, Defendant claims that Gateway Rehab is fully committed to the protection of its patients' health information.[13] The Privacy Policy lists a number of permissible and expected uses of Plaintiff's and the Class's Sensitive Information, none of which is contemplated by the Data Breach here.

26. Plaintiff and the Class had a reasonable expectation that Defendant would protect the Sensitive Information provided to and created by it, especially because, given the publicity of other data breaches and the significant impact they had, Defendant knew or should have known that failing to adequately protect patient information could cause substantial harm. Moreover, through its Notice of Privacy Practices, Defendant acknowledged its obligation to reasonably safeguard sensitive information against security breaches and other types of theft and misuse.

27. As described throughout this Complaint, Defendant did not reasonably protect, secure, or store Plaintiff's and the Class's Sensitive Information prior to, during, or after the Data Breach, but rather, enacted unreasonable data security measures that it knew or should have known were insufficient to reasonably protect the highly sensitive information Defendant maintained. Consequently, cybercriminals circumvented Defendant's security measures, resulting in a significant data breach.

[11] *Id.*

[12] Ex. 2.

[13] *Id.*

B. The Data Breach and Notice Letter

28. On an undisclosed date prior to June 13, 2022, one or more malicious actors gained access to Defendant's computer network and systems.[14] The actor(s) had access to Defendant's computer network and systems from for an undisclosed amount of time.[15] (the "Data Breach").

29. On or around June 13, 2022, Defendant became aware of the Data Breach because some of its computer systems were shut down for a period of time.[16] In response, Defendant launched an investigation, which concluded on or about September 21, 2022.[17]

30. The investigation found the Data Breach resulted in the malicious actor(s) accessing, copying, and/or exfiltrating substantial amounts of patient PII and PHI.[18] (collectively "Sensitive Information) Specifically, the malicious actor(s) took files containing name, date of birth, Social Security number, driver's license or state ID number, financial account and/or payment card number, medical information and health insurance information.[19]

31. On or about November 18, 2022, Defendant ultimately admitted to the Data Breach and began notifying the 130,000 individuals, including Plaintiff and members of the proposed Class.[20] On or about the same day, Defendant publicly acknowledged the data security incident to the United States Department of Health and Human Services' Office for Civil Rights ("DHHS").[21] In its Notice, Defendant admitted that:

---

[14] Ex. 1.

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] *Id.*

[21] U.S. DHHS OFFICE FOR CIVIL RIGHTS, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Nov. 10, 2022).

> On June 13, 2022, Gateway Rehab discovered that it had experienced an incident disrupting access to certain of its systems. Gateway Rehab took immediate steps to secure these systems and promptly launched an investigation. Gateway Rehab engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization as a result. As a result of that investigation, Gateway Rehab confirmed on July 8, 2022 that data potentially containing personal and/or protected health information may have been impacted, and began a comprehensive review process to discern the exact nature of the information and the individuals involved. That review concluded on September 21, 2022 and confirmed that certain personal and/or protected health information of Gateway Rehab current and former patients may have been in the data that was compromised.
>
> The following information may have been involved in the incident: name, date of birth, Social Security number, driver's license or state ID number, financial account and/or payment card number, medical information and health insurance information.

32. Defendant identified only the following actions it undertook to mitigate and remediate the harm caused by the Data Breach in its Notice Letter:

> Gateway Rehab takes the security and privacy of patient information very seriously and has taken steps to prevent a similar event from occurring in the future.

33. Defendant recognized the substantial and high likelihood that Plaintiff and the proposed Class's PII would be misused following the Data Breach, instructing:

> The privacy and protection of personal information is a top priority for Gateway Rehab and we deeply regret any inconvenience this incident may cause.

34. Given that Defendant was storing the PII and PHI of Plaintiff and the Class and knew or should have known of the serious risk and harm caused by a data breach, Defendant was obligated to implement reasonable measures to prevent and detect cyber-attacks, such as those

recommended by the Federal Trade Commission, required by the Health Insurance Portability and Accountability Act, and promoted by data security experts and other agencies.

35. That obligation stems from the foreseeable risk of a Data Breach given that Defendant collected, stored, and had access to a swath of highly sensitive patient records and data and, additionally, because other highly publicized data breaches at different healthcare institutions and providers put Defendant on notice that the higher personal data it stored might be targeted by cybercriminals.

36. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry and the prevalence of health care data breaches, Defendant inexplicably failed to adopt sufficient data security processes.

37. Clearly, the Data Breach at issue here was the inevitable result of Defendant's inadequate approach and/or attention to data security protection of the Sensitive Information it collects, analyzes, and uses in its ordinary course of business.

38. The Data Breach itself, and the information Defendant has disclosed about the breach to date, including its length, the need to remediate Defendant's cybersecurity, the number of people impacted, and the sensitive nature of the impacted data collectively demonstrate Defendant failed to implement reasonable measures to prevent cyber-attacks and the exposure of the Sensitive Information they oversaw.

