Morgan & Morgan Philadelphia, PLLC
2005 Market Street
Suite 350
Philadelphia, PA 19103
(215) 446-9795
(215) 446-9799 (FAX)
www.forthepeople.com

Kevin Clancy Boylan
ID# 314117
cboylan@forthepeople.com

NANETTE KATZ, individually and on behalf of all others similarly situated **505 Deerfield Court** **Blue Bell, PA 19422** **Plaintiff,** **v.** **EINSTEIN HEALTHCARE NETWORK** **5501 Old York Road** **Philadlephia, PA 19144** **Defendant.**	**IN THE COURT OF COMMON PLEAS** **OF PHILADELPHIA COUNTY** **CIVIL ACTION – CLASS ACTION** **JURY TRIAL DEMANDED** **APRIL TERM, 2021** **NO.:**

COMPLAINT - CLASS ACTION
NOTICE TO PLEAD

NOTICE

You have been sued in court. If you wish to defend against the claims set forth in the following pages, you must take action within twenty (20) days after this complaint and notice are served, by entering a written appearance personally or by attorney and filing in writing with the court your defenses or objection to the claims set forth against you. You are warned that if you fail to do so the case may proceed without you and a judgment may be entered against you by the court without further notice for any money claimed in the complaint or for any other claim or relief requested by the plaintiff. You may lose money or property or other rights important to you.

YOU SHOULD TAKE THIS PAPER TO YOUR LAWYER AT ONCE. IF YOU DO NOT HAVE A LAWYER OR CANNOT AFFORD ONE, GO TO OR TELEPHONE THE OFFICE SET FORTH BELOW TO FIND OUT WHERE YOU CAN GET LEGAL HELP.

PHILADELPHIA BAR ASSOCIATION
Lawyer Referral and Information Service
One Reading Center
Philadelphia, Pennsylvania 19107-2911
Telephone: (215) 238-6333

AVISO

Le han demandado a usted en la corte. Si usted quiere defenderse de estas demandas expuestas en las páginas siguientes, usted tiene veinte (20) dias de plazo al partir de la fecha de la demanda y la notificación. Hace falta asentar una comparencia escrita o en persona o con un abogado y entregar a la corte en forma escrita sus defensas o sus objeciones a las demandas en contra de su personá. Sea avisado que si usted no se defiende, la corte tomará medidas y puede continuar la demanda en contra suya sin previo aviso o notificación. Además, la corte puede decidir a favor del demandante y requiere que usted cumpla con todas las provisiones de esta demanda. Usted puede perder dinero o sus propiedades o otros derechos importantes para usted.

LLEVE ESTA DEMANDA A UN ABOGADO INMEDIATAMENTE. SI NO TIENE ABOGADO O SI NO TIENE EL DINERO SUFICIENTE DE PAGAR TAL SERVICO, VAYA EN PERSONA O LLAME POR TELÉFONO A LA OFICINA CUYA DIRECCIÓN SE ENCUENTRA ESCRITA ABAJO PARA AVERIGUAR DONDE SE PUEDE CONSEGUIR ASISTENCIA LEGAL.

ASOCIACIÓN DE LICENCIADOS DE FILADELFIA
Servicio De Referencia E Información Legal
One Reading Center
Filadelfia, Pennsylvania 19107-2911
Teléfono: (215) 238-6333

Morgan & Morgan Philadelphia, PLLC
2005 Market Street
Suite 350
Philadelphia, PA 19103
(215) 446-9795
(215) 446-9799 (FAX)
www.forthepeople.com

Kevin Clancy Boylan
ID# 314117
cboylan@forthepeople.com

NANETTE KATZ, individually and on behalf of all others similarly situated, **Plaintiff,** **v.** **EINSTEIN HEALTHCARE NETWORK,** **Defendant.**	**IN THE COURT OF COMMON PLEAS OF PHILADELPHIA COUNTY** **CIVIL ACTION – CLASS ACTION** **JURY TRIAL DEMANDED** **APRIL TERM, 2021** **NO.:**

COMPLAINT

Plaintiff Nanette Katz ("Plaintiff"), individually and on behalf of the Class defined below of similarly situated persons, brings this Class Action Complaint and alleges the following against Einstein Healthcare Network ("Einstein" or "Defendant"), based upon personal knowledge with respect to Plaintiff and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

NATURE OF THE ACTION

1. Plaintiff brings this class action against Einstein for Einstein's failure to properly secure and safeguard protected health information as defined by the Health Insurance Portability and Accountability Act ("HIPAA"), medical information, and other personally identifiable information, including without limitation names, dates of birth, Social Security numbers, medical record and patient account numbers, health insurance information, diagnoses, medication

information, treatment providers, types of treatment, and treatment locations (collectively, "PHI"), for failing to comply with industry standards to protect information systems that contain that PHI, and for failing to provide timely, accurate, and adequate notice to Plaintiff and other Class Members that their PHI had been compromised. Plaintiff seeks, among other things, orders requiring Einstein to fully and accurately disclose the nature of the information that has been compromised and to adopt reasonably sufficient security practices and safeguards to prevent incidents like the disclosure in the future.

2. Einstein is a leading healthcare provider in Pennsylvania.

3. On or about October 9, 2020, Einstein announced a security incident that occurred in August 2020, involving patient PHI. (the "Data Breach"). The security incident was wide-reaching and compromised the PHI of at least 353,616 individuals, according to the submission Einstein's made to the U.S. Secretary of Health and Human Services at the Office for Civil Rights ("OCR").[1]

4. Einstein began mailing notice letters to patients whose information was compromised on October 9, 2020, but continued its investigation of the incident through November 16, 2020. As a result of the completed investigation, Einstein continued to mail letters to affected patients between January 21, 20201 and February 8, 2021. As such, the number of patients actually affected may be far greater than 353,616, which was the number Einstein reported to the OCR on October 9, 2020. An exemplar of the Notification of Data Security Incident letter from Einstein dated January 21, 2021 (the "Notification Letter") that was sent to Plaintiff is

[1] Department of Health and Human Services, Office for Civil Rights, Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Apr. 19, 2021).

attached hereto as **Exhibit** "**A**."

