UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

LOUIS RUGGIERO, on behalf of himself and all others similarly situated, Plaintiff, v. FLORIDA HEALTH SCIENCES CENTER, INC. d/b/a Tampa General Hospital, Defendant.	**Case No. 8:23-cv-1778** **JURY TRIAL DEMANDED** **(CLASS ACTION)**

CLASS ACTION COMPLAINT

Plaintiff Louis Ruggiero ("Plaintiff") brings this Class Action Complaint on behalf of himself, and all others similarly situated, against Defendant Florida Health Sciences Center, Inc. d/b/a Tampa General Hospital ("Defendant" or "TGH"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to them, which are based on personal knowledge:

NATURE OF THE CASE

1. Hospitals and healthcare providers who handle sensitive, personally identifying information ("PII") and protected health information ("PHI") owe a duty to the persons to whom that data relates.

2. This duty arises based upon the parties' relationship and because it is foreseeable that the exposure of PII or PHI to unauthorized persons—and especially cybercriminals with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private healthcare matters.

3. This harm manifests in several ways, as 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.

4. Defendant is one of the most comprehensive medical facilities in west central Florida—serving a dozen counties with a population in excess of 4 million. As one of the largest hospitals in Florida, TGH is licensed for 1,040 beds.

5. Defendant knowingly obtains patient PII and PHI and has a resulting duty to securely maintain such information in confidence.

6. Plaintiff brings this class action on behalf of patients of Defendant, or otherwise people that are customers of or have their records collected by Defendant,

whose PII and/or PHI was accessed and exposed to unauthorized third parties during a data breach of Defendant's system that occurred between approximately May 12 and May 30, 2023 (the "Data Breach").

7. Despite the fact that Defendant became aware of the Data Breach on or about May 31, 2023, and allegedly finalized its investigation of the Data Breach by June 2, 2023, Defendant failed to notify Plaintiff and Class Members *until* July 28, 2023, when it began sending notification letters out by mail.

8. Plaintiff, on behalf of himself and the Class as defined herein, bring claims for negligence, negligence *per se*, breach of implied contract, unjust enrichment, violation of the consumer protection laws of Florida, and declaratory and injunctive relief, seeking actual, compensatory, punitive, and nominal damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and relief.

9. Based on the public statements of Defendant to date, a wide variety of PII and PHI was implicated in the breach including: names, addresses, phone numbers, dates of birth, Social Security numbers, health insurance information, medical record numbers, patient account numbers, dates of service and/or limited treatment information used by TGH for its business operations (collectively "PII and PHI").

10. As a direct and proximate result of Defendant's inadequate data security, its breach of its duty to handle PII and PHI with reasonable care, and its

failure to maintain the confidentiality of patients' information, Plaintiff's and Class Members' PII and/or PHI has been accessed by hackers and exposed to an untold number of unauthorized individuals.

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

12. To recover from Defendant for these harms, Plaintiff and the Class seek damages in an amount to be determined at trial, along with injunctive relief requiring Defendant to, at minimum: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; (iii) disclose, expeditiously, the full nature of the Data Breach and the types of PII and PHI accessed, obtained, or exposed by the hackers; and (iv) provide lifetime monitoring and identity theft insurance to all Class Members.

PARTIES

13. Plaintiff Louis Ruggiero is an adult individual who currently resides in Mulberry, Florida. Plaintiff Ruggiero's PHI and PII records were maintained within Defendant's networks and servers, as Plaintiff Ruggiero is a patient of TGH.

14. On or around August 4, 2023, Plaintiff Ruggiero received a notice letter from Defendant dated July 28, 2023, informing Plaintiff Ruggiero that his PII and PHI was accessed or exposed to unknown, unauthorized third parties during the Data Breach.

15. On or around May 26, 2023, cybercriminals obtained Plaintiff Ruggiero's PII and PHI and attempted to open a fraudulent credit card account with PayPal.

16. In response and as a result of the Data Breach, Plaintiff and Class Members have spent significant time and effort researching the Data Breach and reviewing and monitoring their accounts for fraudulent activity.

17. Plaintiff and Class Members suffered actual damages as a result of the failures of Defendant to adequately protect the sensitive information entrusted to it, including, without limitation, experiencing fraud or attempted fraud, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of their personal information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identity theft.