C. The Data Breach Was Foreseeable Because the Healthcare Industry is Particularly Susceptible to Cyber Attacks.

39. Data breaches have become alarmingly commonplace in the U.S. In 2021, data breaches increased by nearly 70% over the previous year, which is over 20% higher than the previous all-time high.[22]

40. The healthcare sector was the easiest "mark" among all major sectors last year, meaning it had the highest number of data compromises and categorically had some of the most widespread exposure per data breach.[23] According to the 2021 Healthcare Information and Management Systems Society Cybersecurity Survey, 67% of participating hospitals reported having a significant security incident within the last twelve months, with a majority of those being caused by "bad actors."[24]

41. Healthcare providers and vendors that maintain health care provider data "have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers.[25]

---

[22] *2021 Annual Data Breach Year-End Review*, ITRC, (Jan. 2022), https://www.idtheftcenter.org/publication/2021-annual-data-breach-report-2/

[23] *Id.*

[24] *2021 HIMSS Cybersecurity Survey*, Healthcare Information and Management Systems Society, Inc., accessible at: https://www.himss.org/resources/himss-healthcare-cybersecurity-survey (last accessed Mar. 16, 2022).

[25] Benishti, Eyal, *How to Safeguard Hospital Data from Email Spoofing Attacks*, INSIDE DIGITAL HEALTH (Apr. 4, 2019), https://www.idigitalhealth.com/news/how-to-safeguard-hospitaldata-from-email-spoofing-attacks.

42. A 2010 report focusing on healthcare data breaches found the "average total cost to resolve an identity theft related incident … came to about $20,000."[26] According to survey results and population extrapolations from the National Study on Medical Identity Theft report from the Ponemon Institute, nearly 50% of victims reported losing their healthcare coverage because of a data breach and nearly 30% reported an increase in their insurance premiums.[27] Several individuals were unable to fully resolve their identity theft crises. Healthcare data breaches are an epidemic and they are crippling the impacted individuals—millions of victims every year.[28]

43. According to an analysis of data breach incidents reported to the U.S. Department of Health and Human Services and the media, from 2015 and 2019, the number of healthcare related security incidents increased from 450 annual incidents to 572 annual incidents, likely a conservative estimate.[29]

44. According to the Verizon Data Breach Investigations Report, the health care industry, including hospitals and other providers, experienced 655 known data breaches, 472 of which had confirmed data disclosures in 2021.[30] For the tenth year in a row, the healthcare industry has seen the highest impact from cyber-attacks of any industry.[31]

---

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

[27] *Id.*

[28] *Id.*

[29] Heather Landi, *Number of patient records breached nearly triples in 2019*, FIERCE HEALTHCARE (Feb. 20, 2020), https://www.fiercehealthcare.com/tech/number-patient-records-breached-2019-almost-tripled-from-2018-as-healthcare-faces-new-threats#:~:text=OVer%2041%20million%20patient%20records,close%20to%2021%20million%20records (last visited Jan.19, 2022).

[30] Verizon, 2021 Data Breach Investigations Report: Healthcare NAICS 62 (2021) (last visited Jan. 19, 2021), https://www.verizon.com/business/resources/reports/dbir/2021/data-breach-statistics-by-industry/healthcare-data-breaches-security/.

[31] *Five worthy reads: The never-ending love story between cyberattacks and healthcare,* ManageEngine, https://blogs.manageengine.com/corporate/manageengine/2021/08/06/the-never-

45. As a healthcare provider with several thousands of current and former patients, if not more, Defendant knew or should have known the importance of protecting the Sensitive Information entrusted to it. Defendant also knew or should have known of the foreseeable, and catastrophic consequences if its systems were breached. These consequences include substantial costs to Plaintiff and the Class because of the Data Breach. Despite this, Defendant failed to take reasonable data security measures to prevent or mitigate losses from cyberattacks.

D. Plaintiff's and the Class's PII and PHI are Valuable.

46. The Federal Trade Commission ("FTC") has recognized that consumer data is a lucrative (and valuable) form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour underscored this point by reiterating that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[32]

47. Unlike financial information, such as credit card and bank account numbers, the PHI and certain PII exfiltrated in the Data Breach cannot be easily changed. Dates of birth and social security numbers are given at birth and attach to a person for the duration of his or his life. Medical histories are inflexible. For these reasons, these types of information are the most lucrative and valuable to hackers.[33]

---

ending-love-story-between-cyberattacks-and-healthcare.html#:~:text=According%20to%20Infosec%20Institute%2C%20credit,is%20%24158%20per%20stolen%20record.

[32] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009) (last visited Jan. 18, 2022) http://www/ftc/gov/speeches/harbour/091207privacyroundtable.pdf.

[33] *Calculating the Value of a Data Breach – What Are the Most Valuable Files to a Hacker?* Donnellon McCarthy Enters, https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/ (last visited Jan. 18, 2022).

48. Birth dates, Social Security numbers, addresses, employment information, income, and similar types of information can be used to open several credit accounts on an ongoing basis rather than exploiting just one account until it's canceled.[34] For that reason, Cybercriminals on the dark web are able to sell Social Security numbers for large profits. For example, an infant's social security number sells for as much as $300 per number.[35] Those numbers are often then used for fraudulent tax returns.[36]

49. Consumers place a considerable value on their Sensitive Information and the privacy of that information. One 2002 study determined that U.S. consumers highly value a website's protection against improper access to their Sensitive Information, between $11.33 and $16.58 per website. The study further concluded that to U.S. consumers, the collective "protection against error, improper access, and secondary use of personal information is worth between $30.49 and $44.62.[37] This data is approximately twenty years old, and the dollar amounts would likely be exponentially higher today.