5. This case involves a breach of employee email accounts by an unknown third party, resulting in the unauthorized disclosure of the PHI of Plaintiff and Class Members by Einstein to unknown third parties. As a result of Einstein's failure to implement and follow basic security procedures, Plaintiff's and Class Members' PHI is now in the hands of criminals. Plaintiff and Class Members now and will forever face a substantial increased risk of identity theft. Consequently, Plaintiff and Class Members have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to Einstein's failures.

6. Additionally, as a result of Einstein's failure to follow contractually-agreed upon, federally-prescribed, industry standard security procedures, Plaintiff and Class Members received only a diminished value of the services Einstein was to provide. Einstein expressly represented that it would maintain the confidentiality of Plaintiff and Class Members' PHI obtained throughout the course of treatment.

7. Accordingly, Plaintiff, individually and on behalf of all others similarly situated, alleges claims for negligence, breach of contract, breach of implied contract, breach of fiduciary duty, and breach of confidence.

PARTIES

8. Plaintiff Nanette Katz is a citizen and resident of Blue Bell, Pennsylvania. At all times relevant to this Complaint, Plaintiff was a patient of Einstein, whose PHI was disclosed without authorization to an unknown third party as a result of the Data Breach.

9. Defendant Einstein is a leading private, not-for-profit Pennsylvania healthcare system with its principal address at 5501 Old York Road, Philadelphia, PA 19144.

10. Einstein cares for patients through a network of hospitals, primary and specialty

care practices, and outpatient services located in the Commonwealth of Pennsylvania. Due to the nature of these services, Einstein acquires and electronically stores patient PHI.

JURISDICTION AND VENUE

11. This Court has jurisdiction over this action as Defendant operates its medical facilities throughout the Commonwealth of Pennsylvania, and specifically in Philadelphia County.

12. Einstein regularly and systematically conducted and continues to conduct in Philadelphia County.

13. This Court has personal jurisdiction over Einstein pursuant to 42 Pa. C.S. §§ 931 and 5301. Einstein maintains its principal place of business in this jurisdiction and is authorized to and does conduct substantial business in this jurisdiction.

14. Venue is proper in this Court pursuant to Pa. R. C. P. 1006 and 2179(a)(2) because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in, was directed to, and/or emanated from this County, Einstein is based in this County, Einstein maintains patients' PHI in this County, and has caused harm to Plaintiff and Class Members residing in this County.

FACTUAL BACKGROUND

A. Einstein's Business

15. Defendant began operating as a healthcare facility in Philadelphia in 1866 as the Jewish Hospital. In 1952, the Jewish Hospital merged with two other Philadelphia-based hospitals to create the Albert Einstein Healthcare Network.[2]

[2] *See* https://www.einstein.edu/about (last accessed Apr. 20, 2021).

16. Today, Einstein's facilities consist of 3 hospitals, 15 outpatient centers, and 31 primary care practice locations throughout the Greater Philadelphia region. Einstein employs more than 8,700 employees and over 900 physicians.[3]

17. Einstein also offers residency and fellowship training programs in many specialized areas. Einstein advertises that it has over 450 residents and fellows enrolled in over 35 physician graduate medical education programs.[4]

18. As a healthcare provider, Einstein is required to ensure that such private, personal information is not disclosed or disseminated to unauthorized third parties without the patients' express written consent, as further detailed below.

B. The Data Breach

19. On August 10, 2020, Einstein identified suspicious activity within a number of Einstein employees' email accounts.

20. After engaging a computer forensic firm to investigate the suspicious activity, Einstein determined that an unauthorized third party gained access to employee email accounts between August 5, 2020 and August 17, 2020.

21. The investigation concluded that through these email accounts, the unauthorized third party had access to sensitive patient PHI including: names, dates of birth, medical record and patient account numbers, health insurance information, and treatment information such as diagnosises, medications, providers, types of treatment, and treatment locations.

22. Einstein concluded that in some instances, patient Social Security numbers were also compromised.

---

[3] *See* https://www.einstein.edu/about/about-our-network (last accessed Apr. 20, 2021).
[4] *Id*.

23. The investigation was apparently unable to determine additional details regarding the scope of access, leaving open the possibility that patient PHI was viewed, copied and/or removed from employee emails.

24. On October 9, 2020, Einstein began mailing letters to paitents whose information was identified as compromised.

25. Meanwhile, the investigation into the Data Breach continued until November 16, 2020. Interestingly, between January 21, 2021 and February 8, 2021, nearly two months after the investigation concluded, Einstein sent an additional round of Notification Letters to affected patients.

26. The Notification Letter Plaintiff received, dated nearly five months after Einstein first learned about the Data Breach, was untimely and woefully deficient, failing to provide basic details concerning the Data Breach, including, but not limited to, why sensitive patient information was stored within employee emails which were clearly stored on systems without adequate security, the deficiencies in the security systems that permitted unauthorized access, whether the stolen data was encrypted or otherwise protected, and whether Einstein knows if the data has not been further disseminated.

