UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF PENNSYLVANIA

AMBER NICKEY, individually, on behalf of herself and on behalf of A.N., a minor, and on behalf of all others similarly situated, Plaintiffs, v. KEYSTONE HEALTH, Defendant.	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Amber Nickey, individually ("Plaintiff") and on behalf of A.N., a minor, ("Minor Plaintiff") brings this Class Action Complaint on behalf of herself, A.N. and all others similarly situated, against Defendant, Keystone Health ("Keystone" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to him, which are based on personal knowledge:

NATURE OF THE CASE

1. Healthcare providers that handle sensitive, personally identifying information ("PII") or protected health information ("PHI") owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of PII or PHI to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private health matters.

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

and money to closely monitor their credit, financial accounts, health records, and email accounts, and take a number of additional prophylactic measures.

3. As a healthcare provider, Keystone is required by law to provide every patient with a Notice of Privacy Practices. In its Notice of Privacy, Keystone states that it is "required by law to maintain the privacy and security of your protected health information" and that "We will let you know promptly if a breach occurs that may have compromised the privacy and security of your information."[1]

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

5. Plaintiff brings this class action on behalf of individual patients of Keystone whose PII and/or PHI was accessed and exposed to unauthorized third parties during a data breach of Keystone's computer systems (the "Data Breach").

6. For the duration of time between July 28, 2022 and August 19, 2022, the bad actor(s) had unrestricted access to all PII and PHI in certain Keystone computer systems.

7. Keystone did not announce the Data Breach publicly until October 14, 2022, and only began sending out Data Breach notification letters to Plaintiff and class members during that same time period. A copy of the Notice Letter received by Plaintiff is attached hereto at Exhibit "A." A redacted copy of the Notice Letter received by A.N. is attached hereto at Exhibit "B."

8. Plaintiff, on behalf of herself, A.N. and the Class as defined herein, brings claims for negligence, negligence *per se*, breach of implied contract, breach of fiduciary duty, and declaratory judgment, seeking actual and putative damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

9. Based on the public statements of Keystone to date, a wide variety of PII and PHI was implicated in the breach, including, but not limited to: names, social security numbers, dates

[1] Keystone Health, Notice of Privacy Practices, https://keystonehealth.org/wp-content/uploads/2019/01/notice-of-privacy-practices-January-2019.pdf (last visited Oct. 21, 2022).

of birth, and/or treatment or clinical information, such as diagnosis, medications, provider, type of treatment, or treatment locations.

10. As a direct and proximate result of Keystone's inadequate data security, and its breach of its duty to handle PII and PHI with reasonable care, and its failure to maintain the required confidentiality of patients' medical records, Plaintiff 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 Keystone for these harms, Plaintiff and the Class seek remedies including damages for out of pocket costs in an amount to be determined at trial, declaratory judgment, and injunctive relief requiring Keystone to, at minimum: 1) disclose, expeditiously, the full nature of the Data Breach and the types of PII and PHI accessed, obtained, or exposed by the hackers; 2) implement improved data security practices to reasonably guard against future breaches of PII and PHI possessed by Keystone; and 3) provide, at its own expense, all impacted victims with lifetime identity theft protection services.

PARTIES

13. At all material times, Plaintiffs have been citizens and residents of Cumberland County in the Commonwealth of Pennsylvania.

14. Plaintiff Amber Nickey was a patient of Defendant's, receiving medical services from Defendant in Shippensburg and Chambersburg and other locations through her primary care physician, WellSpan Urgent Care and Chambersburg Hospital among others. All of Ms. Nickey's medical records were maintained by the Defendant.

15. A.N. was a patient of Defendant's, receiving various medical services from Defendant in Chambersburg and other locations through a primary care physician and other health care service locations. All of A.N.'s medical records were maintained by the Defendant.

16. Plaintiff and A.N. received a written notification from Defendant dated October 14, 2022 informing Plaintiff and A.N. that their PII and PHI may have been accessed or exposed to unknown, unauthorized third parties during the Data Breach. *See* Exhibits "A" and "B."

17. Defendant Keystone is a nonprofit corporation and healthcare provider headquartered in Franklin County, Pennsylvania. Its principal place of business is located at 111 Chambers Hill Dr., Chambersburg, PA 17201.

JURISDICTION AND VENUE

18. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

19. This Court has personal jurisdiction over Defendant because it is headquartered in and is a citizen of the Commonwealth of Pennsylvania.