50. Defendant's Data Breach exposed a variety of Sensitive Information, including Social Security numbers and PHI.

51. The Social Security Administration ("SSA") warns that a stolen Social Security number can lead to identity theft and fraud: "Identity thieves can use your number and your credit

[34] Tim Greene, *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Jan. 18, 2022).

[35] *Id.*

[36] *Id.*

[37] 11-Horn Hann, Kai-Lung Hui, *et al*, *The Value of Online Information Privacy: Evidence from the USA and Singapore,* at 17. Marshall Sch. Bus., Univ. So. Cal. (Oct. 2002), https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited Jan. 19, 2022).

to apply for more credit in your name."[38] If the identity thief applies for credit and does not pay the bill, it will damage victims' credit and cause a series of other related problems.

52. Social Security numbers are not easily replaced. In fact, to obtain a new number, a person must prove that he or she continues to be disadvantaged by the misuse—meaning an individual must prove actual damage has been done and will continue in the future.

53. PHI, also at issue here, is likely even more valuable than Social Security numbers and just as capable of being misused. The Federal Bureau of Investigation ("FBI") has found instances of PHI selling for fifty times the price of stolen Social Security numbers or credit card numbers.[39]

54. Other reports found that PHI is ten times more valuable on the black market than credit card information.[40] This is because one's personal health history, including prior illness, surgeries, diagnoses, mental health, and the like cannot be changed or replaced, unlike credit card information and even, under difficult circumstances, social security numbers. Credit card information and PII sell for $1-2 on the black market, but PHI can sell for as much as $363 according to the Infosec Institute.[41]

55. Cybercriminals recognize and exploit the value of PHI and PII. The value of PHI and PII is the foundation to the cyberhacker business model.

---

[38] Social Security Administration, *Identity Theft and Your Social Security Number*, (last visited Jan. 19, 2022), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[39] *FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI (April 8, 2014), https://publicintelligence.net/fbi-healthcare-cyber-intrusions/ (last visited Jan. 18, 2022).

[40] Tim Greene, *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Jan. 18, 2022).

[41] *Hackers Selling Healthcare Data in the Black Market*, INFOSEC, https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Jan. 18, 2022).

56. Because the Sensitive Information exposed in the Defendant's Data Breach is permanent data, there may be a gap of time between when it was stolen and when it will be used. The damage may continue for years. Plaintiff and the Class now face years of monitoring their financial and personal records with a high degree of scrutiny. The Class has incurred and will incur this damage in addition to any fraudulent use of their Sensitive Information.

E. Exposure of Sensitive Information Creates a Substantial Risk of Harm

57. The ramifications of Defendants failure to keep Plaintiff's and the Class's PII and PHI secure are severe.

58. The personal and health information of Plaintiff and the Class is valuable and has become a highly desirable commodity to data thieves. The FBI's Internet Crime Complaint (IC3) 2019 estimated there was more than $3.5 billion in losses to individual and business victims due to identity fraud in that year alone. Accordingly, Defendant's failure to reasonably safeguard Plaintiff's and the Class's sensitive PHI and PII has created a serious risk to Plaintiff and the Class, including both a short-term and long-term risk of identity theft.[42]

59. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[43] This is because stolen Sensitive Information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines and is frequented by criminals, fraudsters, and other wrongdoers. Law enforcement has difficulty policing the "dark web," which allows users and criminals to conceal identities and

[42] The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority. 17 C.F.R. § 248.201 (2013).

[43] *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims,* ThreatPost.com (last visited Jan. 17, 2022), https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/

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

60. Purchasers of Sensitive Information use it to gain access to the victim's bank accounts, social media, credit cards, and tax details. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts. This can result in the discovery and release of additional Sensitive Information from the victim, as well as Sensitive Information from family, friends, and colleagues of the original victim.

61. In addition, cyber-criminals can cross-reference two sources of PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages. The development of "Fullz" packages means that stolen PHI from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

62. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the

damage caused by the theft of their PHI. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

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

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

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

b. The diminution in value of their PHI;

c. The compromise and continuing publication of their PHI;

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

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

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PHI; and

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

F. Defendant failed to sufficiently protect the PII and PHI that patients entrusted to it

(i). Defendant failed to adhere to HIPAA

65. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information same. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[44]

66. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII is properly maintained.[45]

67. Defendant's Data Breach resulted from a combination of inadequacies showing it failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

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

[44] HIPAA lists eighteen types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, inter alia: names, addresses, any dates including dates of birth, social security numbers, and medical record numbers.

[45] *See* 45 C.F.R. § 164.306 (Security standards and General rules); 45 C.F.R. § 164.308 (Administrative safeguards); 45 C.F.R. § 164.310 (Physical safeguards); 45 C.F.R. § 164.312 (Technical safeguards).