27. Even worse, Einstein selectively offered one year of credit monitoring and identity protection to only those patients whose Social Security numbers were compromised.[5] Plaintiff and other Class Members whose sensitive medical information was compromised were not offered this service to protect themselves from inevitable fraud and identity theft. Instead, Einstein warns Plaintiff and those Class Members to "review statements [they] receive from [their] health insurer

[5] *See* https://www.einstein.edu/datasecurity (last accessed Apr. 21, 2021).

or healthcare provider" and if they "see charges for services [they did not receive" to contact the insurer or provider immediately. **See Exhibit "A.**"

28. In deliberate disregard of the fact that the stolen sensitive information was accessed by an unauthorized third party, Einstein downplayed the seriousness of the incident by informing Plaintiff and Class Members that "there is no evidence that any of your information was actually viewed by the unauthorized person or that it has been misused," and that Einstein, simply out of an abundance of caution, wanted to make Plaintiffs and Class Members aware of the Data Breach.

29. These representations are boilerplate language suggesting Einstein's lack of concern for the seriousness of the Data Breach—wherein an unauthorized third party gained access to PHI in Einstein's possession.

30. To date, Einstein has not yet disclosed full details of the Data Breach. Without such disclosure, questions remain as to the full extent of the Data Breach, the number of patients involved, the actual data accessed and compromised, and what measures, if any, Einstein has taken to secure the PHI still in its possession. Through this litigation, Plaintiff seeks to determine the scope of the Data Breach and the information involved, obtain relief that redresses Plaintiff's harms, and ensure Einstein has proper measures in place to prevent another breach from occurring in the future.

C. Einstein's Pricavy Policies

31. Einstein pledges that it takes patient privacy very seriously. Einstein makes numerous promises to its patients that it will maintain the security and privacy of their PHI.

32. Einstein acknowledges in its Notice of Privacy Practices that it is "required by law to keep [patient] PHI private."[6]

33. Einstein discloses certain situations and circumstances in which it uses and discloses PHI, none of which describe the facts involved in the Data Breach.[7]

34. Einstein created these policies, representations, and requirements, and publicly advertises them on its website as a means of increasing the value of its relationships with patients, thus allowing it to charge consumers higher rates under the guise of enhanced security and information security practices.

35. Einstein's Notice of Privacy Practices is also posted in its registration areas and is given to patients as they are admitted to the hospital or visit outpatient areas for services and treatment.[8] Einstein makes a direct effort to inform patients of its promises regarding patient privacy.

D. The Healthcare Sector is Particularly Suseptible to Data Breaches

36. Einstein was on notice that companies in the healthcare industry are susceptible targets for data breaches.

37. Einstein was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems,

---

[6] *See* https://www.einstein.edu/upload/docs/Einstein/privacy%20practices%20poster%208.15.16%20final.pdf (last accessed Apr. 21, 2021).
[7] *Id.*
[8] *See* https://www.einstein.edu/patients-visitors/patient-information/general/privacy/notice-of-privacy-practices (last accessed Apr. 21, 2021).

perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PHI)."[9] The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.

38. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[10] In 2017, a new record high of 1,579 breaches were reported representing a 44.7 percent increase.[11] That trend continues.

39. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[12] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay

---

[9] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), *available at*: https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last accessed Apr. 19, 2021).

[10] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), *available at:* https://www.idtheftcenter.org/surveys-studys (last accessed Apr. 19, 2021).

[11] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review, available at:* https://www.idtheftcenter.org/2017-data-breaches/ (last accessed Apr. 19, 2021).

[12] Identity Theft Resource Center, *2018 End -of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-data-breaches/ (last accessed Apr. 19, 2021).

out-of-pocket costs for healthcare they did not receive in order to restore coverage.[13] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[14]

40. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported having a significant security incident in the last 12 months, with a majority of these known incidents being caused by "bad actors" such as cybercriminals.[15] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[16]

41. As the number of healthcare data breaches continues to rise, email remains the primary outlet through which health data is exposed. For example, in 2017, there were 85 reported

[13] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed Apr. 19, 2021).
[14] *Id.*
[15] *2019 HIMSS Cybersecurity Survey, available at*: https://www.himss.org/2019-himss-cybersecurity-survey (last accessed Apr. 19, 2021).
[16] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last accessed Apr. 19, 2021).

email-related healthcare breaches—more than double the number reported in 2016—accounting for nearly one-quarter of all healthcare breaches.[17]

42. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[18]

43. In the healthcare industry, the number one threat vector from a cyber security standpoint is phishing. Cybersecurity firm Proofpoint reports that "phishing is the initial point of compromise in most significant [healthcare] security incidents, according to a recent report from the Healthcare Information and Management Systems Society (HIMSS). And yet, 18% of healthcare organizations fail to conduct phishing tests, a finding HIMSS describes as 'incredible.'"[19]

44. The report from Proofpoint was published March 27, 2019, and summarized findings of recent healthcare industry cyber threat surveys and recounted good, common sense steps that the targeted healthcare companies should follow to prevent email-related cyberattacks.

45. One of the best protections against email related threats is security awareness training and testing on a regular basis. This should be a key part of a company's on-going training

---

[17] Jessica Kim Cohen, *Email Is Now the Top Source of Healthcare Breaches*, Modern Healthcare (Mar. 23, 2019), *available at*: https://www.modernhealthcare.com/technology/email-now-top-source-healthcare-breaches (last accessed Apr. 19, 2021).

[18] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited Apr. 19, 2021).