18. As a result of the Data Breach, Plaintiff and Class Members have been and will continue to be at a heightened and substantial risk of future identity theft

and its attendant damages for years to come. Such risk is certainly real and impending and is not speculative given the highly sensitive nature of the PII compromised by the Data Breach.

19. Defendant Florida Health Sciences Center, Inc. d/b/a Tampa General Hospital is a non-profit corporation incorporated in Florida, with its principal place of business located in Hillsborough County, Florida.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over the subject matter of this action pursuant to 28 U.S.C § 1332(d), because the amount in controversy for the Class exceeds $5,000,000, exclusive of interest and costs, there are more than 100 putative Members of the Class defined below, and a significant portion of putative Class Members are citizens of a different state than Defendant.

21. This Court has personal jurisdiction over Defendant TGH because it is a domestic Florida not-for-profit corporation and conducts business within the State of Florida and this District.

22. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL BACKGROUND

A. Defendant Knew the Risks of Storing Valuable PII and PHI and the Foreseeable Harm to Victims

23. At all relevant times, Defendant knew it was storing and permitting its internal networks and servers to transmit valuable, sensitive PII and PHI and that, as a result, Defendant's systems would be attractive targets for cybercriminals.

24. Defendant also knew that any breach of its systems, and 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.

25. These risks are not merely theoretical; in recent years, numerous high-profile breaches have occurred at businesses such as Equifax, Yahoo, Marriott, and many others.

26. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as a result of the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[1]

27. PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

[1] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

28. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the United States.

29. According to the Identity Theft Resource Center, in 2019, there were 1,473 reported data breaches in the United States, exposing 164 million sensitive records and 705 million "non-sensitive" records.[2]

30. In tandem with the increase in data breaches, the rate of identity theft and the resulting losses has also increased over the past few years. For instance, in 2018, 14.4 million people were victims of some form of identity fraud, and 3.3 million people suffered unrecouped losses from identity theft, nearly three times as many as in 2016. And these out-of-pocket losses more than doubled from 2016 to $1.7 billion in 2018.[3]

31. 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."[4]

[2] *Data Breach Reports: 2019 End of Year Report*, IDENTITY THEFT RESOURCE CENTER, at 2, *available at* https://notified.idtheftcenter.org/s/resource#annualReportSection.
[3] Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available at https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20(1).
[4] https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/.

32. "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."[5]

33. 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.

34. As indicated by Jim Trainor, 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."[6] 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.[7]

35. According to Experian:

[5] *Id.*
[6] IDExperts, You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows: https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.
[7] PriceWaterhouseCoopers, *Managing cyber risks in an interconnected world*, Key findings from The Global State of Information Security® Survey 2015: https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

> 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.
>
> 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.[8]

36. The "high value of medical records on the dark web has surpassed that of social security and credit card numbers. These records can sell for up to $1,000 online."[9]

37. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held

[8] Experian, Healthcare Data Breach: What to Know About them and What to Do After One: https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.
[9] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[10]

38. 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.

39. The healthcare sector suffered about 295 breaches in the first half of 2023 alone, according to the U.S. Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") data breach portal. More than 39 million individuals were implicated in healthcare data breaches in the first six months of the year.

[10] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/assets/gao-07-737.pdf.

B. Defendant Breached its Duty to Protect its PII and PHI

40. On May 31, 2023, Defendant detected unusual activity on its computer systems and began an investigation with the assistance of a third-party forensic firm.

41. On June 2, 2023, Defendant's investigation determined that an unauthorized third party accessed its network and obtained certain files from its systems between May 12 and May 30, 2023.

42. Defendant reviewed the files involved and determined that some patient information was included. According to Defendant, the information varied by individual, but may have included names, addresses, phone numbers, dates of birth, Social Security numbers, health insurance information, medical record numbers, patient account numbers, dates of service and/or limited treatment information used by TGH for its business operations (collectively the "PII and PHI").

43. Defendant posted a notice to its website (the "Cybersecurity Notice") describing the Data Breach on or around July 19, 2023, however it did not begin notifying affected patients by mail until on or around July 28, 2023.

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

45. Plaintiff received the notice letter from Defendant dated July 28, 2023, advising that Plaintiff was a victim of Defendant's data security failures exposing his PII and PHI.