20. Venue is proper in this District, pursuant to 28 U.S.C. § 1391(b)(1), because a substantial part of the acts, omissions, and events giving rise to Plaintiff's claims occurred in this District. Further, Defendant resides in this District and is a resident of Pennsylvania.

FACTUAL BACKGROUND

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

21. At all relevant times, Keystone knew it was storing and permitting its employees to use internet accessible email accounts to transmit, valuable, sensitive PII and PHI and that, as a result, Keystone's systems would be attractive targets for cybercriminals.

22. Keystone 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.

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

24. 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."[2] 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.

25. 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 U.S. According to the IRTC, in 2019, there were 1,473 reported data breaches in the United States, exposing 164 million sensitive records and 705 million "non-sensitive" records.[3]

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 2021, there was a 68 percent increase in the number of data compromises reported in the U.S., compared to 2020. Similarly, there was a record 847,376 complaints of cyber-crime reported to the FBI, a seven percent increase

[2] 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/ (last visited 11/16/2022).

[3] *Data Breach Reports: 2019 End of Year Report*, IDENTITY THEFT RESOURCE CENTER, at 2, *available at* https://notified.idtheftcenter.org/s/resource#annualReportSection (last visited 11/16/2022).

over 2020. In addition, forty-seven percent of Americans experienced financial identity theft in 2020. The cost of the average data breach rose from $3.86 million in 2020 to $.24 million in 2021.[4]

26. 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."[5]

27. "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."[6]

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

29. As indicated by Jim Trainor, formerly 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."[7] A complete identity theft kit that includes health insurance

[4] 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) (last visited 11/16/2022).

[5] https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited 11/16/2022).

[6] *Id.*

[7] 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 (last visited 11/16/2002).

credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[8]

30. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> 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.[9]

31. 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.**"[10]

32. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that

---

[8] 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 (last visited 11/16/2002).

[9] 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/ (last visited 11/16/2002).

[10] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited 11/16/2002).

attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[11]

33. 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.

B. Keystone Breached its Duty to Protect its Patients PII and PHI

34. On July 28, 2022, one or more malicious actors gained access to Defendant's computer network and systems.

35. The actor(s) had access to Defendant's computer network and systems from July 28, 2022, to August 19, 2022.

36. On or around August 19, 2022, Defendant became aware of the Data Breach because some of its computer systems were shut down for a period of time.

37. In response, Defendant launched an investigation, which concluded at an unknown date before October 14, 2022.

38. The investigation found the Data Breach resulted in the malicious actor(s) copying and exfiltrating substantial amounts of patient PII and PHI.

39. Specifically, the malicious actor(s) took files containing patient names, Social Security Numbers, and records regarding patient care with Defendant.

40. On or about October 14, 2022, Defendant ultimately admitted to the Data Breach and began notifying the 235,237 individuals, including Plaintiff and members of the proposed Class. *See, e.g.*, Exhibits "A" and "B" attached hereto.

[11] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited 11/16/2002).

41. On or about the same day, Defendant publicly acknowledged the data security incident to the United States Department of Health and Human Services' Office for Civil Rights ("DHHS"). In its Notice, Defendant admitted the details of the Data Breach.

42. Defendant identified only the following actions it undertook to mitigate and remediate the harm caused by the Data Breach in its Notice Letter: "Keystone is mailing letters to affected patients and offering credit monitoring services to those who are eligible."

43. Defendant recognized the substantial and high likelihood that Plaintiff and the proposed Class's PII and PHI would be misused following the Data Breach, stating: "We value the trust our community places in Keystone Health, and we deeply regret any concern this may cause our patients and their families. To help prevent something like this from happening again, we are implementing new network security measures and providing additional training to our employees."

44. Given that Defendant was storing the PII and PHI of Plaintiff, A.N. and the Class and knew or should have known of the serious risk and harm caused by a data breach, Defendant was obligated to implement reasonable measures to prevent and detect cyber-attacks, such as those recommended by the Federal Trade Commission, required by the Health Insurance Portability and Accountability Act, and promoted by data security experts and other agencies.

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

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

C. Plaintiff, A.N. and Class Members Suffered Damages

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

48. For example, Plaintiff and A.N. have already suffered and will continue to suffer lost personal time spent reviewing credit reports and checking medical billing and statements from health insurers and/or providers, as was specifically directed to do by Keystone as a result of the Data Breach. *See* Exhibits "A" and "B".