[19] Aaron Jensen, Healthcare Phishing Statistics: 2019 HIMSS Survey Results (Mar. 27, 2019), https://www.proofpoint.com/us/security-awareness/post/healthcare-phishing-statistics-2019-himss-survey-results (last visited Apr. 19, 2021).

of its employees. "[S]ince phishing is still a significant, initial point of compromise, additional work needs to be done to further lower the click rate," the HIMSS report states. "This can be done through more frequent security awareness training, phishing simulation, and better monitoring of metrics pertaining to phishing (including whether there are any particular repeat offenders)."[20]

46. ProtonMail Technologies publishes a guide for IT Security to small businesses (i.e., companies without the heightened standard of care applicable in the healthcare industry). In its 2019 guide, ProtonMail dedicates a full chapter of its Book guide to the danger of phishing and ways to prevent a small business from falling prey to it. It reports:

> Phishing and fraud are becoming ever more extensive problems. A recent threat survey from the cybersecurity firm Proofpoint stated that between 2017 and 2018, email-based attacks on businesses increased 476 percent. The FBI reported that these types of attacks cost companies around the world $12 billion annually.
>
> Similar to your overall IT security, your email security relies on training your employees to implement security best practices and to recognize possible phishing attempts. This must be deeply ingrained into every staff member so that every time they check their emails, they are alert to the possibility of malicious action.[21]

As a major healthcare provider, Einstein knew, or should have known, the importance of safeguarding the patients' PHI entrusted to it and of the foreseeable consequences if that data was disclosed. This includes the significant costs that would be imposed on Einstein's patients as a result of a breach. Einstein failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

E. Einstein Obtains, Collects, and Stores Plaintiff's and Class Members' PHI

[20] *Id.*

[21] *The ProtonMail Guide to IT Security for Small Businesses*, ProtonMail (2019), *available at* https://protonmail.com/it-security-complete-guide-for-businesses (last visited Sept. 7, 2020).

47. Einstein obtains, collects, and stores a massive amount of its patients' protected health information and personally identifiable data.

48. As a condition of engaging in health services, Einstein requires that patients entrust it with highly confidential PHI.

49. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PHI, Einstein assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff and Class Members' PHI from disclosure.

50. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PHI and, as current and former patients, they rely on Einstein to keep this information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

F. The Value of PHI and the Effects of Unauthorized Disclosure

51. Einstein was well aware that the protected health information and personally identifiable information it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

52. PHI is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[22] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

[22] Federal Trade Commission, *Warning Signs of Identity Theft, available at:* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last accessed Apr. 19, 2021).

53. While credit card information and associated personally identifiable information can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute.[23]

54. Protected health information is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

55. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[24]

56. The ramifications of Einstein's failure to keep its patients' PHI secure are long lasting and severe. Once PHI is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

---

[23] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at:* https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last accessed Apr. 19, 2021).

[24] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, *available at*: https://khn.org/news/rise-of-indentity-theft/ (last accessed Apr. 18, 2021).

57. Further, criminals often trade stolen PHI on the "cyber black-market" for years following a breach. Cybercriminals can post stolen PHI on the internet, thereby making such information publicly available.

58. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened. [25] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[26]

59. Here, not only was sensitive medical information compromised, but also patient Social Security numbers. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.[27] This time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used, compounds an identity theft victim's ability to detect and address the harm.

60. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the

---

[25] *See* Medical ID Theft Checklist, *available at:* https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last accessed Apr. 18, 2021).
[26] Experian, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages*"), *available at:* https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last accessed Apr. 19, 2021).
[27] *Identity Theft and Your Social Security Number*, Social Security Administrative *available at* http://www.ssa.gov/pubs/EN-05-10064.pdf.

individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

61. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security Number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

62. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[28]

63. Einstein knew, or should have known, the importance of safeguarding its patients' PHI entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Einstein's patients as a result of a breach. Einstein failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

64. The ramifications of Einstein's failure to keep its patients' PHI secure are long lasting and severe.

G. The Data Breach Exposed Plaintiff and Class Members to Identity Theft and Monetary Injuries

[28] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Apr. 21, 2021).

65. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PHI.

66. Despite all of the publicly available knowledge of the continued compromises of PHI, Einstein's approach to maintaining the privacy of Einstein's patients' protected health information was lackadaisical, cavalier, reckless, or in the very least, negligent.

67. In all contexts, time has constantly been recognized as compensable, and for many people, it is the basis on which they are compensated. Plaintiff and Class Members should be sparing having to deal with the consequences of Einstein's misfeasance.

68. Once PHI is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[29]

69. Einstein's delay in identifying and reporting the Data Breach caused additional harm to Plaintiff and Class Members. Although their PHI was improperly exposed as early as August 5, 2020, Plaintiff was not notified of the Data Breach until January 21, 2021, depriving her of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

70. As a result of a result of Einstein's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at increased risk of suffering:

a. Actual identity theft;

[29] *2014 LexisNexis True Cost of Fraud Study, available at:* https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last accessed Apr. 19, 2021).

b. Unauthorized use and misuse of their PHI;

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

d. The diminution in value of their PHI;

e. The compromise, publication, and/or theft of their PHI;

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

g. Lost opportunity costs and lost wages associated with effort 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;

h. Costs associated with placing freezes on credit reports;

i. Delay in receipt of tax refund monies;

j. The diminished value of Einstein's goods and services they received;

k. Lost opportunity and benefits of electronically filing of income tax returns;

l. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PHI being placed in the hands of criminals;

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

n. 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 Class Members.

H. Einstein's Conduct Violates HIPAA

71. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

72. Einstein's Data Breach resulted from a combination of insufficiencies that indicate Einstein failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from Einstein's Data Breach that Einstein either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Plaintiff's and Class Members' PHI

73. Plaintiffs' and Class Members' Personal and Medical Information is "protected health information" as defined by 45 CFR § 160.103.

74. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

75. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

76. Plaintiffs' and Class Members' Personal and Medical Information is "unsecured protected health information" as defined by 45 CFR § 164.402.