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

C. Defendant's Representations and Privacy Policies

47. Plaintiff was and is very careful about sharing his PII and PHI.

48. Plaintiff took reasonable steps to maintain the confidentiality of his PII and relied on Defendant to keep his PII and PHI confidential and securely maintained, to use this information for related business purposes only, and to make only authorized disclosures of this information.

49. Defendant made promises and representations to its patients, including Plaintiff and Class Members, that the PII and PHI it collected from them as a condition of obtaining medical services at TGH would be kept safe, confidential, that the privacy of that information would be maintained.

50. Defendant's privacy policy provides that: "[w]e are committed to protecting the privacy of your health information."[11]

51. Defendant's privacy policy further states that "[w]e are required by law to maintain the privacy of your PHI and to provide you with notice of our legal duties

[11] *See* https://www.tgh.org/patients-visitors/joint-notice-privacy-policy.

and privacy practices with respect to your PHI. PHI is information about you, including demographic information, that may identify you and that relates to your health or condition and related health care services."[12]

52. Plaintiff and Class Members provided their PII and PHI to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

D. Defendant Failed to Comply with the FTC Act

53. Defendant is prohibited by the Federal Trade Commission ("FTC") Act, 15 U.S.C. § 45 (Section 5 of the FTC Act), from engaging in "unfair or deceptive acts or practices in or affecting commerce." The 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.

54. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice that violates the FTC Act.

55. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices.

[12] *Id.*

According to the FTC, the need for data security should be factored into all business decision-making.

56. In 2007, the FTC published guidelines establishing reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

57. The FTC has also published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

58. Defendant is aware of and failed to follow the FTC guidelines and failed to adequately secure PII and PHI.

59. 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.

60. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII and PHI, or to prevent the disclosure of such information to unauthorized individuals constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

61. Defendant was at all times fully aware of its obligations to protect the PII and PHI of consumers because of its business of obtaining, collecting, and storing PII and PHI. Defendant was also aware of the significant repercussions that would result from its failure to do so.

E. Defendant Failed to Comply with HIPAA

62. The federal Health Insurance Portability and Accountability Act ("HIPAA") requires the healthcare industry to have a generally accepted set of security standards for protecting health information.

63. HIPAA defines Protected Health Information ("PHI") as individually identifiable health information and electronic PHI ("e-PHI") that is transmitted by electronic media or maintained in electronic media. This protected information

includes: names, dates, phone numbers, fax numbers, email addresses, Social Security numbers, medical record numbers, health insurance beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers, device identifiers and serial numbers, URLs, IP addresses, biometric identifiers, photographs, and any other unique identifying number, characteristic, or code.

64. To this end, HHS promulgated the *HIPAA Privacy Rule* in 2000 and the *HIPAA Security Rule* in 2003. The security standards for the protection of e-PHI, known as "the Security Rule," establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities," must put in place to secure individuals' e-PHI.

65. Defendant is either an entity covered by HIPAA, *see* 45 C.F.R. § 160.102, or "business associates" covered by HIPAA, *see* 45 C.F.R. § 160.103, and therefore must comply with the HIPAA Privacy Rule and Security Rule, *see* 45 C.F.R. Part 160 and Part 164, Subpart A, C, and E.

66. HIPAA limits the permissible uses of e-PHI and prohibits the unauthorized disclosure of e-PHI. *See* 45 C.F.R. § 164.502. HIPAA also requires that covered entities implement appropriate safeguards to protect this information. *See* 45 C.F.R. § 164.530(c)(1).

67. The electronically stored images and healthcare information accessed by unauthorized third parties on Defendant's servers are e-PHI under the HIPAA Privacy Rule and the Security Rule, which protects all e-PHI a covered entity "creates, receives, maintains or transmits" in electronic form. 45 C.F.R. § 160.103.

68. The Security Rule requires covered entities, including Defendant to implement and maintain appropriate administrative, technical, and physical safeguards for protecting e-PHI. *See* 45 C.F.R. § 164.530(c)(1). Among other things, the Security Rule requires Defendant to identify and "[p]rotect against any reasonably anticipated threats or hazards to the security or integrity of [the] information" and "[p]rotect against any reasonably anticipated uses or disclosures." 45 C.F.R. § 164.306.