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

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

d. Failing to ensure compliance with HIPAA security standards by Defendant's workforce, in violation of 45 C.F.R. § 164.306(a)(4);

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

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

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

h. Failing to effectively train all staff members on the policies and procedures with respect to PII as necessary and appropriate for staff members to carry out their functions and to maintain security of PII, in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

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

(ii). Defendant failed to adhere to FTC guidelines

68. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.[46] To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

69. In 2016, the FTC updated its publication Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business.[47] The guidelines explain that businesses should:

a. Protect the personal customer information that they keep;

b. Properly dispose of personal information that is no longer needed;

c. Encrypt information stored on computer networks;

d. Understand their network's vulnerabilities; and

e. Implement policies to correct security problems.

70. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

71. The FTC recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used

[46] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (Sep. 2, 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[47] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Sep. 28, 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting personalinformation.pdf.

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.[48]

72. 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 Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

73. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

(iii). Defendant failed to adhere to industry standards

74. As stated above, the healthcare industry continues to be a high value target among cybercriminals. In 2021, the U.S. healthcare sector experienced over 330 data breaches, a number which is likely to continue to grow.[49] The costs of healthcare data breaches per record are among the highest across all industries and are well over the global average per record.[50] As a result, both the government and private sector have developed industry best standards to address this growing problem.

[48] *See Start with Security*, *supra* note 46.

[49] *2021 Annual Data Breach Year-End Review*, ITRC, (Jan. 2022), https://www.idtheftcenter.org/publication/2021-annual-data-breach-report-2/

[50] *Id.*

75. The United States Department of Health and Human Services' Office for Civil Rights ("DHHS") notes that, "[w]hile all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations as they store large quantities of highly sensitive and valuable data."[51] DHHS highlights "several basic cybersecurity safeguards that can be implemented to improve cyber resilience which only require a relatively small financial investment, yet they can have a major impact on an organization's cybersecurity posture."[52] Most notably, organizations must properly encrypt PII to mitigate against misuse.

76. The private sector has similarly identified the healthcare sector as particularly vulnerable to cyberattacks both because of the of value of the PII that it maintains and because, as an industry, it has been slow to adapt and respond to cybersecurity threats.[53]

77. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, Defendant failed to adopt sufficient data security processes, a fact highlighted in its notification to affected patients in which it revealed that only after the Data Breach, Defendant has taken steps to increase the security of its systems.[54]

78. Moreover, Defendant failed to properly implement, maintain, and safeguard its computer systems, networks, and data including (but not limited to):

---

[51] *Cybersecurity Best Practices for Healthcare Organizations*, HIPAA JOURNAL (Nov. 1, 2018), https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/ (last accessed Mar. 16, 2022).

[52] *Id.*

[53] *10 Cyber Security Best Practices For the Healthcare Industry*, NTIVA (Jun. 19, 2018), https://www.ntiva.com/blog/10-cybersecurity-best-practices-for-the-healthcare-industry.

[54] Ex. 1.

a. Failing to maintain an adequate data security system to reduce the risks of data breaches and cyber-attacks;

b. Failing to properly monitor its own data security systems for existing intrusion, brute force attempts, and clearing of logs;

c. Failing to apply all available security updates; and

d. Failing to install the latest software patches, updates its firewalls, check user account privileges; or ensure proper security practices.

79. Defendant's failure to implement these rudimentary measures made it an easy target for the Data Breach.

80. Despite Defendant's failure to reasonably protect Plaintiff's and the Class's Sensitive Information, they have not offered any compensation or adequate remedy considering the significant and long-term risks Plaintiff and the Class face. Defendant has merely offered 12 months of identity protection services.[55]

G. Defendant's Delay in Identifying and Reporting the Breach Caused Additional Harm

81. It is axiomatic that:

> The quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act.[56]

82. Indeed, once a data breach has occurred:

> [o]ne thing that does matter is hearing about a data breach quickly. That alerts consumers to keep a tight watch on credit card bills, insurance invoices, and

[55] Ex. 3.

[56] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study,* BUSINESS WIRE, https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million (last accessed Mar. 21, 2022).

> suspicious emails. It can prompt them to change passwords and freeze credit reports. And notifying officials can help them to catch cybercriminals and warn other businesses of emerging dangers. If consumers don't know about a breach because it wasn't reported, they can't take action to protect themselves (internal citations omitted). [57]

83. Additionally, pursuant to 45 CFR § 164.404, Gateway Rehab was required to provide notice to Plaintiff and members of the proposed class no later than 60 days after discovering the breach.

84. Although their Sensitive Information was improperly exposed, viewed, exfiltrated and/or stolen at least on June 13, 2022, and Gateway Rehab confirmed as much on July 8, 2022, affected persons were not notified of the Data Breach until, at the earliest, November 18, 2022, depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

85. As a result of Gateway Rehab's delay in detecting and notifying client's and/or Plaintiff and members of the proposed Class of the Data Breach, Plaintiff and members of the proposed Class's risk of fraud has been driven even higher.

PLAINTIFF'S EXPERIENCES

86. Christopher Ciccozzi is a resident and citizen of Pennsylvania. He is a former patient of Gateway Rehab.

87. As a condition of receiving healthcare related services, Gateway Rehab required Christopher Ciccozzi to provide Gateway Rehab with his PII and PHI. Accordingly, Christopher Ciccozzi provided Gateway Rehab with his PII and PHI in order to purchase and receive healthcare

[57] *The Data Breach Next Door Security breaches don't just hit giants like Equifax and Marriott. Breaches at small companies put consumers at risk, too,* CONSUMER REPORTS (January 31, 2019), https://www.consumerreports.org/data-theft/the-data-breach-next-door/ (last accessed Mar. 21, 2022).

and related services. Plaintiff believed his PII and PHI provided to Gateway Rehab for healthcare and related services would be protected by Gateway Rehab.

88. On or about late-November of 2022, Christopher Ciccozzi received notice from Gateway Rehab, which informed him of the Data Breach and that he faced a substantial and significant risk of his PII and PHI being misused.

89. Subsequent to and as a direct and proximate result of the Data Breach, Mr. Ciccozzi Has experienced a substantial number of spam emails and phone calls regarding outstanding bills on large purchases, which Plaintiff believes is related to his private information being placed in the hands of an illicit actor as a result of the Data Breach. As a result, Plaintiff has and continues to mitigate against any potential identity theft and fraud by, among other things, changing his passwords, monitoring his accounts, requesting new credit cards, monitoring debit and credit card purchases, etc.

90. Plaintiff Ciccozzi is very careful about sharing his sensitive PII and PHI. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Furthermore, Plaintiff Ciccozzi stores any documents containing his sensitive information in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts. Finally, Plaintiff Ciccozzi has never previously had his identity stolen.

91. Plaintiff Ciccozzi suffered actual injury from having his sensitive information exposed and/or stolen as a result of the Data Breach including, but not limited to: (a) continuous imminent and impending injury arising from the increased risk of financial, medical, and identity fraud and theft; (b) entrusting PII and PHI to Gateway Rehab that he would not have had Gateway Rehab disclosed it lacked data security practices adequate to safeguard its patients; (c) damages to

and diminution in the value of his Sensitive Information–a form of intangible property that he entrusted to Gateway Rehab as a condition of receiving healthcare services; (d) loss of his privacy; (e) continuous imminent and impending injury arising from the increased risk of financial, medical, and identity fraud and theft; and (e) time and expense of his mitigation efforts as a result of the data breach.

92. In addition, knowing that hackers accessed and/or stole his PII and PHI and that this will likely be used in the future for identity theft, fraud, and related purposes has caused Mr. Ciccozzi to experience feelings of rage, anger, anxiety, sleep disruption, stress, fear, and physical pain. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

CLASS ALLEGATIONS

93. Pursuant to Federal Rules of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4), Plaintiff brings this action on behalf of himself and on behalf of all members of the proposed Class defined as:

> **Nationwide Class**: All persons residing in the United States Who received notice or were otherwise sent notice that they were impacted by Defendant's Data Breach.
>
> **Pennsylvania Subclass**: All persons residing in Pennsylvania who received notice or were otherwise sent notice that they were impacted by Defendant's Data Breach.

94. The following people are excluded from the Classes: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or its parents have a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose

claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

Plaintiff and members of the Classes satisfy the numerosity, commonality, typicality, adequacy, and predominance prerequisites for suing as representative parties pursuant to Federal Rule of Civil Procedure 23.

Numerosity, Fed. R. Civ. P. 23(a)(1): The exact number of members of the Classes are unknown but, upon information and belief, they are estimated to number in the tens or hundreds of thousands at this time, and individual joinder in this case is impracticable. Members of the Classes can be easily identified through Defendant's records and objective criteria permitting self-identification in response to notice, and notice can be provided through techniques similar to those customarily used in other data breach, consumer breach of contract, unlawful trade practices, and class action controversies.

Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of the claims of other members of the Classes in that Plaintiff, and the members of the Classes sustained damages arising out of Defendant's Data Breach, wrongful conduct and misrepresentations, false statements, concealment, and unlawful practices, and Plaintiff and members of the Classes sustained similar injuries and damages, as a result of Defendant's uniform illegal conduct.

Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Classes and has retained counsel competent and experienced in complex class actions to vigorously prosecute this action on behalf of the Classes. Plaintiff has no interests that conflict with, or are antagonistic to those of, the Classes, and Defendant has no defenses unique to Plaintiff.

Commonality and Predominance, Fed. R. Civ. P. 23(a)(2) and (b)(3): There are many questions of law and fact common to the claims of Plaintiff and the Classes, and those questions predominate over any questions that may affect individual members of the Classes. Common questions for the Classes include, but are not necessarily limited to the following:

a. Whether Defendant violated the laws asserted herein;

b. Whether Defendant had a duty to use reasonable care to safeguard Plaintiff's and members of the Classes' PII and PHI;

c. Whether Defendant breached the duty to use reasonable care to safeguard members of the Classes' PII and PHI;

d. Whether Defendant knew or should have known about the inadequacies of their data security policies and system and the dangers associated with storing sensitive PII and PHI;

e. Whether Defendant failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiff's and members of the Classes' PII and PHI from unauthorized release and disclosure;

f. Whether Defendant breached its contractual promises to safeguard Plaintiffs' and members of the Class's PII and PHI;

g. Whether the proper data security measures, policies, procedures, and protocols were in place and operational within Defendant's computer systems to safeguard and protect Plaintiff's and members of the Classes' PII and PHI from unauthorized release and disclosure;

h. Whether Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;

i. Whether Defendant's delay in informing Plaintiff and members of the Classes of the Data Breach was unreasonable;

j. Whether Defendant's method of informing Plaintiff and other members of the Classes of the Data Breach was unreasonable;

k. Whether Defendant is liable for negligence or gross negligence;

l. Whether Defendant's conduct, practices, statements, and representations about the Data Breach of the PII and PHI violated applicable state laws;

m. Whether Plaintiff and members of the Classes were injured as a proximate cause or result of the Data Breach;

n. What the proper measure of damages is; and

o. Whether Plaintiff and members of the Class are entitled to restitutionary, injunctive, declaratory, or other relief.

Superiority, Fed. R. Civ. P. 23(b)(3): This cause is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by the individual members of the Classes will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual members of the Classes to obtain effective relief from Defendant's misconduct. Even if members of the Classes could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and

comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered, and uniformity of decisions ensured.

A class action is therefore superior to induvial litigation because:

a. The amount of damages available to an individual Plaintiff is insufficient to make litigation addressing Defendant's conduct economically feasible in the absence of the class action procedural device;

b. Individualized litigation would present a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system; and

c. The class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

CLAIMS

COUNT I
Negligence
(On behalf of Plaintiff and the Nationwide Class or, Alternatively, the Pennsylvania Subclass)

95. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

96. Defendant collected, created, and maintained Plaintiff's and the Class's Sensitive Information for the purpose of providing medical or related services to Plaintiff and the Class.

97. Plaintiff and the Class are a well-defined, foreseeable, and probable group of patients that Defendant was aware, or should have been aware, could be injured by inadequate data security measures. The nature of Defendant's business requires patients to disclose Sensitive Information to receive adequate care, including, but not limited to, medical histories, dates of birth,

addresses, phone numbers, and medical insurance information. Thus, for Defendant to provide its services, it must use, handle, gather, and store the Sensitive Information of Plaintiff and the Class and, additionally, solicit and create records containing Plaintiff's and the Class's Sensitive Information.

98. A large depository of highly valuable health care information is a foreseeable target for cybercriminals looking to steal and profit from that sensitive information. Defendant knew or should have known that, given its repository of a host of Sensitive Information for hundreds of thousands of patients posed a significant risk of being targeted for a data breach. Thus, Defendant had a duty to reasonably safeguard its patients' data by implementing reasonable data security measures to protect against data breaches. The foreseeable harm to Plaintiff and the Class of inadequate data security created a duty to act reasonably and safeguard the Sensitive Information.

99. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting their Sensitive Information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

100. This duty included, among other things, designing, maintaining, and testing its security systems to ensure that Plaintiff's and the Class's PHI and PII was adequately protected and secured. Defendant further had a duty to implement processes that would detect a breach of its security system in a timely manner.

101. Defendant also had a duty to timely and adequately disclose to Plaintiff and the Class that their Sensitive Information had been or was reasonably believed to have been compromised. Timely and adequate disclosure is necessary so that, among other things, Plaintiff and the Class may take appropriate measures to monitor their accounts for unauthorized access, to

contact the credit bureaus to request freezes or place alerts and take all other appropriate precautions, including those recommended by Defendant.

102. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair ... practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice of failing to use reasonable measures to protect PII.

103. Additionally, HIPAA creates industry standards for maintaining the privacy of health-related data. Defendant knew or should have known it had a legal obligation to secure and protect Plaintiff's and the Class's Sensitive Information and that failing to do so is a serious violation of HIPAA.

104. Defendant also should have known that, given the Sensitive Information it held, Plaintiff and the Class would be harmed should it suffer a Data Breach. Defendant knew or should have known that its systems and technologies for processing and securing Plaintiff's and the Class's PHI and PII had security vulnerabilities susceptible to cyber-attacks.

105. Despite that knowledge, Defendant failed to implement reasonable data security measures which allowed cybercriminals to successfully breach Defendant's network and data environments, reside there undetected for a significant period of time, and access or steal a host of personal and healthcare information on thousands of Defendant's patients.

106. Defendant, through its actions and/or omissions, failed to provide reasonable security for the data in its possession.

107. Defendant breached its duty to Plaintiff and the Class by failing to adopt, implement, and maintain reasonable security measures to safeguard their Sensitive Information, allowing unauthorized access to Plaintiff's and the Class's PHI and PII, and failing to recognize

the Data Breach in a timely manner. Defendant further failed to comply with industry regulations and exercise reasonable care in safeguarding and protecting Plaintiff's and the Class's PHI and PII.

108. But for Defendant's wrongful and negligent breach of its duties, their Sensitive Information would not have been accessed and exfiltrated by unauthorized persons, and they would not face a risk of harm of identity theft, fraud, or other similar harms.

109. As a result of Defendant's negligence, Plaintiff and the Class suffered damages including, but not limited to, ongoing and imminent threat of identity theft crimes; out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or fraud; credit, debit, and financial monitoring to prevent and/or mitigate theft, identity theft, and/or fraud incurred or likely to occur as a result of Defendant's security failures; the value of their time and resources spent mitigating the identity theft and/or fraud; decreased credit scores and ratings; and irrecoverable financial losses due to fraud.

110. As a direct and proximate result of Defendant's negligence, Plaintiff and members of the Class suffered and continue to suffer injuries and are entitled to and demand actual, consequential, and nominal damages in an amount to be proven at trial.

COUNT II
Breach of Implied Contract
(On behalf of Plaintiff and the Nationwide Class or, Alternatively, the Pennsylvania Subclass)

111. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

112. Plaintiff and the Class entrusted their Private Information to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and

confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

113. In its Privacy Policy, Defendant represented that it would not disclose Plaintiff's and Class Members' Private Information to unauthorized third-parties.

114. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

115. Defendant breached the implied contracts they made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

116. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered or will suffer ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

117. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
Unjust Enrichment
(On behalf of Plaintiff and the Nationwide Class or, Alternatively, the Pennsylvania Subclass)

118. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

119. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable Private Information.

120. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information.

121. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

122. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

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

124. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

125. Plaintiff and Class Members have no adequate remedy at law.

126. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered or will suffer injury, including but not limited to: actual identity theft; the loss of the opportunity how their Private Information is used; the compromise, publication, and/or theft of their PII; out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

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

COUNT IV
Breach of Fiduciary Duty
(On behalf of Plaintiff and the Nationwide Class or, Alternatively, the Pennsylvania Subclass)

129. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

130. Plaintiff and members of the Class incorporate the above allegations as fully set forth herein.

131. Defendant owed a fiduciary duty to Plaintiff and the Class to protect their private and sensitive PHI and PII and keep them apprised of when that information becomes exposed or compromised in an accurate manner.

132. Defendant breached that fiduciary duty by, inter alia, failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect the private information of Plaintiff and members of the Class. This failure resulted in the Data Breach that ultimately came to pass.

133. Defendant further breached its fiduciary duty by failing to dispose of PHI and PII that was no longer required to render care, which unnecessarily exposed additional patients to the Data Breach, and by failing to timely and accurately inform Plaintiff and the Class of the Data Breach which materially impaired their mitigation efforts.

134. As a direct and proximate cause of Defendant's breaches of its fiduciary duty, Plaintiff and members of the Class have suffered or will suffer injury, including but not limited to: the compromise, publication, theft, and /or unauthorized use of their PII and PHI; out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft and fraud; lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; the continued risk to their PII and PHI, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect PII and PHI in its possession; and current and future

costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and members of the Class.

135. Plaintiff, on behalf of himself and the Class, seeks actual, consequential, and nominal damages and injunctive relief for breach of fiduciary duty.

COUNT V
Breach of Confidence
(On behalf of Plaintiff and the Nationwide Class or, Alternatively, the Pennsylvania Subclass)

136. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

137. Plaintiff and Class members have an interest, both equitable and legal, in the Private Information that was conveyed to, collected by, and maintained by Defendant and that was ultimately accessed or compromised in the Data Breach.

138. As a healthcare provider, Defendant has a special relationship to its patients, like Plaintiff and the Class members.

139. Because of that special relationship, Defendant was provided with and stored private and valuable PII and PHI related to Plaintiff and the Class, which it was required to maintain in confidence.

140. Plaintiff and the Class provided Defendant with their Private Information under both the express and/or implied agreement of Defendant to limit the use and disclosure of such Private Information.

141. Defendant had a common law duty to maintain the confidentiality of Plaintiff's and Class members' Private Information.

142. Defendant owed a duty to Plaintiff and Class members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

143. Plaintiff and Class members have a privacy interest in their personal medical matters, and Defendant had a duty not to disclose confidential medical information and records concerning its patients.

144. As a result of the parties' relationship, Defendant had possession and knowledge of the confidential Private Information of Plaintiff and Class members Plaintiff's and the Class's Private Information is not generally known to the public and is confidential by nature.

145. Plaintiff and Class members did not consent to nor authorize Defendant to release or disclose their Private Information to an unknown criminal actor.

146. Defendant breached the duty of confidences it owed to Plaintiff and Class members when Plaintiff's and Class's Private Information was disclosed to unknown criminal hackers.

147. Defendant breached its duties of confidence by failing to safeguard Plaintiff's and Class members' Private Information, including 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 the Private Information; (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; (h) storing PII, PHI and medical records/information in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiff and the Class members' Private Information to a criminal third party.

148. But for Defendant's wrongful breach of its duty of confidences owed to Plaintiff and Class members, their privacy, confidences, and Private Information would not have been compromised.

149. As a direct and proximate result of Defendant's breach of Plaintiff's and the Class's confidences, Plaintiff and Class members have suffered or will suffer injuries, including: the erosion of the essential and confidential relationship between Defendant—as a health care services provider—and Plaintiff and Class members as patients; loss of their privacy and confidentiality in their Private Information; theft of their Private Information; costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts; costs associated with purchasing credit monitoring and identity theft protection services; lowered credit scores resulting from credit inquiries following fraudulent activities; 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 Defendant's 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; the imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals; damages to and diminution in value of their Private Information entrusted,

directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others; continued risk of exposure to hackers and thieves of their Private Information, 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 Plaintiff's and Class members' data; loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received, as directed to do by Defendant; and/or mental anguish accompanying the loss of confidences and disclosure of their confidential Private Information.

150. Additionally, Defendant received payments from Plaintiff and Class members for services with the understanding that Defendant would uphold its responsibilities to maintain the confidences of Plaintiff and Class members' Private Information.