77. Plaintiffs' and Class Members' unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

78. Based upon the breach notification letter, Einstein reasonably believes Plaintiffs' and Class Members' unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

79. Plaintiffs' and Class Members' unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

80. Einstein reasonably believes Plaintiffs' and Class Members' unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

81. Plaintiffs' and Class Members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

82. Plaintiffs' and Class Members' unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

83. Einstein reasonably believes Plaintiffs' and Class Members' unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

84. It is reasonable to infer that Plaintiffs' and Class Members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

85. It should be rebuttably presumed that unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

86. After receiving notice that they were victims of a data breach that required the filing of a Breach Report in accordance with 45 CFR § 164.408(a), it is reasonable for recipients of that notice, including Plaintiffs and Class Members in this case, to believe that future harm (including identity theft) is real and imminent, and to take steps to mitigate that risk of future harm.

87. In addition, Einstein's Data Breach could have been prevented if Einstein implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its patients.

88. Einstein's security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Einstein creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only

to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

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

g. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

h. Failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

i. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 CFR 164.306(a)(94);

j. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq.*

89. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Einstin to provide notice of the breach to each affected individual "without unreasonable delay

and ***in no case later than 60 days following discovery of the breach***."[30]

90. Because Einstein has failed to comply with industry standards, while monetary relief may cure some of Plaintiff's and Class Members' injuries, injunctive relief is necessary to ensure Einstein's approach to information security is adequate and appropriate. Einstein still maintains the protected health information and other sensitive information of Plaintiff and Class Members; and without the supervision of the Court via injunctive relief, Plaintiff and Class Members' PHI remains at risk of subsequent Data Breaches.

I. Einstein Failed to Comply with FTC Guidelines

91. Einstein was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

92. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[31]

93. In 2016, the FTC updated its publication, *Protecting Personal Information: A*

[30] Breach Notification Rule, U.S. Dep't of Health & Human Services, *available at*: hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added) (last visited Apr. 18, 2021).

[31] Federal Trade Commission, *Start With Security: A Guide for Business*, *available at:* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Apr. 19, 2021).

Guide for Business, which established cybersecurity guidelines for businesses.[32] 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 to correct any security problems.

94. The FTC further recommends that companies not maintain PHI longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[33]

95. 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.

96. Einstein failed to properly implement basic data security practices. Einstein's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

---

[32] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, *available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Apr. 17, 2021).

[33] FTC, *Start With Security*, *supra* note 16.

97. Einstein was at all times fully aware of its obligation to protect the PHI of patients because of its position as a leading healthcare provider. Einstein was also aware of the significant repercussions that would result from its failure to do so.

CLASS ACTION ALLEGATIONS

98. Plaintiff brings this suit as a class action on behalf of herself and on behalf of all others similarly situated pursuant to Rules 1701-1706 of the Pennsylvania Rules of Civil Procedure.

99. The Class that Plaintiffs seek to represent is defined as follows:

> **All individuals whose PHI was compromised in the Einstein Healthcare Network Data Breach which occurred in August 2020.**

100. Excluded from the Class are the officers, directors, and legal representatives of Einstein, and the judges and court personnel in this case and any members of their immediate families.

101. Plaintiff reserves the right to modify or amend the definition of the proposed Class as additional information becomes available to plaintiff.

102. Numerosity.: The Class Members are so numerous that joinder of all Members is impractical. In its initial report to the U.S. Department of Health and Human Services - Office for Civil Rights, Einstein attested that the Data Breach affected at least 353,616 patients. Einstein has sent additional Notification Letters to Plaintiff and Class Members since its report to the OCR on October 9, 2020, thus the actual number of affected patients may be exponentially higher.

103. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether and to what extent Defendant had a duty to protect the PHI of Class Members;

b. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PHI;

c. Whether Defendant had duties not to disclose the PHI of Class Members to unauthorized third parties;

d. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class Members' PHI;

e. Whether Defendant failed to adequately safeguard the PHI of Class Members;

f. Whether Defendant breached its duties to exercise reasonable care in handling Plaintiff's' and Class Members' PHI by storing that information in employee email accounts;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether implied or express contracts existed between Defendant, on the one hand, and Plaintiff and Class Members on the other;

i. Whether Defendant had respective duties not to use the PHI of Class Members for non-business purposes;

j. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PHI had been compromised;

k. Whether Plaintiff and Class Members are entitled to actual, damages, statutory damages, and/or punitive damages as a result of Defendant's wrongful conduct;

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

p. 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; and

q. Whether Plaintiff and Class Members are entitled to identity theft protection for their respective lifetimes.

104. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PHI, like that of every other Class Member, was disclosed by Einstein. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Members of the Class were injured through the common misconduct of Einstein. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

105. Policies Generally Applicable to the Class. This class action is also appropriate for certification because Einstein has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members, and making final injunctive relief appropriate with respect to the Class as a whole. Einstein's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Einstein's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

106. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Class in that she has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic

or adverse to the Members of the Class and the infringement of the rights and the damages she has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex consumer class action litigation and in particular privacy class litigation, and Plaintiff intends to prosecute this action vigorously.

107. Superiority of Class Action. The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against large corporations, like Einstein. Further, even for those class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

108. The nature of this action and the nature of laws available to Plaintiff and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and the Class for the wrongs alleged because Einstein would necessarily gain an unconscionable advantage since Einstein would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action

alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

109. The litigation of the claims brought herein is manageable. Einstein's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

110. Adequate notice can be given to Class Members directly using information maintained in Einstein's records.

111. Unless a Class-wide injunction is issued, Einstein may continue in its failure to properly secure the PHI of Class Members, Einstein may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Einstein may continue to act unlawfully as set forth in this Complaint.

112. Further, Einstein has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under the Federal Rules of Civil Procedure.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

113. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs .

114. As a condition of their utilizing the services of Einstein, patients were obligated to provide Einstein with certain PHI, including their dates of birth, Social Security numbers, personal medical information, and other protected health information.

115. Plaintiff and the Class Members entrusted their PHI to Einstein on the premise and

with the understanding that Einstein would safeguard their information, use their PHI for business purposes only, and/or not disclose their PHI to unauthorized third parties.

116. Einstein has full knowledge of the sensitivity of PHI and the types of harm that Plaintiff and Class Members could and would suffer if PHI was wrongfully disclosed.

117. Einstein knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of patients' PHI involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

118. Einstein had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Einstein's security protocols to ensure that Plaintiff's and Class Members' information in Einstein's possession was adequately secured and protected, and that employees tasked with maintaining such information were adequately trained on security measures regarding the security of patients' personal and medical information.

119. Einstein had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' PHI.

120. Additionally, violations of statutes which establish a duty to take precautions to protect a particular class of persons from a particular injury or type of injury may constitute negligence *per se.*

121. 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 businesses, such as Einstein, of failing to use reasonable measures to protect PHI. The FTC publications and orders described above also form part of the basis of Einstein's duty in this regard.

122. Einstein violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and Class Members' PHI and not complying with applicable industry standards, as described in detail herein. Einstein's conduct was particularly unreasonable given the nature and amount of PHI they obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class Members.

123. Einstein's violation of Section 5 of the FTC Act constitutes negligence *per se.*

124. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

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

126. Einstein's violation of HIPAA also independently constitutes negligence *per se*.

127. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of patients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

128. Plaintiff and Class Members are within the class of persons that HIPAA privacy laws were intended to protect.

129. The harm that occurred as a result of the Data Breach is the type of harm HIPAA privacy laws were intended to guard against.

130. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class Members was reasonably foreseeable, particularly in light of the growing amount of data breaches for health care providers and other industries.

131. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Einstein knew or should have known of the inherent risks in collecting and storing the PHI of Plaintiff and the Class, the critical importance of providing adequate security of that PHI, and that it had inadequate employee training and education and IT security protocols in place to secure the PHI of Plaintiff and the Class.

132. Einstein's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Einstein's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Einstein's misconduct also included its decisions not to comply with industry standards for the safekeeping and unauthorized disclosure of the PHI of Plaintiff and Class Members.

133. Plaintiff and the Class Members had no ability to protect their PHI that was in Einstein's possession.

134. Einstein was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

135. Einstein had and continues to have a duty to adequately disclose that the PHI of Plaintiff and Class Members within Einstein's possession might have been compromised, how it was compromised, and precisely the types of information that were compromised and when. Such notice was necessary to allow Plaintiff and the Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PHI by third parties.

136. Einstein has admitted that the PHI of Plaintiffs and Class Members was wrongfully

disclosed to unauthorized third persons as a result of the Data Breach.

137. Einstein, through its actions and/or omissions, unlawfully breached einstein's duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PHI of Plaintiff and Class Members during the time the PHI was within Einstein's possession or control.

138. Einstein improperly and inadequately safeguarded the PHI of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

139. Einstein failed to heed industry warnings and alerts to provide adequate safeguards to protect patients' PHI in the face of increased risk of theft.

140. Einstein, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its patients' PHI.

141. Einstein, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

142. But for Einstein's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the PHI of Plaintiff and Class Members would not have been compromised.

143. There is a close causal connection between Einstein's failure to implement security measures to protect the PHI of current and former patients and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and Class Members' PHI was accessed as the proximate result of Einstein's failure to exercise reasonable care in safeguarding such PHI by adopting, implementing, and maintaining appropriate security measures.

144. As a direct and proximate result of Einstein's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PHI is used; (iii) the compromise, publication, and/or theft of their PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI; (v) 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 tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PHI, which remain in Einstein's possession and is subject to further unauthorized disclosures so long as Einstein fails to undertake appropriate and adequate measures to protect the PHI of patients and former patients in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of Einstein's goods and services Plaintiff and Class Members received.

145. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

SECOND CAUSE OF ACTION
Breach of Contract
(On Behalf of Plaintiff and the Class)

146. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs .

147. As a healthcare provider, Einstein entered into contracts with Plaintifs and Class Members.

148. The promises and representations described above relating to HIPAA and other industry practices, and about Einstein's purported concern about its patients' privacy rights became terms of the contract between Einstein and its patients, including Plaintiff and Class Members.

149. Einstein breached these promises by failing to comply with HIPAA and other reasonable industry practices.

150. Plaintiff and Class Members fully performed their obligations under the contracts with Einstein. Einstein breached its agreements with Plaintiff and Class Members by failing to protect their PHI. Specifically, Einstein: (1) failed to take reasonable steps to use safe and secure systems to protect PHI; (2) failed to have appropriate security protocols and measures in place; (3) allowed unauthorized third parties to gain access to patients' PHI; and (4) failed to promptly alert or give notice of the Data Breach to Plaintiff and Class Members.

151. As a result of Einstein's breach of these terms, Plaintiff and Class Members have been harmed and put at risk of future harm.

152. Plaintiff and Class Members are therefore entitled to damages, including restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and attorney fees, costs, and expenses.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

153. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs .

154. Plaintiff and Class Members were required to provide their PHI, including names, Social Security numbers, dates of birth, medical histories, and other personal information to Einstein as a condition of their use of Einstein's services.

155. Plaintiff and Class Members paid money to Einstein in exchange for goods and services, as well as Einstein's promises to protect PHI from unauthorized disclosure.

156. In its written privacy policy, Defendant expressly promised Plaintiff and Class Members that Defendant would only disclose protected health information and sensitive information under certain circumstances, none of which relate to the Data Breach.