69. HIPAA also obligates Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations. *See* 45 C.F.R. § 164.308(a)(1)(i).

70. HIPAA further obligates Defendant to ensure that its workforces comply with HIPAA security standard rules, *see* 45 C.F.R. § 164.306(a)(4), to effectively train its workforces on the policies and procedures with respect to protected health information, as necessary and appropriate for those individuals to carry out their functions and maintain the security of protected health information. *See* 45 C.F.R. § 164.530(b)(1).

71. Defendant failed to comply with these HIPAA rules. Specifically, Defendant failed to put in place the necessary technical and non-technical safeguards required to protect Plaintiff's and other Class Members' PHI.

F. Plaintiff and Class Members Suffered Damages

72. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways. Plaintiff and Class Members 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.

73. Once PII or PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendant's conduct. Further, the value of Plaintiff's and Class Members' PII and PHI has been diminished by its exposure in the Data Breach.

74. As a result of Defendant's failures, Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their PII and PHI.

75. 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%.[13]

76. 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."[14]

77. "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."[15]

78. 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."[16]

[13] *See* https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud.
[14] https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud.
[15] *Id.*
[16] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

79. 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, and serious and long-term identity theft.[17]

80. "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."[18]

81. Plaintiff and the Class members have also been injured by Defendant's unauthorized disclosure of their confidential and private medical records and PHI.

82. Plaintiff and Class Members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and are 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.

CLASS ACTION ALLEGATIONS

83. Plaintiff brings this action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and (b)(3), individually and on behalf of the following Nationwide Class:

[17] *Id.*
[18] https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

> All persons whose PII and/or PHI was compromised in Defendant's Data Breach that was announced on or about July 19, 2023 (the "Nationwide Class").

84. Plaintiff brings this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and (b)(3) on behalf of the following Florida Subclass:

> All persons in Florida whose PII and/or PHI was compromised in Defendant's Data Breach that was announced on or about July 19, 2023 (the "Florida Subclass").

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

86. **Numerosity**. All requirements of Fed. R. Civ. P. 23(a)(1) are satisfied. The class described above is so numerous that joinder of all individual members in one action would be impracticable. While Plaintiff is informed and believes that there are likely hundreds of thousands of members of the Class, the precise number of Class members is unknown to Plaintiff. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach.

87. **Commonality and Predominance**. All requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3) are satisfied. This action involves questions of law and fact that are common to the Class Members. Such common questions include, but are not limited to:

a. Whether Defendant had a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether Defendant had a duty to maintain the confidentiality of Plaintiff's and Class Members' PHI;

c. Whether Defendant breached its obligation to maintain Plaintiff's and the Class Members' medical information in confidence;

d. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PII and PHI, and breached its duties thereby;

e. Whether Defendant failed to properly give notice pursuant to state and/or federal law;

f. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct;

g. Whether Plaintiff and Class Members are entitled to restitution or disgorgement as a result of Defendant's wrongful conduct; and

h. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

88. **Typicality**. All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. Plaintiff's claims are typical of the claims of the Class Members. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same failure by Defendant to safeguard PII and PHI. Plaintiff and Class Members were all patients of Defendant, each having their PII and PHI obtained by an unauthorized third party.

89. **Adequacy of Representation**. All requirements of Fed. R. Civ. P. 23(a)(4) are satisfied. Plaintiff is an adequate representative of the Class because his interests does not conflict with the interests of the other Class Members that Plaintiff seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation, including data breach litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's 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 Plaintiff and Plaintiff's counsel.

90. **Predominance and Superiority.** All requirements of Fed. R. Civ. P. 23(b)(3) are satisfied. As described above, common issues of law or fact

predominate over individual issues. Resolution of those common issues in Plaintiff's case will also resolve them for the Class's claims. In addition, a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Members of the Class to individually seek redress for Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

91. **Cohesiveness**. All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. Defendant has acted, or refused to act, on grounds generally applicable to the Nationwide Class and Subclass such that final declaratory or injunctive relief is appropriate.

92. Plaintiff reserves the right to modify, amend, or revise the foregoing class allegations and definitions prior to moving for class certification based on

newly learned facts or legal developments that arise following additional investigation, discovery, or otherwise.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(By Plaintiff on behalf of the Nationwide Class, or, alternatively, the Florida Subclass)

93. Plaintiff restates and realleges paragraphs 1 through 92 above as if fully set forth herein.

94. Defendant owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

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

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

97. Defendant's duty also arose from Defendant's position as a provider of healthcare. Defendant holds itself out as a trusted provider of healthcare, and thereby assumes a duty to reasonably protect its patients' information.