151. Defendant breached the confidence of Plaintiff and Class members when it made an unauthorized release and disclosure of their confidential Private Information and, accordingly, it would be inequitable for Defendant to retain the benefit at Plaintiff and Class members' expense.

152. As a direct and proximate result of Defendant's breach of confidences, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT VI
Violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Act Law, 73 P.S. 201-1, et seq.
(On behalf of Plaintiff and the Pennsylvania Subclass)

153. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

154. Plaintiff Ciccozzi and the Subclass members are "persons" within the meaning of 73 P.S. § 201-2(2).

155. Plaintiff and Class Subclass purchased goods and/or services from Defendant in that they purchased healthcare related good/or services.

156. Defendant engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 P.S. § 201-3, including the following:

a. Representing that its goods and services have characteristics, uses, benefits, and qualities that they do not have (73 P.S. § 201-2(4)(v));

b. Representing that its goods and services are of a particular standard or quality if they are another (73 P.S. § 201-2(4)(vii));

c. Failing to comply with the terms of any written guarantee or warranty given to the buyer at, prior to or after a contract for the purchase of goods or services is made (73 P.S. § 201-2(4)(xiv)); and

d. Engaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or of misunderstanding (73 P.S. § 201-2(4)(xxi)).

157. Defendant's unfair or deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass Members' PII and PHI, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures

in response to increasing cybersecurity risks in the healthcare sector, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C and § 45, HIPAA, 42 U.S.C. § 1320d, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII and PHI, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. and § 1320d;

f. Failing to timely and adequately notify Plaintiffs and Subclass Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass Members' PII and PHI; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with the common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. and § 45, HIPAA, 42 U.S.C. § 1320d.

158. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and the Subclass Members, about the

adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII and PHI.

159. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and the Subclass Members, leading them to believe for several months that their PII and PHI was secure and that they did not need to take actions to secure their data.

160. Defendant intended to mislead Plaintiffs and Subclass Members and induce them to rely on its misrepresentations and omissions.

161. Had Defendant disclosed to Plaintiff and Subclass Members that its Network systems were not secure and thus vulnerable to attack, Defendant would have been forced to adopt reasonable data security measures and comply with the law. Instead, Plaintiff and Subclass Members entrusted Defendant with their sensitive and valuable PII and PHI. Defendant accepted the responsibility of being a steward of this data, while keeping the inadequacy of its security measures secret from the public. Accordingly, because Defendant held itself out as maintaining a secure system and comply with state and federal law as well as industry standards, Plaintiffs and Subclass Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

162. Defendant acted intentionally, knowingly, willfully, wantonly, maliciously, and outrageously to violate Pennsylvania's Unfair Trade Practices and Consumer Protection Law and recklessly disregarded Plaintiff's and Subclass Members' rights.

163. As a result of Defendant's above-described conduct, Plaintiff and Subclass members have suffered damages from the disclosure of their information to unauthorized individuals.

164. The injury and harm that Plaintiff and the other Subclass members suffered was the direct and proximate result of Defendant's violations of the UTPCPL. Plaintiff and Subclass members have suffered or will suffer economic damages and other injury and actual harm in the form of, inter alia: actual identity theft and fraud; 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; improper disclosure of their PII/PHI; breach of the confidentiality of their PII/PHI; deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or 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.

165. Plaintiff Ciccozzi, individually and on behalf of the Subclass, requests that this Court enter such orders or judgments as may be necessary to enjoin Defendant from continuing its unfair and deceptive practices

166. Plaintiff and Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $100 (whichever is greater), treble damages, punitive damages, attorneys' fees or costs, and any additional relief the Court deems necessary or proper.

PRAYER FOR RELIEF

167. WHEREFORE, Plaintiff respectfully prays for judgment in his favor as follows:

a. Certification of the Class pursuant to Federal Rule of Civil Procedure 23;

b. Designation of Plaintiff as representative of the Class and the undersigned counsel, as Class Counsel;

c. An award of damages in an amount to be determined at trial or by this Court;

d. An order for injunctive relief, enjoining Defendant from engaging in the wrongful and unlawful acts described herein;

e. Pre-judgment interest at the maximum amount allowed by law;

f. Post-judgment interest at the maximum rate allowed by law;

g. An award of costs and attorneys' fees; and

h. Such other relief the Court may deem just and proper.

DEMAND FOR TRIAL BY JURY

168. Plaintiff hereby demands a trial by jury of all issues so triable.

Respectfully submitted,

Dated: December 14, 2022

/s/ Gary F. Lynch

Gary F. Lynch
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Phone: 412-322-9243
Email: gary@lcllp.com

Brian C. Gudmundson*
Jason P. Johnston*
Michael J. Laird*
Rachel K. Tack*
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
brian.gudmundson@zimmreed.com
jason.johnston@zimmreed.com
michael.laird@zimmreed.com
rachel.tack@zimmreed.com

Christopher D. Jennings*
Nathan I. Reiter III*
THE JOHNSON FIRM
610 President Clinton Ave., Suite 300

Little Rock, AR 72201
Tel: (501) 372-1300
chris@yourattorney.com
nathan@yourattorney.com

*To be admitted *pro hac vice*
Counsel for Plaintiff and the Proposed Class

ClassAction.org