157. Defendant promised to comply with HIPAA standards and to make sure that Plaintiff's and Class Members' protected health information would remain protected.

158. Implicit in the agreement between Einstein's patients, including Plaintiff and Class Members, to provide PHI, and Einstein's acceptance of such PHI, was Einstein's obligation to use the PHI of its patients for business purposes only, take reasonable steps to secure and safeguard that PHI, and not make unauthorized disclosures of the PHI to unauthorized third parties.

159. Further, implicit in the agreement, Einstein was obligated to provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their protected health information and other PHI.

160. Without such implied contracts, Plaintiff and Class Members would not have provided their PHI to Einstein.

161. Einstein had an implied duty to reasonably safeguard and protect the PHI of Plaintiff and Class Members from unauthorized disclosure or uses.

162. Additionally, Einstein implicitly promised to retain this PHI only under conditions that kept such information secure and confidential.

163. Plaintiff and Class Members fully performed their obligations under the implied contract with Einstein; however, Einstein did not.

164. Einstein breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff and Class Members' PHI, which was compromised as a result of the Data Breach.

165. Einstein further breached the implied contracts with Plaintiff and Class Members by failing to comply with its promise to abide by HIPAA.

166. Einstein further breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Einstein created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1).

167. Einstein further breached the implied contracts with Plaintiff and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).

168. Einstein further breached the implied contracts with Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1).

169. Einstein further breached the implied contracts with Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii).

170. Einstein further breached the implied contracts with Plaintiff and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity

of electronic protected health information in violation of 45 CFR 164.306(a)(2).

171. Einstein further breached the implied contracts with Plaintiff and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3).

172. Einstein further breached the implied contracts with Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations in violation of 45 CFR 164.306(a)(94).

173. Einstein further breached the implied contracts with Plaintiff and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq*.

174. Einstein further breached the implied contracts with Plaintiff and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c).

175. Einstein further breached the implied contracts with Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' PHI.

176. Einstein's failures to meet these promises constitute breaches of the implied contracts.

177. Because Einstein allowed unauthorized access to Plaintiff's and Class Members' PHI and failed to safeguard the PHI, Einstein breached its contracts with Plaintiffs and Class Members.

178. A meeting of the minds occurred, as Plaintiff and Class Members agreed, *inter alia*,

to provide accurate and complete PHI and to pay Einstein in exchange for Einstein's agreement to, *inter alia*, protect their PHI.

179. Einstein breached its contracts by not meeting the minimum level of protection of Plaintiff's and Class Members' PHI, because Defendant did not prevent against the breach of over 300,000 patients' PHI.

180. Furthermore, the failure to meet its confidentiality and privacy obligations resulted in Einstein providing goods and services to Plaintiff and Class Members that were of a diminished value.

181. As a direct and proximate result of Einstein's breach of its implied contracts with Plaintiff and Class Members, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PHI is used; (iii) the compromise, publication, and/or theft of their PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI; (v) 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 tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PHI, which remain in Einstein's possession and is subject to further unauthorized disclosures so long as Einstein fails to undertake appropriate and adequate measures to protect the PHI of customers/patients and former customers/patients in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value

of Einstein's goods and services they received.

182. As a direct and proximate result of Einstein's breach of its implied contracts with Plaintiff and Class Members, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

FOURTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

183. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs.

184. In light of the special relationship between Einstein and its patients, whereby Einstein became a guardian of Plaintiff's and Class Members' highly sensitive, confidential, personal, financial information, and other PHI, Einstein was a fiduciary, created by its undertaking and guardianship of the PHI, to act primarily for the benefit of its patients, including Plaintiff and Class Members, for: (1) the safeguarding of Plaintiff's and Class Members' PHI; (2) timely notifying Plaintiff and Class Members of a data breach or disclosure; and (3) maintaining complete and accurate records of what and where Einstein's patients' information was and is stored.

185. Einstein had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its patients' relationship, in particular to keep secure the PHI of its patients.

186. Einstein breached its fiduciary duties to Plaintiff and Class Members by failing to diligently investigate the Data Breach to determine the number of Members affected in a reasonable and practicable period of time.

187. Einstein breached its fiduciary duties to Plaintiff and Class Members by failing to

protect Plaintiff's and Class Members' PHI.

188. Einstein breached its fiduciary duties to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

189. Einstein breached its fiduciary duties to Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Einstein created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

190. Einstein breached its fiduciary duties to Plaintiff and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).

191. Einstein breached its fiduciary duties to Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

192. Einstein breached its fiduciary duties to Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii).

193. Einstein breached its fiduciary duties to Plaintiff and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

194. Einstein breached its fiduciary duties to Plaintiff and Class Members by failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health

information in violation of 45 CFR 164.306(a)(3).

195. Einstein breached its fiduciary duties to Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 CFR 164.306(a)(94).

196. Einstein breached its fiduciary duties to Plaintiff and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq.*

197. Einstein breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' PHI.

198. As a direct and proximate result of Einstein's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PHI is used; (iii) the compromise, publication, and/or theft of their PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI; (v) 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 tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PHI, which remain in Einstein's possession and is subject to further unauthorized disclosures so long as Einstein fails to undertake appropriate and adequate measures to protect the PHI of customers/patients and former customers/patients in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PHI compromised as a result of the Data Breach for the remainder of the

lives of Plaintiff and Class Members; and (ix) the diminished value of Einstein's goods and services they received.

199. As a direct and proximate result of Einstein's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

FIFTH CAUSE OF ACTION
INJUNCTIVE/DECLARATORY RELIEF
(On Behalf of Plaintiff and the Class)

200. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs .

201. This cause of action is brought under the Pennsylvania Declaratory Judgments Act, 42 Pa.C.S.A. § 7531.

202. As previously alleged, Plaintiff and Class Members entered into a contract that required Einstein to provide adequate security for the PHI they collected from Plaintiff and Class Members.

203. Einstein owes a duty of care to Plaintiffs and Class Members requiring them to adequately secure PHI.

204. Einstein still possesses Plaintiff's and Class Members' PHI.

205. Since the Data Breach, Einstein has announced no specific changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent further attacks.

206. Einstein has not satisfied its contractual obligations and legal duties to Plaintiff and Class Members. In fact, now that Einstein's insufficient data security is known to hackers, the PHI in Einstein's possession is even more vulnerable to cyberattack.

207. Actual harm has arisen in the wake of the Data Breach regarding Einstein's contractual obligations and duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their PHI and Einstein's failure to address the security failings that lead to such exposure.

208. There is no reason to believe that Einstein's security measures are any more adequate now than they were before the Data Breach to meet Einstein's contractual obligations and legal duties.

209. Plaintiffs, therefore, seek a declaration (1) that Einstein's existing security measures do not comply with their contractual obligations and duties of care to provide adequate security, and (2) that to comply with their contractual obligations and duties of care, Einstein must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;
c. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment patient data by, among other things, creating firewalls and access controls so that if one area of Defendant's system is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner patient data not necessary for its provisions of services;

f. Ordering that Defendant conduct regular computer system scanning and security checks;

g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Defendant to meaningfully educate its current, former, and prospective patients about the threats it faces as a result of the loss of their PHI to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

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

a. For an Order certifying the Class as defined herein, and appointing Plaintiff and her Counsel to represent the Class;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' PHI, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

c. For equitable relief compelling Defendant to use appropriate cyber security methods and policies with respect to PHI collection, storage, and protection, and to disclose with specificity to Class Members the type of PHI compromised;

d. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

e. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

f. For prejudgment interest on all amounts awarded; and

g. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

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

Respectfully submitted,
MORGAN & MORGAN
PHILADELPHIA PLLC

BY: /s/ Clancy Boylan
CLANCY BOYLAN, ESQUIRE

Date: April 23, 2021

LINDA P. NUSSBAUM*
BART D. COHEN (PA Bar 57606)
NUSSBAUM LAW GROUP, P.C.
1211 Avenue of the Americas, 40th Fl.
New York, NY 10036
Telephone: (917) 438-9102
Facsimile: (212) 753-0396
lnussbaum@nussbaumpc.com
bcohen@nussbaumpc.com

JEAN S. MARTIN*
FRANCESCA KESTER (PA Bar No. 324523)
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402
jeanmartin@forthepeople.com
fkester@forthepeople.com

MICHAEL E. CRIDEN
CRIDEN & LOVE, P.A.
7301 SW 57th Court, Suite 515
South Miami, FL 33143
Telephone: (305) 357-9000
Facsimile: (305) 357-9050
mcriden@cridenlove.com

* *Pro Hac Vice applications to be submitted*

Attorneys for Plaintiff and the Proposed Class

VERIFICATION

I, Nanette Katz, hereby verify that I am the plaintiff in the foregoing action; that the attached Complaint in Civil Action is based upon information which I have furnished to counsel, and information which has been gathered by counsel in the preparation of the lawsuit. The language of the Complaint is that of counsel and not mine. I have read the Complaint, and to the extent the statements therein are based upon information I have given counsel, they are true and correct to the best of my knowledge, information and belief. To the extent the contents of the Complaint are that of counsel, I have relied upon counsel in making this Verification. I understand that if false statements were made herein I would be subject to the penalties of 18 Pa. C.S.A. §4904 relating to unsworn falsification to authorities.

By: Nanette Katz

Nanette Katz

DATE: 4-21-21

EXHIBIT “A”

Einstein
HEALTHCARE NETWORK

Return mail will be processed by: IBC
PO Box 847, Holbrook, NY 11741

Nanette Katz
[redacted]

9

January 21, 2021

Dear Nanette Katz,

Einstein Healthcare Network is committed to maintaining the privacy and security of our patients' information. Regrettably, we are writing to inform you that we recently identified and addressed a security incident that may have involved some of your information.

On August 10, 2020, we identified suspicious activity within a limited number of Einstein employees' email accounts. We immediately took steps to secure the email accounts and a leading computer forensic firm was engaged to assist with our investigation. The investigation indicated that an unauthorized person gained access to the employee email accounts between August 5, 2020 and August 17, 2020. The investigation was unable to determine whether the unauthorized person actually viewed any emails or attachments in the email accounts. Out of an abundance of caution, we reviewed the contents of the email accounts to identify patient information that was contained in the email accounts. As a result of that review, we identified one or more emails and/or attachments that may have included your name, date of birth, medical record or patient account number, health insurance information, and/or treatment or clinical information, such as diagnosis, medications, provider, type of treatment, or treatment location.

There is no evidence that any of your information was actually viewed by the unauthorized person, or that it has been misused. However, we wanted to notify you of this incident and assure you we take this very seriously. As a precaution, we recommend that you review statements you receive from your health insurer or healthcare provider. If you see charges for services you did not receive, please contact the insurer or provider immediately.

We deeply regret any concern or inconvenience this incident may cause you. To help prevent something like this from happening in the future, we reinforced education with our staff regarding how to identify and avoid suspicious emails and are making additional security enhancements to our email environment. If you have any questions, please call us at **1-833-689-1142**, Monday through Friday, between 9:00 a.m. and 7:00 p.m. Eastern Time.

Sincerely,

D. Crump

Derrick Crump
Chief Privacy Officer

ALBE-ADT-NOCM-P2