98. Indeed, Defendant, as a direct healthcare provider, was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

99. Defendant was subject to an "independent duty" untethered to any contract between Plaintiff and Class Members and Defendant.

100. Defendant's privacy policy provides that: "[w]e are committed to protecting the privacy of your health information," and that "[w]e are required by law to maintain the privacy of your PHI."

101. Defendant violated its own policies by actively disclosing Plaintiff's and the Class Members' PII and PHI; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII and PHI; failing to maintain the confidentiality of Plaintiff's and the Class Members' records; and by failing to provide timely notice of the breach of PII and PHI to Plaintiff and the Class.

102. Defendant breached the duties owed to Plaintiff and Class Members and thus was negligent. Defendant breached these duties 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; and

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

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

104. As a direct and proximate result of Defendant's negligence, Plaintiff 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 the financial accounts;

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 Defendant 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 Plaintiff's 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 Plaintiff's and Class Members' data;

i. Loss of their privacy and confidentiality in their PII and PHI;

j. The erosion of the essential and confidential relationship between Defendant – as a health care services provider – and Plaintiff and Class members as patients; and

k. Loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received.

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

106. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, among other things: (i) strengthen its data security systems

and monitoring procedures; (ii) submit to future annual audits of those systems; (iii) disclose, expeditiously, the full nature of the Data Breach and the types of PII and PHI accessed, obtained, or exposed by the hackers; and (iv) provide lifetime monitoring and identity theft insurance to all Class Members.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(By Plaintiff on behalf of the Nationwide Class, or, alternatively, the Florida Subclass)

Negligence *Per Se* Under the FTC Act

107. Plaintiff restates and realleges paragraphs 1 through 92 above as if fully set forth herein.

108. 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 Defendant or failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of Defendant's duty.

109. Defendant 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.

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

111. The harm that has occurred as a result of Defendant's conduct is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

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

113. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

114. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; (iii) disclose, expeditiously, the full nature of the Data Breach and the types of PII and PHI accessed, obtained, or exposed by the hackers; and (iv) provide lifetime monitoring and identity theft insurance to all Class Members.

Negligence *Per Se* Under HIPAA

115. Defendant is an entity covered under HIPAA which sets minimum federal standards for privacy and security of PHI.

116. The HIPAA Security Rule requires Defendant to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting PHI, which Defendant negligently failed to implement. The HIPAA Security Rule requires Defendant to protect against reasonably anticipated threats to the security or integrity of PHI and protect against reasonably anticipated impermissible uses or disclosures, which Defendant negligently failed to do. *See* 45 C.F.R. Part 160 and Part 164, Subpart A, C, and E.

117. Plaintiff and Class Members are within the class of persons the HIPAA Security Rule was intended to protect. The harm that has occurred is the type of harm the HIPAA was intended to guard against.

118. Defendant's failure to secure Plaintiff's and Class Members' PHI, failure to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PHI, and failure to timely notify them that such information had been accessed by unauthorized third parties violated HIPAA, in at least the following HIPAA regulations:

- The HIPAA Privacy and Security Rule 45 C.F.R. § 160 and 45 C.F.R. § 164, Subpart A, C, and E

- 45 C.F.R. § 164.306
- 45 C.F.R. § 164.308
- 45 C.F.R. § 164.312
- 45 C.F.R. § 164.314
- 45 C.F.R. § 164.502
- 45 C.F.R. § 164.530

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

120. Defendant's violation of HIPAA constitutes *negligence per se*.

121. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; (iii) disclose, expeditiously, the full nature of the Data Breach and the types of PII and PHI accessed, obtained, or exposed by the hackers; and (iv) provide lifetime monitoring and identity theft insurance to all Class Members.

122. Whether under Section 5 of the FTC Act or under HIPAA, each independently constitutes negligence *per se*.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(By Plaintiff on behalf of the Nationwide Class, or, alternatively, the Florida Subclass)

123. Plaintiff restates and realleges paragraphs 1 through 92 above as if fully set forth herein.

124. When Defendant required Plaintiff and Class Members to supply their PII and PHI, Defendant entered into implied contracts with Plaintiff and Class Members to protect the security of such information.

