UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF PENNSYLVANIA

ALEXANDRA BRAKE, individually and on behalf of her son, T.B., and all others similarly situated, Plaintiff, v. KEYSTONE RURAL HEALTH CENTER, d/b/a/ KEYSTONE HEALTH Defendant.	Case No.:

CLASS ACTION COMPLAINT

Plaintiff Alexandra Brake ("Plaintiff") individually, and on behalf of her son, T.B., and all others similarly situated, through her undersigned counsel, hereby alleges the following against Defendant Keystone Rural Health Center, d/b/a/ Keystone Health ("Keystone Health" or "Defendant"). Facts pertaining to Plaintiff and her personal experiences and circumstances are alleged based upon personal knowledge, and all other facts herein are alleged based upon information and belief, *inter alia*, the investigation of Plaintiff's counsel.

NATURE OF THE ACTION

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 based upon the parties' relationship and 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. This is a class action for damages against Keystone Health for its failure to exercise reasonable care in securing and safeguarding sensitive patient PII and/or PHI—including first and last names, Social Security numbers, dates of birth, health insurance information, personal addresses, and sensitive patient medical treatment information (collectively defined herein as "Private Information").

3. Plaintiff brings this action on behalf of similarly situated patients whose sensitive Private Information was stolen by cybercriminals in a cyber-attack on Keystone Health's systems that took place in or around July and August of 2022 and which resulted in the access and exfiltration of Private Information (the "Data Breach" or "Breach").

4. Keystone Health sent notice of the Data Breach to Plaintiff and members of the putative "Class" (defined below).

5. Plaintiff and Class members were notified of the Breach two months later, in October 2022.

6. 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. As a result of the Data Breach, Plaintiff and Class members are at imminent and substantial risk of experiencing various types of misuse of their Private Information in the coming years, including but not limited to, unauthorized access to email accounts, tax fraud, and identity theft—including medical identity theft.

7. 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 several additional prophylactic measures.

8. There has been no assurance offered by Keystone Health that all impacted Private Information or copies thereof have been recovered or destroyed.

9. Accordingly, Plaintiff asserts claims for negligence, breach of third-party beneficiary contract, breach of implied contract, breach of fiduciary duty, breach of confidences, and declaratory and injunctive relief.

PARTIES

A. Plaintiff Alexandra Brake

10. Plaintiff Alexandra Brake is a resident and citizen of Mercersburg, Pennsylvania, and brings this action in her individual capacity and on behalf of all others similarly situated.

11. Plaintiff gave birth to her son, T.B., in a hospital operated by Keystone Health. To receive medical care, she was required to give her and her son's Private Information to Keystone.

12. In maintaining her Private Information, Defendant expressly and impliedly promised to safeguard it. Defendant, however, failed to implement proper, industry-standard safeguards to protect Plaintiff's Private Information, leading to its exposure and exfiltration by cybercriminals, which cybercriminals stole the Private Information at issue with the intent to sell it and/or fraudulently misuse it for their own gain.

13. In October of 2022, Plaintiff received a notification letter from Defendant stating that her Private Information was compromised by cybercriminals.

14. She also received one on behalf of her son, stating that T.B.'s information had been compromised by cybercriminals.

15. Plaintiff, her son, and Class members have faced and will continue to face a certainly impending and substantial risk of future harms because of Defendant's ineffective data security measures, as further set forth herein. Some of these harms will include fraudulent charges,

medical procedures ordered in patients' names without their permission, targeted advertising without patient consent, social engineering efforts, and fraudulent applications for benefits in their names, leading to Class members being denied necessary loans or benefits in the future.

16. Plaintiff greatly values her privacy, and the privacy of her son, especially while receiving medical services, and would not have paid the amount that she did to receive medical services had she known that Keystone Health would negligently disclose her Private Information as it did.

B. Defendant Keystone Health

17. Keystone Health is a healthcare nonprofit based in Franklin County, Pennsylvania, and the surrounding area. It has its principal place of business at 111 Chambers Hill Dr, Chambersburg, PA, 17201. Its corporate policies, including those on data privacy, are established in and emanate from the Commonwealth of Pennsylvania.

JURISDICTION AND VENUE

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

19. The Court has personal jurisdiction over Defendant because Defendant's primary place of business is located within this District.

20. Venue is proper in this district under 28 U.S.C. § 1391(b)(1) because Defendant is incorporated in this District and therefore resides in this District pursuant to 28 U.S.C. § 1391(c)(2).

FACTS

21. In August of 2022, Defendant discovered unauthorized activity on its computer systems, which contained patients' Private Information, including names, medical treatment records, and Social Security numbers (SSNs).

22. Defendant discovered that an unauthorized actor had seized patient Private Health Information (PHI), on or around July 28 to August 19, 2022

23. In October of 2022, Plaintiff Brake received a letter from Keystone Health, addressed to the parent or guardian of T.B. The letter reads:

> 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 Are We Doing and What You Can Do.** We are offering your child a free one-year membership to Experian© IdentityWorks^{SM} 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. **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 enrolled in IdentityWorks, please call Experian at (877) 288-8057.

24. Plaintiff Brake also received a letter addressed to her directly. The letter was substantively identical, but Keystone offered her a different Experian product.

25. Defendant offered no explanation for the delay between the initial discovery of the Breach and the belated notification to affected patients – delay that resulted in Plaintiff and Class members suffering harm they otherwise could have avoided had a timely disclosure been made.

26. Defendant's notice was not just untimely but woefully deficient, failing to provide basic details, including, but not limited to, how unauthorized parties accessed its networks, whether the information was encrypted or otherwise protected, how it learned of the Data Breach, whether the Breach occurred system-wide, whether servers storing information were accessed, and how many patients were affected by the Data Breach.

27. Even worse, Keystone Health's offer to provide 12 months of credit monitoring is woefully inadequate. Credit monitoring only alerts individuals to the misuse of their information after it happens, which might not take place until years after the Data Breach. This potential future damage is especially acute with regard to T.B., whose Private Information was released before he had a chance to develop his own credit.

28. In light of the types of Private Information at issue, and the fact that the Private Information was specifically targeted by cybercriminals with the intent to steal and misuse it, it can be determined that Plaintiff's and Class members' Private Information will be offered for sale on the dark web.

29. The Data Breach occurred because Keystone Health failed to take reasonable measures to protect the Private Information it collected and stored. Among other things, Defendant failed to implement data security measures designed to prevent this attack, despite repeated warnings to the healthcare industry, insurance companies, and associated entities about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past on other healthcare providers.

30. Defendant disregarded the rights of Plaintiff and Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff and Class members' Private Information was safeguarded, failing to take available steps to prevent unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the Private Information of Plaintiff and Class members was exfiltrated through unauthorized access by an unknown, malicious cyber hacker with the intent to fraudulently misuse it. Plaintiff and Class members have a continuing interest in ensuring that their compromised Private Information is and remains safe.

A. Defendant's Privacy Promises

31. Defendant made and continues to make various promises to its patients, including Plaintiff, that it will maintain the security and privacy of their Private Information.

32. For example, Keystone Health, in its Notice of Privacy Practices (which was applicable to Plaintiff), under a bolded section titled "Our Responsibilities," promises "to maintain the privacy and security of your protected health information."[1]

33. By failing to protect Plaintiff's and Class members' Private Information, and by allowing the Data Breach to occur, Keystone Health Specialists broke these promises to Plaintiff and Class members.

B. Defendant Failed to Maintain Reasonable and Adequate Security Measures to Safeguard its Patients' Private Information

34. Keystone Health acquires, collects, and stores a massive amount of its patients' protected Private Information, including health information and other personally identifiable data.

35. As a condition of engaging in health-related services, Keystone Health requires that its patients entrust it with their highly confidential Private Information.

36. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class members' Private Information, Keystone Health assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff and Class members' Private Information from disclosure.

37. Defendant had obligations created by the Health Insurance Portability and Accountability Act (42 U.S.C. § 1320d *et seq.*) ("HIPAA"), industry standards, common law, and

[1] Keystone Health, Notice of Privacy Practices, notice-of-privacy-practices-January-2019.pdf (keystonehealth.org) (last accessed Nov. 1, 2022).

representations made to Class members, to keep Class members' Private Information confidential and to protect it from unauthorized access and disclosure.

38. As evidenced by Defendant's failure to comply with its legal obligations established by HIPAA and Pennsylvania law, Defendant failed to properly safeguard Class members' Private Information, allowing hackers to access their Private Information.

39. Plaintiff and Class members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant and any of its affiliates would comply with their obligation to keep such information confidential and secure from unauthorized access.

40. Prior to and during the Data Breach, Defendant implicitly and explicitly promised patients that their Private Information would be kept confidential.

41. Defendant's failure to provide adequate security measures to safeguard Plaintiff's and Class members' Private Information is especially egregious because Defendant operates in a field which has recently been a frequent target of scammers attempting to fraudulently gain access to patients' highly confidential Private Information.

42. In fact, Defendant has been on notice for years that the healthcare industry and health insurance companies are a prime target for scammers because of the amount of confidential customer information maintained.

43. Defendant 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, perhaps for the purpose of obtaining the [PHI] and/or [PII]."[2]

44. 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.[3]

45. The number of US 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.[4] In 2017, a new record high of 1,579 breaches were reported—representing a 44.7 percent increase.[5] That trend continues.

46. The healthcare sector reported the second-largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[6] 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 out-of-pocket costs for healthcare they did not receive in order to restore coverage.[7] Almost 50

---

[2] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warnshealthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820.

[3] 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.

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

[5] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review*, https://www.idtheftcenter.org/2017-data-breaches/.

[6] Identity Theft Resource Center, *2018 End -of-Year Data Breach Report*, https://www.idtheftcenter.org/2018-data-breaches/.

[7] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for- victims/.

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.[8]

47. A 2017 study conducted by HIMSS Analytics showed that email was the most likely cause of a data breach, with 78 percent of providers stating that they experienced a healthcare ransomware or malware attack in the past 12 months.

48. Healthcare related data breaches continued to rapidly increase into 2021.[9]

49. 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."[10]

50. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precaution for protection."[11]

51. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

---

[8] *Id.*
[9] *2019 HIMSS Cybersecurity Survey*, https://www.himss.org/2019-himsscybersecurity-survey.
[10] Aaron Jensen, *Healthcare Phishing Statistics: 2019 HIMSS Survey Results*, PROOFPOINT (Mar. 27, 2019), https://www.proofpoint.com/us/security-awareness/post/healthcare-phishingstatistics-2019-himss-survey-results.
[11] *See How to Protect Your Networks from RANSOMWARE*, FBI (2016) https ://www. fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege; no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[12]

52. The threat continues. In August 2022, the Consumer Finance Protection Bureau (CFPB) published a circular on data security. The CFPB noted that "[w]idespread data breaches and cyberattacks have resulted in significant harms to consumers, including monetary loss, identity theft, significant time and money spent dealing with the impacts of the breach, and other forms of financial distress," and the circular concluded that the provision of insufficient security for consumers' data can violate the prohibition on "unfair acts or practices" in the Consumer Finance Protection Act (CFPA).[13]

53. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks . . .

- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those

[12] *Id.*

[13] CONSUMER FIN. PROT. BUREAU, *Consumer Financial Protection Circular 2022-04: Insufficient data protection or security for sensitive consumer information* (Aug. 11, 2022), https://files.consumerfinance.gov/f/documents/cfpb_2022-04_circular_2022-08.pdf.

> you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) . . .
>
> - **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
>
> - **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it . . .
>
> - **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
>
> - **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
>
> - **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic . . .[14]

54. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
  - Apply the latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privilege credentials;

[14] *See Security Tip (ST19-001) Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (Apr. 11, 2019), https://us-cert.cisa.gov/ncas/tips/ST19-001.

- **Thoroughly investigate and remediate alerts**
  - Prioritize and treat commodity malware infections as potential full compromise

- **Include IT Pros in security discussions**
  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

- **Build credential hygiene**
  - use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

- **Apply principle of least-privilege**
  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events

- **Harden infrastructure**
  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection
  - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[15]

55. These are basic, common-sense email security measures that every business, not only healthcare businesses, should be doing. Keystone Health, with its heightened standard of care should be doing even more. But by adequately taking these common-sense measures, Keystone Health could have prevented this Data Breach from occurring.

56. Charged with handling sensitive Private Information, including healthcare information, Defendant knew, or should have known, the importance of safeguarding its patients'

[15] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-apreventable-disaster/.

Private Information that was 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 its patients after a breach. Keystone Health failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

57. With respect to training, Defendant specifically failed to:

- Implement a variety of anti-ransomware training tools, in combination, such as computer-based training, classroom training, monthly newsletters, posters, login alerts, email alerts, and team-based discussions;
- Perform regular training at defined intervals such as bi-annual training and/or monthly security updates; and
- Craft and tailor different approaches to different employees based on their base knowledge about technology and cybersecurity.

58. The Private Information was also maintained on Keystone Health's computer system in a condition vulnerable to cyberattacks, such as through the infiltration of Defendant's systems through ransomware attacks. The mechanism of the cyberattack and the potential for improper disclosure of Plaintiff and Class members' Private Information was a known risk to Keystone Health, and thus Keystone Health was on notice that failing to take reasonable steps necessary to secure the Private Information from those risks left it in a vulnerable position.

C. The Monetary Value of Privacy Protections and Private Information

59. The fact that Plaintiff and Class members' Private Information was stolen means that Class members' information is likely for sale by cybercriminals and will be misused in additional instances in the future.

60. At all relevant times, Defendant was well aware that the Private Information it collects from Plaintiff and Class members is highly sensitive and of significant value to those who would use it for wrongful purposes.

61. Private Information 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.[16] Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information including sensitive health information on multiple underground Internet websites, commonly referred to as the dark web.

62. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[17]

63. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 Billion per year online advertising industry in the United States.[18]

64. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information

---

[16] Federal Trade Commission, *Warning Signs of Identity Theft* (Sept. 2018), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft .

[17] *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, FED. TRADE COMM'N Tr. at 8:2-8 (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

[18] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html [hereinafter *Web's New Hot Commodity*].

> may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[19]

65. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[20] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

66. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[21]

67. The value of Plaintiff and Class members' Private Information on the black market is substantial. Sensitive health information can sell for as much as $363.[22] This 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.

68. Medical identity 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

---

[19] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

[20] *Web's Hot New Commodity*, *supra* note 17.

[21] *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

[22] Center for Internet Security, *Data Breaches: In the Healthcare Sector*, https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/.

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."[23]

69. The ramifications of Keystone Health's failure to keep its patients' Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to twelve months or even longer.

70. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened.[24] 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.[25]

71. Breaches are particularly serious in healthcare industries, with healthcare related data among the most private and personally consequential, as set forth above.[26]

72. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud. Defendant should have particularly been

[23] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER (Feb. 7, 2014) https://khn.org/news/rise-of-indentity-theft/.
[24] *See Medical ID Theft Checklist*, IDENTITYFORCE, https://www.identityforce.com/blog/medical-id-theft-checklist-2.
[25] *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches*, EXPERIAN, (Apr. 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.
[26] *See supra* Facts, Section B.

aware of these risks, given the significant number of data breaches affecting the health care industry and related industries.

73. Had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented the ransomware attack into its systems and, ultimately, the theft of its patients' Private Information.

74. The compromised Private Information in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[27] For example, different PII and PHI elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.[28] Based upon information and belief, the unauthorized parties utilized the Private Information they obtained through the Data Breach to obtain additional information from Plaintiff and Class members that was misused.

75. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

---

[27] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, FED. TRADE COMM'N 35-38 (Dec. 2010), https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework.

[28] *See id.* (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

76. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts. Thus, even if payment card information was not involved in the Data Breach, the unauthorized parties could use Plaintiff and Class members' Private Information to access accounts, including, but not limited to email accounts and financial accounts, to engage in the fraudulent activity identified by Plaintiff.

77. Given these facts, any healthcare or other type of entity that transacts business with patients or customers and then compromises the privacy of its patients' or customers' Private Information has thus deprived them of the full monetary value of the transaction with the entity.

78. Acknowledging the damage to Plaintiff and Class members, Defendant instructed patients like Plaintiff to "review the statements you receive from your health insurer" and call the insurer "immediately" if fraudulent charges appear. Plaintiff and Class members now face an impending, substantial risk of identity theft and medical insurance fraud.

79. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

D. Keystone Health's Conduct violated HIPAA

80. HIPAA requires covered entities like Keystone Health to protect against reasonably anticipated threats to the security of PHI. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[29]

[29] *What is Considered Protected Health Information Under HIPAA*?, HIPPA JOURNAL, https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/.

81. 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 Private Information like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

82. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant 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]

83. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations. Keystone Health's security failures include, but are not limited to, the following:

- Failing to ensure the confidentiality and integrity of electronic protected health information that Defendant creates, receives, maintains, and transmits in violation of 45 C.F.R. §164.306(a)(1);
- 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 C.F.R. §164.312(a)(1);
- Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. §164.308(a)(1);
- 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 C.F.R. §164.308(a)(6)(ii);

[30] *Breach Notification Rule*, U.S. DEP'T HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

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

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

- Failing to ensure compliance with HIPAA security standard rules by its workforce in violation of 45 C.F.R. §164.306(a)(94);

- Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. §164.502, *et seq.*;

- Failing to effectively train all members of its workforce (including agents and independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §164.308(a)(5); and

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

E. Keystone Health Specialists Failed to Comply with FTC Guidelines

84. Keystone Health 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).

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

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

87. The FTC further recommends that companies not maintain Private Information 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]

88. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

---

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

[32] *Protecting Personal Information: A Guide for Business*, FED. TRADE. COMM'M (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf- 0136_proteting-personal-information.pdf.

[33] *Start with Security*, *supra* note 32.

89. Keystone Health was at all times fully aware of its obligation to protect the Private Information of its patients. Keystone Health was also aware of the significant repercussions that would result from its failure to do so.

90. As evidenced by Defendant's failure to comply with its legal obligations established by the FTC Act, Defendant failed to properly safeguard Class members' Private Information, allowing hackers to access their Private Information

F. Keystone Health Failed to Comply with Healthcare Industry Standards

91. HHS's Office for Civil Rights has stated:

> While all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations, as they store large quantities of highly Private and valuable data.[34]

92. HHS highlights several basic cybersecurity safeguards that can be implemented to improve cyber resilience that require a relatively small financial investment yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of Private Information; (b) educating and training healthcare employees on how to protect Private Information; and (c) correcting the configuration of software and network devices.

93. Private cybersecurity firms have also identified the healthcare sector as being particularly vulnerable to cyber-attacks, both because the of the value of the Private Information which they maintain and because as an industry they have been slow to adapt and respond to cybersecurity threats.[35] They too have promulgated similar best practices for bolstering cybersecurity and protecting against the unauthorized disclosure of Private Information.

---

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

[35] *See, e.g.*, *10 Best Practices For Healthcare Security*, INFOSEC, https://resources.infosecinstitute.com/topics/healthcare-information-security/#gref.

94. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, Keystone Health chose to ignore them. These best practices were known, or should have been known by Keystone Health, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure of Private Information.

G. Damages to Plaintiff and the Class

95. Plaintiff and the Class have been damaged by the compromise of their Private Information in the Data Breach.

96. The ramifications of Keystone Health's failure to keep its patients' Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to the victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[36]

97. In addition to its obligations under state and federal laws and regulations, Defendant owed a common law duty to Plaintiff and Class members to protect the Private Information they entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

98. Defendant further owed and breached its duty to Plaintiff and Class members to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

99. Defendant also failed to maintain Plaintiff's and Class members' confidences by improperly disclosing their Private Information without consent.

[36] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

100. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise commit the identity theft and misuse of Plaintiff and Class members' Private Information as detailed above, and Plaintiff and members of the Class are at a heightened and increased substantial risk of suffering identity theft and fraud.

101. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds to thousands of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

102. Some of the injuries and risks associated with the loss of Private Information have already manifested themselves in Plaintiff and other Class members' lives. Each Plaintiff received a cryptically written notice letter from Defendant stating that their Private Information was released, and that they should remain vigilant for fraudulent activity, with no other explanation of where this Private Information could have gone, or who might have access to it.

103. Plaintiff and the Class face a substantial risk of suffering out-of-pocket fraud losses such as fraudulent charges on online accounts, credit card fraud, applications for benefits made fraudulent in their names, loans opened in their names, medical services billed in their names, government benefits fraudulently drawn in their name, and identity theft. Many Class members may already be victims of identity theft and fraud without realizing it.

104. Plaintiff and Class members have, may have, and/or will have incurred out of pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

105. Plaintiff and Class members have lost confidence in their medical provider, Keystone Health, as a result of the Data Breach.

106. Plaintiff and Class members did not receive the full benefit of their bargain when paying for medical services, and instead received services that were of a diminished value to those described in their agreements with their respective healthcare institutions that had made agreements with Keystone Health for the benefit and protection of Plaintiff and Class members and their respective Private Information. Plaintiff and Class members were damaged in an amount at least equal to the difference in the value between the services they thought they paid for (which would have included adequate data security protection) and the services they actually received.

107. Plaintiff and Class members would not have obtained services from their medical providers had they known that Defendant failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from criminal theft and misuse.

108. Plaintiff and the Class will continue to spend significant amounts of time to monitor their financial and medical accounts for misuse.

109. The theft of Social Security numbers, which were purloined as part of this Data Breach, is particularly detrimental to victims. The U.S. Social Security Administration ("SSA") warns that "[i]dentity theft is one of the fastest growing crimes in America."[37] The SSA has stated that "[i]dentity thieves can use your number and your good credit to apply for more credit in your

37 *Identity Theft And Your Social Security Number*, SOCIAL SECURITY ADMIN. (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf.

name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought."[38] In short, "[s]omeone illegally using your Social Security number and assuming your identity can cause a lot of problems."[39]

110. In fact, a new Social Security number is substantially less effective where "other personal information, such as [the victim's] name and address, remains the same" and for some victims, "a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit."[40]

111. Identity thieves can use the victim's Private Information to commit any number of frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest. In the healthcare industry context, Private Information can be used to submit false insurance claims. As a result, Plaintiff and Class members now face a real and continuing immediate risk of identity theft and other problems associated with the disclosure of their Social Security numbers and will need to monitor their credit for an indefinite duration. For Plaintiff and Class members, this risk creates unending feelings of fear and annoyance. Private Information is especially valuable to identity thieves. Defendant knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

[38] *Id.*
[39] *Id.*
[40] *Id.*

112. As a result of the Data Breach, Plaintiff and Class members' Private Information has diminished in value.

113. The Private Information belonging to Plaintiff and Class members is private and was left inadequately protected by Defendant who did not obtain Plaintiff or Class members' consent to disclose such Private Information to any other person as required by applicable law and industry standards. Defendant disclosed Plaintiff and Class members' Private Information as a direct result of its inadequate security measures.

114. The Data Breach was a direct and proximate result of Defendant's failure to: (a) properly safeguard and protect Plaintiff and Class members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff and Class members' Private Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

115. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect customer data.

116. Defendant did not properly train its employees, particularly its information technology department, to timely identify and/or avoid ransomware attacks.

117. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiff and Class members' Private Information.

118. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class members have been placed at an imminent, immediate, and continuing

increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

119. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[41]

120. Other than offering 12 months of credit monitoring, Defendant did not take any measures to assist Plaintiff and Class members.

121. Defendant's failure to adequately protect Plaintiff and Class members' Private Information has resulted in Plaintiff and Class members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money–while Defendant sits by and does nothing to assist those affected by the incident. Instead, as Keystone's notice confirms, the burden is on Plaintiff and Class members to discover possible fraudulent activity and identity theft and mitigate the negative impacts arising from such fraudulent activity on their own.

122. While Defendant offered one year of credit monitoring Class members, the credit monitoring offered does not guarantee privacy or data security for Plaintiff. Thus, to mitigate harm, Plaintiff and Class members are now burdened with indefinite monitoring and vigilance of their accounts. This is particular acute in the case of T.B., who will have to be extraordinarily vigilant for his entire life.

[41] *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

123. Worse still, the limited offer of credit monitoring is woefully inadequate. While some harm has already taken place, the worst is yet to come. There may be a time lag between when harm occurs versus when it is discovered, and between when Private Information is acquired and when it is used. Furthermore, identity theft monitoring only alerts someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's Private Information) – it does not prevent identity theft.[42] This is especially true for many kinds of medical identity theft, for which most credit monitoring plans provide little or no monitoring or protection.

124. Plaintiff and Class members have been damaged in several other ways as well. Plaintiff and Class members have been exposed to an impending, imminent, and ongoing increased risk of fraud, identity theft, and other misuse of their Private Information. Plaintiff and Class members must now and indefinitely closely monitor their financial and other accounts to guard against fraud. This is a burdensome and time-consuming task. Class members have also been forced to purchase adequate credit reports, credit monitoring and other identity protection services, and have placed credit freezes and fraud alerts on their credit reports, while also spending significant time investigating and disputing fraudulent or suspicious activity on their accounts. Plaintiff and Class members also suffered a loss of the inherent value of their Private Information.

125. The Private Information stolen in the Data Breach can be misused on its own or can be combined with personal information from other sources such as publicly available information, social media, etc. to create a package of information capable of being used to commit further identity theft. Thieves can also use the stolen Private Information to send spear-phishing emails to

[42] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-beworth-the-cost.html.

Class members to trick them into revealing sensitive information. Lulled by a false sense of trust and familiarity from a seemingly valid sender (for example Wells Fargo, Amazon, or a government entity), the individual agrees to provide sensitive information requested in the email, such as login credentials, account numbers, and the like.

126. As a result of Defendant's failures to prevent the Data Breach, Plaintiff and Class members have suffered, will suffer, and are at increased risk of suffering:

- The compromise, publication, theft and/or unauthorized use of their Private Information;
- Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;
- Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;
- The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the Private Information in its possession;
- 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; and
- Anxiety and distress resulting fear of misuse of their Private Information.

127. In addition to a remedy for the economic harm, Plaintiff and Class members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

128. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), 23(b)(3), and/or 23(c)(4).

129. Specifically, Plaintiff proposes the following Nationwide Class and Pennsylvania Subclass (collectively, the "Class") definitions:

> **Nationwide Class**
> All persons residing in the United States whose Private Information was compromised as a result of the Data Breach discovered on or about August of 2022.
>
> **Pennsylvania Subclass**
> All persons residing in Pennsylvania whose Private Information was compromised as a result of the Data Breach discovered on or about August of 2022.

Excluded from the Class are Defendant and Defendant's affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded are any judicial officers presiding over this matter and the members of their immediate families and judicial staff.

130. Plaintiff reserves the right to modify, change, amend, or expand the definitions of the Nationwide Class and Pennsylvania Subclass based upon discovery and further investigation.

131. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

132. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. Upon information and belief, the Class numbers number in the tens of thousands. Moreover, the Class is composed of an easily ascertainable set of individuals and entities who were patients of Defendant

and who were impacted by the Data Breach of Defendant's systems. The precise number of Class members can be further confirmed through discovery, which includes Defendant's records. The disposition of Plaintiff's and Class members' claims through a class action will benefit the parties and this Court.

133. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, *inter alia*:

- Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- Whether Defendant properly implemented its purported security measures to protect Plaintiff's and the Class's Private Information from unauthorized capture, dissemination, and misuse;
- Whether Defendant took reasonable measures to determine the extent of the Data Breach after it first learned of same;
- Whether Defendant disclosed Plaintiff's and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;
- Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and the Class's Private Information;
- Whether Defendant was negligent in failing to properly secure and protect Plaintiff's and the Class's Private Information;
- Whether Defendant was unjustly enriched by its actions; and

- Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

134. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of themselves and other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

135. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other members of the Class because, among other things, all Class members were similarly injured and sustained similar monetary and economic injuries as a result of Defendant's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to either Plaintiff.

136. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate representatives of the Class because their interests do not conflict with the interests of the Class they seek to represent, they have retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and their counsel.

137. **Injunctive Relief—Federal Rule of Civil Procedure 23(b)(2).** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

138. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy,

and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

139. Class certification is also appropriate under Rules 23(b)(1) and/or (b)(2) because:

a. The prosecution of separate actions by the individual members of the Class would create a risk of inconsistent or varying adjudications establishing incompatible standards of conduct for Defendant;

b. The prosecution of separate actions by individual Class members would create a risk of adjudication that would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or would substantially impair or impede their ability to protect their interests; and

c. Defendant has acted and refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief with respect to the members of the Class as a whole.

140. Class certification is also appropriate because this Court can designate particular claims or issues for class-wide treatment and may designate multiple subclasses pursuant to Fed. R. Civ. P. 23(c)(4).

141. No unusual difficulties are likely to be encountered in the management of this action as a class action.

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

142. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

143. Upon Defendant's acceptance and storage of the Private Information of Plaintiff and the Class in its computer systems and on its networks, Defendant undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that Information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should be protected as private and confidential.

144. Defendant owed a duty of care not to subject Plaintiff and the Class's Private Information to an unreasonable risk of exposure and theft because Plaintiff and the Class were foreseeable and probable victims of any inadequate security practices.

145. Defendant owed numerous duties to Plaintiff and the Class, including the following:

- to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in its possession;
- to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

- to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

146. Defendant also breached its duty to Plaintiff and Class members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering its dilatory practices, Defendant failed to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiff and Class members' Private Information for the purpose of misusing and intentionally disclosing it to others without consent.

147. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendant knew or should have known about numerous well-publicized data breaches within the medical industry.

148. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff and Class members' Private Information.

149. Defendant breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and Class members' Private Information.

150. Because Defendant knew that a breach of its systems would damage thousands of its patients, including Plaintiff and Class members, Defendant had a duty to adequately protect its data systems and the Private Information contained thereon.

151. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and Class members, which is

recognized by laws and regulations including but not limited to common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

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

153. Defendant also had a duty under HIPAA privacy laws, which were enacted with the objective of protecting the confidentiality of clients' 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.

154. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

155. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Private Information. Defendant's misconduct included failing to: (1) secure Plaintiff and Class member's Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

156. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class members' Private Information, and by failing to provide timely notice

of the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information;

b. Failing to adequately monitor the security of Defendant's networks and systems;

c. Allowing unauthorized access to Class members' Private Information;

d. Failing to detect in a timely manner that Class members' Private Information had been compromised; and

e. Failing to timely notify Class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages

157. Through Defendant's acts and omissions described in this Complaint, including its failure to provide adequate security and failure to protect Plaintiff and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff and Class members' Private Information during the time it was within Defendant's possession or control.

158. Defendant's conduct was grossly negligent and departed from reasonable standards of care, including but not limited to, failing to adequately protect the Private Information and failing to provide Plaintiff and Class members with timely notice that their sensitive Private Information had been compromised.

159. Neither Plaintiff nor Class members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

160. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members suffered damages as alleged above.

161. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide lifetime free credit monitoring to all Class members.

COUNT II
BREACH OF CONTRACT
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, Plaintiff and the Pennsylvania Subclass)

14. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

15. Plaintiff and other Class members entered into valid and enforceable express contracts with Defendant under which Plaintiff and other Class members agreed to provide their Private Information to Defendant, and Defendant agreed to provide healthcare services and, impliedly, if not explicitly, agreed to protect Plaintiff and Class members' Private Information.

16. These contracts include HIPAA privacy notices and explanation of benefits documents.

17. To the extent Defendant's obligation to protect Plaintiff's and other Class members' Private Information was not explicit in those express contracts, the express contracts included implied terms requiring Defendant to implement data security adequate to safeguard and protect the confidentiality of Plaintiff's and other Class members' Private Information, including in accordance with HIPAA regulations; federal, state and local laws; and industry standards. Plaintiff would not have entered into these contracts with Defendant without understanding that her, her son's, and other Class members' Private Information would be

safeguarded and protected. Stated otherwise, data security was an essential implied term of the parties' express contracts.

18. A meeting of the minds occurred, as Plaintiff and other Class members agreed, among other things, to provide their Private Information in exchange for Defendant's agreement to protect the confidentiality of that Private Information.

19. The protection of Plaintiff and Class members' Private Information were material aspects of Plaintiff's and Class members' contracts with Defendant.

20. Defendant's promises and representations described above relating to HIPAA and industry practices, and about Defendant's purported concern about their clients' privacy rights became terms of the contracts between Defendant and their clients, including Plaintiff and other Class members. Defendant breached these promises by failing to comply with HIPAA and reasonable industry practices.

21. Plaintiff and Class members read, reviewed, and/or relied on statements made by or provided by Defendant and/or otherwise understood that Defendant would protect its patients' Private Information if that information were provided to Defendant.

22. Plaintiff and Class members fully performed their obligations under the implied contract with Defendant; however, Defendant did not.

23. As a result of Defendant's breach of these terms, Plaintiff, her son, and other Class members have suffered a variety of damages including but not limited to: the lost value of their privacy; they did not get the benefit of their bargain with Defendant; they lost the difference in the value of the secure health services Defendant promised and the insecure services received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, inter alia, that required to place "freezes" and "alerts" with

credit reporting agencies, to contact financial institutions, to close or modify financial and medical accounts, to closely review and monitor credit reports and various accounts for unauthorized activity, and to file police reports; and Plaintiff, her son, and other Class members have been put at increased risk of future identity theft, fraud, and/or misuse of their Private Information, which may take years to manifest, discover, and detect.

162. 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

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Pennsylvania Subclass)

163. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

164. Plaintiff brings this claim in the alternative to her breach of express contract claim.

165. Through its course of conduct, Defendant, Plaintiff, and Class members entered into implied contracts for the provision of healthcare and data administration services, as well as implied contracts for the implementation of data security adequate to safeguard and protect the privacy of Plaintiff and Class members' Private Information.

166. Specifically, Plaintiff and Class members entered into valid and enforceable implied contracts with Defendant when they first entered into contracts with Defendant to receive medical services.

167. The valid and enforceable implied contracts to provide medical services that Defendant entered into with Plaintiff and Class members include Defendant's promise to protect

nonpublic Private Information given to Defendant or that Defendant created on its own from disclosure.

168. When Plaintiff and Class members provided their Private Information to Defendant in exchange for medical services from Defendant, they entered into implied contracts pursuant to which Defendant agreed to reasonably protect such Private Information.

169. Defendant solicited and invited Class members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class members accepted Defendant's offers and provided their Private Information to Defendant.

170. By entering into such implied contracts, Plaintiff and Class members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

171. Class members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

172. Under these implied contracts, Defendant was obligated to: (a) provide medical services to Plaintiff and Class members; and (b) protect Plaintiff and Class members' Private Information provided to obtain the benefits of such services. In exchange, Plaintiff and members of the Class agreed to pay money for these services, and to turn over their Private Information.

173. Both the provision of medical services and the protection of Plaintiff and Class members' Private Information were material aspects of these implied contracts.

174. The implied contracts for the provision of medical services include the contractual obligations to maintain the privacy of Plaintiff and Class members' Private Information, which are also acknowledged, memorialized, and embodied in multiple documents (including, among other

documents, Defendant's Data Breach notification letter and Defendant's Notice of Privacy Practices).

175. Defendant's express representations, including, but not limited to the express representations found in its Notice of Privacy Practices, memorializes and embodies the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff and Class members' Private Information.

176. Consumers of medical services value their privacy, the privacy of their dependents, and the ability to keep confidential their Private Information associated with obtaining such services. Plaintiff and Class members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected; nor would they have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

177. A meeting of the minds occurred as Plaintiff and Class members agreed and provided their Private Information to Defendant and paid for the provided services in exchange for, among other things, both the provision of healthcare and the protection of their Private Information.

178. Plaintiff and Class members performed their obligations under the contract when they paid for Defendant's services and provided Defendant with their Private Information.

179. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when the Private Information was accessed and exfiltrated through the Data Breach.

180. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices. Defendant did not maintain the privacy of Plaintiff and Class members' Private Information as evidenced by its notifications of the Data Breach to Plaintiff and Class members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA or HIPAA, or otherwise protect Plaintiff and Class members' private information as set forth above.

181. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

182. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Class members did not receive full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiff and Class members, therefore, were damaged in an amount at least equal to the difference in the value between the healthcare with data security protection they paid for and the healthcare they received.

183. Had Defendant disclosed that its data security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, Class members, nor any reasonable person would have gone to Defendant to obtain healthcare services.

184. As a direct and proximate result of the Data Breach, Plaintiff and Class members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out of pocket expenses to mitigate the effects of the

Data Breach, including time lost responding to the Breach, and the loss of the benefit of the bargain they struck with Defendant.

185. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

186. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

COUNT IV
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the State Subclass)

187. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

188. In providing their Private Information to Defendant, Plaintiff and Class members justifiably placed a special confidence in Defendant to act in good faith and with due regard for the interests of Plaintiff and Class members to safeguard and keep confidential that Private Information.

189. Defendant accepted the special confidence Plaintiff and Class members placed in it, as evidenced by its assertion that it is "committed to protecting the privacy and security of [its] patients' information" as included in the form Data Breach notification letters distributed to Class members.

190. In light of the special relationship between Defendant and Plaintiff and Class members, whereby Defendant became a guardian of Plaintiff and Class members' Private Information and Personal Health Information (PHI), Defendant became a fiduciary by its

undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiff and Class members for the safeguarding of Plaintiff and Class members' Private Information.

191. Additionally, the special relationship of patient and health care provider gives rise to a fiduciary duty on the part of Defendant to protect Plaintiff and Class members' Private Information.

192. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of its patient relationships, in particular, to keep secure the Private Information of its patients.

193. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to protect the integrity of the systems containing Plaintiff and Class members' Private Information.

194. Defendant breached its fiduciary duties to Plaintiff and Class members by otherwise failing to safeguard Plaintiff and Class members' Private Information.

195. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and/or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate

measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of the services they paid for and received.

196. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V
BREACH OF CONFIDENCES
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the State Subclass)

197. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

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

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

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

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

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

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

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

205. As a result of the parties' relationship, Defendant had possession and knowledge of the confidential Private Information of Plaintiff and Class members.

206. Plaintiff's and the Class's Private Information is not generally known to the public and is confidential by nature.

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

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

209. Defendant breached its duties of confidence by failing to safeguard Plaintiff's and Class members' Private Information, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of the Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement

information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the Breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its patients; (h) storing PII, PHI and medical records/information in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiff and the Class members' Private Information to a criminal third party.

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

211. As a direct and proximate result of Defendant's breach of Plaintiff's and the Class's confidences, Plaintiff and Class members have suffered or will suffer injuries, including: the erosion of the essential and confidential relationship between Defendant—as a health care services provider—and Plaintiff and Class members as patients; loss of their privacy and confidentiality in their Private Information; theft of their Private Information; costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts; costs associated with purchasing credit monitoring and identity theft protection services; lowered credit scores resulting from credit inquiries following fraudulent activities; costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendant's Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on

compromised accounts; the imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals; damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others; continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data; loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received, as directed to do by Defendant; and/or mental anguish accompanying the loss of confidences and disclosure of their confidential Private Information.

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

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

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

COUNT VI
DECLARATORY RELIEF
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Pennsylvania Subclass)

215. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

216. 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 granting 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 statutes described in this Complaint.

217. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiff and Class members' Private Information, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class members from future data breaches that compromise their Private Information. Plaintiff and the Class remain at imminent risk that additional compromises of their Private Information will occur in the future.

218. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect consumers' PII and PHI.

219. Defendant still possesses the Private Information of Plaintiff and the Class.

220. Defendant has made no announcement that it has changed its data storage or security practices relating to the storage of Plaintiff's and Class members' Private Information.

221. To Plaintiff's knowledge, Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

222. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Keystone Health. The risk of another such breach is real, immediate, and substantial.

223. The hardship to Plaintiff and Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at Keystone Health, Plaintiff and Class members will likely continue to be subjected to a heightened, substantial, imminent risk of fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

224. 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 Health, thus eliminating the additional injuries that would result to Plaintiff and Class members, along with other consumers whose Private Information would be further compromised.

225. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Keystone Health Specialists implement and maintain reasonable security measures, including but not limited to the following:

a. Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on Keystone Health's systems on a periodic basis, and ordering Keystone Health to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. purging, deleting, and destroying Private Information not necessary for its provisions of services in a reasonably secure manner;

e. conducting regular database scans and security checks; and

f. routinely and continually conducting 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.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in favor of Plaintiff and the Class and against Defendant, as follows:

A. For an Order certifying this action as a class action 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 and Class members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to

disclose with specificity the type of PII and PHI compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. Ordering Defendant to pay for no less than three (3) years of credit monitoring services for Plaintiff and the Class;

F. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

G. For an award of punitive damages, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded; and

J. Such other and further relief as this court may deem just and proper.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Dated: November 8, 2022

Respectfully submitted,

/s/ Gary F. Lynch

Gary F. Lynch
Jamisen A. Etzel
Nicholas A. Colella
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Phone: 412-322-9243
Fax: 412-231-0246
Email:
gary@lcllp.com
jamisen@lcllp.com
nickc@lcllp.com

Nicholas A. Migliaccio
(*pro hac vice* admission to be sought)
Jason S. Rathod
(*pro hac vice* admission to be sought)
Tyler J. Bean
(*pro hac vice* admission to be sought)
MIGLIACCIO & RATHOD, LLP
412 H Street, NE, Suite 302
Washington, DC 20002
Phone: 202-470-520
Fax: 202-800-2730
Email:
nmigliaccio@classlawdc.com
jrathod@classlawdc.com

Attorneys for Plaintiff and the Putative Class

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: Keystone Health Responsible for 2022 Data Breach, Class Action Alleges

---