49. 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, A.N. and Class members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Keystone's conduct. Further, the value of Plaintiff, A.N. and Class members' PII and PHI has been diminished by its exposure in the Data Breach.

50. As a result of Keystone's failures, Plaintiff, A.N. and Class members are at substantial increased risk of suffering identity theft and fraud or misuse of their PII and PHI.

51. 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%.[12]

[12] https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last visited 11/16/2022).

52. 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."[13]

53. "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."[14]

54. 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."[15]

55. 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.[16]

56. "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."[17]

57. Plaintiff, A.N. and the Class members have also been injured by Keystone's unauthorized disclosure of their confidential and private medical records.

58. Plaintiff, A.N. and Class members are also at a continued risk because their information remains in Keystone's systems, which have already been shown to be susceptible to

---

[13] https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud (last visited 11/16/2022).

[14] *Id.*

[15] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited 11/16/2022).

[16] *Id.*

[17] https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited 11/16/2022) .

compromise and attack and is subject to further attack so long as Keystone fails to undertake the necessary and appropriate security and training measures to protect its patients' PII and PHI.

CLASS ALLEGATIONS

59. Plaintiff and A.N. bring this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following classes:

Nationwide Classes

> All individuals in the United States whose PII and/or PHI was compromised in the Keystone data breach which occurred starting in July 2022 (the "Nationwide Class").
>
> All minor individuals as of the date of this filing in the United States whose PII and/or PHI was compromised in the Keystone data breach which occurred starting in July 2022 (the "Nationwide Minor Class").

Pennsylvania Sub-Classes

> All individuals in the Commonwealth of Pennsylvania whose PII and/or PHI was compromised in the Keystone data breach which occurred starting in July 2022 (the "Pennsylvania Sub-Class").
>
> All minor individuals as of the date of this filing in the Commonwealth of Pennsylvania whose PII and/or PHI was compromised in the Keystone data breach which occurred starting in July 2022 (the "Pennsylvania Minor Sub-Class").

60. 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.

61. Plaintiff reserves the right to modify or amend the definition of the proposed Classes prior to moving for class certification.

62. The requirements of Rule 23(a)(1) are satisfied. The class described above is so numerous that joinder of all individual members in one action would be impracticable. 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, but based on public information, the Class includes over two hundred thousand individuals.

63. The requirements of Rule 23(a)(2) are satisfied. There is a well-defined community of interest, and there are common questions of fact and law affecting members of the Class. The questions of fact and law common to the Class predominate over questions which may affect individual members and include the following:

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

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

c. Whether Defendant breached its obligation to maintain Plaintiff, A.N. and the Class members' medical information in confidence.

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

e. Whether Defendant breached its fiduciary duty to Plaintiff, A.N. and the Class.

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

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

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

64. The requirements of Rule 23(a)(3) are satisfied. Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff, A.N. 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.

65. Plaintiff, A.N. and members of the Class were all patients or employees of Keystone, each having their PII and PHI obtained by an unauthorized third party.

66. The requirements of Rule 23(a)(4) are satisfied. Plaintiff, individually and in her representative capacity for A.N., is an adequate representative of the Class because her interests do not conflict with the interests of the members of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the members of the Classes and has no interests antagonistic to the members of the Classes. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff, A.N. and the Class members are substantially identical as explained above.

67. The requirements of Rule 23(b)(3) are satisfied here because a class action is the superior method of litigation for these issues, and common issues will predominate. While the aggregate damages that may be awarded to the members of the Class are likely to be substantial, the damages suffered by the individual members of the Class are relatively small. As a result, the expense and burden of individual litigation make it economically infeasible and procedurally impracticable for each member of the Class to individually seek redress for the wrongs done to them. Certifying the case as a Class will centralize these substantially identical claims in a single proceeding, which is the most manageable litigation method available to Plaintiff, A.N. and the Class and will conserve the resources of the parties and the court system, while protecting the rights of each member of the Class. Defendant's uniform conduct is generally applicable to the Class as a whole, making relief appropriate with respect to each Class member.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff, A.N. and Nationwide Classes, or alternatively, Pennsylvania Sub-Classes)

68. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

69. Keystone owed a duty under common law to Plaintiff, A.N. 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.

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

71. Keystone had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff, A.N. 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, Keystone was obligated to act with reasonable care to protect against these foreseeable threats.

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

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

74. Keystone 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. Keystone'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.

75. Keystone's violation of Section 5 of the FTC Act constitutes negligence *per se*.

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

77. Keystone is an entity covered under the Health Insurance Portability and Accountability Act ("HIPAA"), which sets minimum federal standards for privacy and security of PHI.

78. Pursuant to HIPAA, 42 U.S.C. § 1302d, *et. seq.*, and its implementing regulations, Keystone had a duty to implement and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect electronic PHI.

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

80. HIPAA also requires Keystone to provide Plaintiff, A.N. and the Class members with notice of any breach of their individually identifiable PHI "without unreasonable delay and in no case later than 60 calendar days after discovery of the breach." 45 CFR §§ 164.400-414.

81. Keystone violated HIPAA by actively disclosing electronic PHI; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PHI; and by failing to provide Plaintiff, A.N. and Class members with timely notification of the Data Breach.

82. Plaintiff, A.N. and the Class members are patients within the class of persons HIPAA was intended to protect.

83. Keystone's violation of HIPAA constitutes negligence *per se*.

84. Pursuant to Pennsylvania's Policies and Procedures for Medical Records Services, 28 Pa. Code § 115.1, *et. seq*. (the "Pa. Policies"), Keystone was required to have a medical record service "properly equipped to enable its personnel to function in an effective manner and to maintain medical records so that they are readily accessible and secure from unauthorized use."

85. It was also required to train its medical record service personnel. *Id.*

86. Additionally, Keystone was required to store medical records "in such a manner as to provide protection from loss, damage and unauthorized access." *Id.*

87. Pursuant to the Pa. Policies, Keystone was required to treat "all records" (including those of the Plaintiff, A.N. and the Class members) "as confidential." *Id.*

88. Keystone violated the Pa. Policies by actively disclosing the Plaintiff, A.N. and the Class members' PHI; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PHI; and failing to maintain the confidentiality of the Plaintiff, A.N. and the Class members' records.

89. Plaintiff the Plaintiff, A.N. and the Class members are patients within the class of persons the Pa. Policies was intended to protect.

90. Keystone's violation of the Pa. Policies constitutes negligence *per se*.

91. The harm that has occurred as a result of Keystone's conduct is the type of harm that the FTC Act, HIPAA, and the Pa. Policies was intended to guard against.

92. Keystone breached the duties owed to Plaintiff the Plaintiff, A.N. and Class Members and thus was negligent and/or negligent *per se*. Keystone 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; (g) failing to follow its own privacy policies and practices published to its patients; and (h) failing to maintain the confidentiality of medical information and records.

93. But for Keystone's wrongful and negligent breach of its duties owed to the Plaintiff, A.N. and Class Members, their privacy, confidences, PII, and PHI would not have been compromised.

94. As a direct and proximate result of Keystone's negligence, Plaintiff, A.N. 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 Keystone 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 Keystone with the mutual understanding that Keystone would safeguard 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 Keystone's possession and is subject to further breaches so long as

Keystone fails to undertake appropriate and adequate measures to protect Plaintiff, A.N. and Class Members' data;

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

j. Loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received, as directed to do by Keystone.

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

SECOND CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY/CONFIDENCES
(On Behalf of Plaintiff, A.N. and Nationwide Classes, or alternatively, Pennsylvania Sub-Classes)

96. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

97. Plaintiff, A.N. and Class Members have an interest, both equitable and legal, in the PII and PHI about them that was conveyed to, collected by, and maintained by Keystone and that was ultimately accessed or compromised in the Data Breach.

98. As a healthcare provider, Keystone has a fiduciary relationship to its patients, like Plaintiff, A.N. and the Class members.

99. Because of that fiduciary and special relationship, Keystone was provided with and stored private and valuable PHI related to Plaintiff, A.N. and the Class which it was required to maintain in confidence.

100. Keystone owed a fiduciary duty under common law to Plaintiff, A.N. and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

101. As a result of the parties' relationship, Keystone had an obligation to maintain the confidentiality of the information within Plaintiff, A.N. and the Class members' medical records.

102. Patients like Plaintiff, A.N. and Class members have a privacy interest in personal medical matters, which Keystone had a fiduciary duty not to disclose medical data concerning its patients.

103. As a result of the parties' relationship, Keystone had possession and knowledge of confidential PHI and confidential medical records of Plaintiff, A.N. and Class members, information not generally known.

104. Plaintiff, A.N. and Class members did not consent to nor authorize Keystone to release or disclose their PHI to an unknown criminal actor.

105. Keystone breached the duties owed to Plaintiff, A.N. and Class Members and thus was negligent. Keystone 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; (g) failing to follow its on privacy policies and practices published to its patients; and (h) making an unauthorized and unjustified disclosure and release of Plaintiff, A.N. and Class members' PHI and medical information to a criminal third party.

106. But for Keystone's wrongful breach of its duties and confidences owed to Plaintiff, A.N. and Class Members, their privacy, confidences, PII, and PHI would not have been compromised.

107. As a direct and proximate result of Keystone's breach of its fiduciary duty, Plaintiff, A.N. 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 Keystone 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 Keystone with the mutual understanding that Keystone would safeguard Plaintiff, A.N. 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 Keystone's possession and is subject to further breaches so long as Keystone fails to undertake appropriate and adequate measures to protect Plaintiff, A.N. and Class Members' data;

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

j. The erosion of the essential and confidential relationship between Keystone – as a health care services provider – and Plaintiff, A.N. 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, as directed to do by Keystone.

108. Additionally, Keystone received payments from Plaintiff, A.N. and Class members for services with the understanding that Keystone would uphold its fiduciary responsibilities to maintain the confidences of Plaintiff, A.N. and Class members' private medical information.

109. Keystone breached the confidence of Plaintiff, A.N. and Class members when it made an unauthorized release and disclosure of their confidential medical information and/or PHI.

110. It would be inequitable for Keystone to retain the benefit at Plaintiff, A.N. and Class members' expense.

111. As a direct and proximate result of Keystone's breach of its fiduciary duty, Plaintiff, A.N. and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff, A.N. and Nationwide Classes, or alternatively, Pennsylvania Sub-Classes)

112. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

113. Plaintiff, A.N. and the Class entrusted their Private Information to Defendant. In so doing, Plaintiff, A.N. and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff, A.N. and the Class if their data had been breached and compromised or stolen.

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

115. Plaintiff, A.N. and the Class fully performed their obligations under the implied contracts with Defendant.

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

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

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

FOURTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff, A.N. and Nationwide Classes, or alternatively, Pennsylvania Sub-Classes)

119. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

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

further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

121. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff, A.N. and Class Members' PII and PHI and whether Keystone is currently maintaining data security measures adequate to protect them from further data breaches that compromise their PII and PHI. Plaintiff and A.N. allege that Keystone's data security measures remain inadequate. Keystone denies these allegations. Furthermore, Plaintiff and A.N. continue to suffer injury as a result of the compromise of PII and PHI and remains at imminent risk that further compromises of their PII and/or PHI will occur in the future.

122. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Keystone owes a legal duty to secure patients' PII and PHI and to timely notify patients of a data breach under the common law, Section 5 of the FTC Act, HIPAA, various state statutes, and the common law; and

b. Keystone continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII and PHI.

123. This Court also should issue corresponding prospective injunctive relief requiring Keystone to, at minimum 1) disclose, expeditiously, the full nature of the Data Breach and the types of PII and PHI accessed, obtained, or exposed by the hackers; 2) implement improved data security practices to reasonably guard against future breaches of PII and PHI possessed by Keystone; and 3) provide, at its own expense, all impacted victims with lifetime identity theft protection services.

124. If an injunction is not issued, Plaintiff and A.N. will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Keystone. The risk of another such breach is real, immediate, and substantial. If another breach at Keystone occurs, Plaintiff and A.N. will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

125. The hardship to Plaintiff and A.N. if an injunction does not issue exceeds the hardship to Keystone if an injunction is issued. Plaintiff and A.N. will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Keystone of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Keystone has a pre-existing legal obligation to employ such measures.

126. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Keystone, thus eliminating the additional injuries that would result to Plaintiff, A.N. and consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and on behalf of minor A.N., as well as all other similarly situated, prays for relief as follows:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff and A.N. as representatives of the Classes and Plaintiff's attorneys as Class Counsel to represent the Classes;

b. For an order finding in favor of Plaintiff, A.N. and the Classes on all counts asserted herein;

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

d. For an order of restitution, 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;

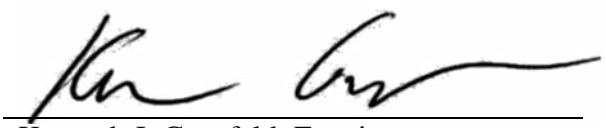
g. Awarding pre- and post-judgment interest on any amounts awarded; and

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

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Respectfully submitted,



Kenneth J. Grunfeld, Esquire
Pa. Bar No.: 84121
Kevin W. Fay, Esquire
Pa. Bar No.: 308252
GOLOMB SPIRT GRUNFELD, P.C.
1835 Market Street, Suite 2900
Philadelphia, PA 19103
Phone: (215) 985-9177
Fax: (215) 985-4169
Email: kgrunfeld@golomblegal.com
kfay@golomblegal.com

Date: November 17, 2022

Attorneys for Plaintiffs

EXHIBIT A

Keystone Health

October 14, 2022

103 1 39990 ********AUTO**5-DIGIT 17013
AMBER NICKEY
500 1ST ST
CARLISLE, PA 17013-1803

Dear Amber Nickey:

At Keystone Health, we are committed to protecting the privacy and security of our patients' information. We have a robust information security system in place. Unfortunately, no system is perfect, and we recently identified and addressed a cybersecurity incident. This letter explains the incident, measures we have taken, and some steps you may consider taking in response.

What Happened? On August 19, 2022, we identified an incident that shut down some of our computer systems for a short period of time. We took measures to contain the incident, reported it to law enforcement, and did an investigation with the help of a third-party cybersecurity firm. Our investigation found that an unauthorized party accessed our systems and took some files from our network between July 28, 2022 and August 19, 2022.

What Information Was Involved? The files contained your name, Social Security number, and records regarding your care with Keystone Health.

What We Are Doing and What You Can Do. We are offering you a free one-year membership to Experian© IdentityWorks℠ Credit 3B. This product helps find possible misuse of your personal information and provides you with credit and identity protection services focused on immediate identification and resolution of identity theft. Enrolling in this program will not affect your credit score. **For more information on Experian© IdentityWorks, including instructions to enroll in your free membership, please see the pages that follow this letter.**

We value the trust our community places in Keystone Health, and we regret any concern this incident may cause you and your family. To help prevent something like this from happening again, we are implementing new network security measures and providing additional training to our employees.

For More Information. If you have any questions about this incident, please call our Keystone Health dedicated assistance line at (855) 532-1263, Monday through Friday, 9:00 a.m. to 6:30 p.m., Eastern Standard Time, excluding major U.S. holidays. If you need help enrolling in IdentityWorks, please call Experian at (877) 288-8057.

Sincerely,

Joanne Cochran
President

ELN-15871-39990

EXHIBIT B

Keystone Health

October 14, 2022

162 1 61464 **********AUTO**5-DIGIT 17257
Parent or Guardian of
[redacted]
17257-8232

Dear Parent or Guardian of [redacted]

At Keystone Health, we are committed to protecting the privacy and security of our patients' information. We have a robust information security system in place. Unfortunately, no system is perfect, and we recently identified and addressed a cybersecurity incident. This letter explains the incident, measures we have taken, and some steps you may consider taking in response.

What Happened? On August 19, 2022, we identified an incident that shut down some of our computer systems for a short period of time. We took measures to contain the incident, reported it to law enforcement, and did an investigation with the help of a third-party cybersecurity firm. Our investigation found that an unauthorized party accessed our systems and took some files from our network between July 28, 2022 and August 19, 2022.

What Information Was Involved? The files contained your child's name, Social Security number, and records regarding your child's care with Keystone Health.

What We Are Doing and What You Can Do. We are offering your child a free one-year membership to Experian© IdentityWorks℠ Minor Plus. This product helps find possible misuse of your personal information and provides you with credit and identity protection services focused on immediate identification and resolution of identity theft. Enrolling in this program will not affect your credit score. **For more information on Experian© IdentityWorks Minor Plus, including instructions to enroll in your free membership, please see the pages that follow this letter.**

We value the trust our community places in Keystone Health, and we regret any concern this incident may cause you and your family. To help prevent something like this from happening again, we are implementing new network security measures and providing additional training to our employees.

For More Information. If you have any questions about this incident, please call our Keystone Health dedicated assistance line at (855) 532-1263, Monday through Friday, 9:00 a.m. to 6:30 p.m., Eastern Standard Time, excluding major U.S. holidays. If you need help enrolling in IdentityWorks, please call Experian at (877) 288-8057.

Sincerely,

Joanne Cochran

Joanne Cochran
President

ELN-15869-61464