125. Defendant collects and uses Plaintiff's and Class Member's PII and PHI for the purpose of treating patients.

126. Such implied contracts arose from the course of conduct between Plaintiff and Class Members and Defendant.

127. The implied contracts required Defendant to safeguard and protect Plaintiff's and Class Members' PII and PHI from being compromised and/or stolen.

128. Defendant did not safeguard or protect Plaintiff's and Class Members' PII and PHI from being accessed, compromised, and/or stolen. Defendant did not maintain sufficient security measures and procedures to prevent unauthorized access to Plaintiff's and Class Members' PII and PHI.

129. Because Defendant failed to safeguard and/or protect Plaintiff's and Class Members' PII and PHI from being compromised or stolen, Defendant breached its contracts with Plaintiff and Class Members.

130. Plaintiff and Class Members fully performed their obligations under the implied contracts by supplying their PII and PHI to Defendant and paying Defendant for its services.

131. As a direct and proximate result of Defendant's breaches of implied contracts, Plaintiff and Class Members sustained damages as alleged herein and will continue to suffer damages as the result of Defendant's Data Breach.

132. Plaintiff and Class Members have been injured as described herein and above, and are entitled to damages, including actual, compensatory, punitive, and nominal damages, in an amount to be proven at trial.

133. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; (iii) disclose, expeditiously, the full nature of the Data Breach and the types of PII and PHI accessed, obtained, or exposed by the hackers; and (iv) provide lifetime monitoring and identity theft insurance to all Class Members.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(By Plaintiff on behalf of the Nationwide Class, or, alternatively, the Florida Subclass)

134. Plaintiff restates and realleges paragraphs 1 through 92 above as if fully set forth herein.

135. Plaintiff and Class Members conferred a monetary benefit on Defendant when they paid for services from Defendant and/or its agents and in so doing also provided Defendant with their PII and PHI.

136. In exchange, Plaintiff and Class Members expected to receive from Defendant the services that were the subject of the transactions and should have had their PII and PHI protected with adequate data security.

137. Defendant appreciated the benefits that Plaintiff and Class Members conferred, and Defendant profited from these transactions and used Plaintiff's and Class Members' PII and PHI for business purposes.

138. Defendant funds its data security measures from revenues derived from the payments made by and on behalf of Plaintiff and Class Members.

139. Defendant, however, failed to secure Plaintiff's and Class Members' PII and PHI and, therefore, did not provide adequate data security in return for the benefits Plaintiff and Class Members provided.

140. Plaintiff and Class Members expected that Defendant would use a portion of that revenue to fund adequate data security practices.

141. Defendant acquired Plaintiff's and Class Members' PII and PHI through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

142. If Plaintiff and Class Members knew that Defendant had not reasonably secured their PII and PHI, they would not have allowed their PII and PHI to be provided to Defendant.

143. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII and PHI.

144. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant increased its own profit at the expense of Plaintiff and Class Members by utilizing ineffective security measures.

145. Plaintiff 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 and the safety of their PII and PHI.

146. Defendant should not be permitted to retain the money wrongfully obtained Plaintiff and Class Members, because Defendant failed to implement appropriate data security measures.

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

148. As a direct and proximate result of Defendant's unjust enrichment, Plaintiff and Class Members sustained damages as alleged herein and will continue to suffer damages as the result of Defendant's Data Breach.

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

FIFTH CAUSE OF ACTION
FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT
Fla. Stat. §§ 501.201, *et seq.*
(By Plaintiff on behalf of the Nationwide Class, or, alternatively, the Florida Subclass)

150. Plaintiff restates and realleges paragraphs 1 through 92 above as if fully set forth herein.

151. Plaintiff and Class Members are "consumers" as defined by Fla. Stat. § 501.203.

152. Defendant advertised, offered, or sold goods or services and engaged in trade or commerce directly or indirectly affecting Plaintiff and Class Members.

153. Defendant engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

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

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, 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 Plaintiff's and Class Members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Data Breach;

d. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII and PHI; and

e. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' PII and PHI including by implementing and maintaining reasonable security measures.

154. These omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII and PHI. Plaintiff and Class

Members would have discontinued Defendant's access to their PII and PHI had this information been disclosed.

155. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII and PHI; overpayment for Defendant's services; loss of the value of access to their PII and PHI; and the value of identity protection services made necessary by the Breach.

156. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including actual damages under Fla. Stat. § 501.211; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

SIXTH CAUSE OF ACTION
DECLARATORY AND INJUNCTIVE RELIEF
28 U.S.C. §§ 2201, *et seq.*
(By Plaintiff on behalf of the Nationwide Class)

157. Plaintiff restates and realleges paragraphs 1 through 92 above as if fully set forth herein.

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

159. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and statutory duties to reasonably safeguard its patients' sensitive personal information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches. Plaintiff alleges that Defendant's data security practices remain inadequate.

160. Plaintiff and Class Members continue to suffer injury as a result of the compromise of their sensitive personal information and remain at imminent risk that further compromises of their personal information will occur in the future.

161. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Defendant continues to owe a legal duty to secure patients' sensitive personal information, to timely notify patients of any data breach, and to establish and implement data security measures that are adequate to secure customers' sensitive personal information.

162. The Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect consumers' sensitive personal information.

163. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, for which they lack an adequate legal remedy. The threat of another data breach is real, immediate, and substantial. If another data breach at TGH occurs, Plaintiff and Class Members will not have an adequate remedy at law because not all of the resulting injuries are readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

164. The hardship to Plaintiff and Class Members if an injunction does not issue greatly exceeds the hardship to Defendant if an injunction is issued. If another data breach occurs, Plaintiff and Class Members will likely be subjected to substantial risk of identity theft and other damages. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

165. Issuance of the requested injunction will serve the public interest by preventing another data breach at TGH, thus eliminating the additional injuries that would result to Plaintiff and the millions of patients whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all other similarly situated, prays for relief as follows:

a. For an order certifying the Class(es) defined above and naming Plaintiff as representatives of the Class(es) and Plaintiff's attorneys as Class Counsel to represent the Class(es);

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

c. For actual, compensatory, punitive, and nominal damages, in amounts to be determined by the trier of fact;

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

e. Declaratory and injunctive relief as described herein;

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

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

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

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial as to all issues triable by a jury.

Dated: August 8, 2023

/s/ Nicholas A. Colella

Nicholas A. Colella
FL Bar No. 1002941
Gary F. Lynch (*pro hac vice* forthcoming)
Jamisen A. Etzel (*pro hac vice* forthcoming)
LYNCH CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
Email: nickc@lcllp.com
Email: gary@lcllp.com
Email: jamisen@lcllp.com

Christian Levis (*pro hac vice* forthcoming)
Amanda G. Fiorilla (*pro hac vice* forthcoming)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Email: clevis@lowey.com
Email: afiorilla@lowey.com

Anthony M. Christina (*pro hac vice* forthcoming)
LOWEY DANNENBERG, P.C.
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA
Telephone: (215) 399-4770
Email: achristina@lowey.com

Attorneys for Plaintiff and the Proposed Class

JS 44 (Rev. 04/21)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

LOUIS RUGGIERO

(b) County of Residence of First Listed Plaintiff Polk
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Lynch Carpenter, LLP, 1133 Penn Ave, 5th Floor, Pittsburgh, PA 15222. T: (412) 322-9243

DEFENDANTS

FLORIDA HEALTH SCIENCES CENTER, INC. d/b/a Tampa General Hospital

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☒ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☒ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

INTELLECTUAL PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. 1332(d)

Brief description of cause:
Data breach

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE a) Mary S. Scriven; b) Kathryn Kimball Mizelle DOCKET NUMBER a) 8:23-cv-01728; b) 8:23-cv-01757

DATE
8/8/2023

SIGNATURE OF ATTORNEY OF RECORD
/s/ Nicholas A. Colella

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Middle District of Florida

LOUIS RUGGIERO, on behalf of himself and all others similarly situated,

Plaintiff(s)

v.

FLORIDA HEALTH SCIENCES CENTER, INC. d/b/a Tampa General Hospital

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* FLORIDA HEALTH SCIENCES CENTER, INC.
c/o NICOLE JUSTICE, MSJ
ONE DAVIS BLVD - STE. 401
TAMPA, FL 33606

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Nicholas A. Colella
Lynch Carpenter, LLP
1133 Penn Ave, 5th Floor
Pittsburgh, PA 15222

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

SANDY OPACICH, CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc: