UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF TENNESSEE

J. PAUL MCHENRY, individually and on behalf of all others similarly situated,	)	
	)	Case No.:
Plaintiff,	)	
v.	)	
ADVENT HEALTH PARTNERS, INC.,	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff J. Paul McHenry ("McHenry" or "Plaintiff McHenry"), individually and on behalf of all others similarly situated, through undersigned counsel, hereby alleges the following against Defendant Advent Health Partners, Inc. ("AHP" or "Defendant"). Facts pertaining to Plaintiff and his 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. This is a class action for damages with respect to Advent Health Partners for its failure to exercise reasonable care in securing and safeguarding its customers' sensitive personal data—including first and last names, Social Security numbers, drivers' license information, dates of birth, health insurance information, medical treatment information, and financial account information, collectively known as personally identifiable information ("PII" or "Private Information").

2. This class action is brought on behalf of patients whose sensitive PII was stolen by cybercriminals in a cyber-attack on Advent Health Partner's systems that took place in or around September of 2021 and which resulted in the access and exfiltration of sensitive patient information (the "Data Breach").

3. Advent Health Partners reported to Plaintiff and members of the putative "Class" (defined below) that information compromised in the Data Breach included their PII.

4. Plaintiff and Class members were not notified of the data breach until, at the earliest, the end of March 2022 – more than six months after their Private Information was first accessed.

5. As a result of the Data Breach and Defendant's failure to promptly notify Plaintiff and Class members of the Data Breach, Plaintiff and Class members have and will continue to experience various types of misuse of their PII in the coming months and years, including but not limited to, unauthorized credit card charges, unauthorized access to email accounts, identity theft, and other fraudulent use of their Private Information.

6. There has been no assurance offered by Advent Health Partners that all personal data or copies of data have been recovered or destroyed.

7. Accordingly, Plaintiff asserts claims for negligence, breach of contract, breach of implied contract, breach of fiduciary duty, and declaratory and injunctive relief.

PARTIES

A. Plaintiff J. Paul McHenry

8. Plaintiff J. Paul McHenry is a resident and citizen of Oklahoma and brings this action in his individual capacity and on behalf of all others similarly situated. McHenry was a patient at Saint Francis Health in Tulsa, Oklahoma where he went for doctor's visits several times

before the Data Breach. To receive services at Advent Health Partners, Plaintiff was required to disclose his PII, which was then entered into Advent Health Partners' database and maintained by Defendant without his knowledge. In maintaining his Private Information, Defendant expressly and impliedly promised to safeguard Plaintiff McHenry's PII. Defendant, however, did not take proper care of Plaintiff McHenry's PII, leading to its exposure to, and exfiltration by, cybercriminals as a direct result of Defendant's inadequate security measures.

9. In March of 2022, Plaintiff McHenry received a notification letter from Defendant stating that his Private Information was compromised by cybercriminals.

10. The letter also offered one year of credit monitoring through Transunion, which was and continues to be ineffective for Plaintiff McHenry and other Class members. In order to receive the free credit monitoring services from, Transunion, Plaintiff McHenry would have had to share additional sensitive private information with third parties connected to Advent Health.

11. In or around February of 2022, Plaintiff McHenry was sent a notification letter informing him that he had been denied healthcare benefits under SoonerCare, a state-sponsored healthcare program in Oklahoma. Mr. McHenry has no knowledge of ever applying for SoonerCare benefits. The notice that Mr. McHenry received informing him of his rejection from the program without his knowledge is likely the result of a fraudulent application for benefits under his name using the Private Information compromised in the Data Breach.

12. Plaintiff McHenry and Class members have faced and will continue to face a certainly impending and substantial risk of a slew of future harms as a result 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, and

targeted advertising without patient consent. These harms will also include fraudulent applications for benefits in their names, similar to what Plaintiff McHenry has already experienced.

13. Plaintiff McHenry greatly values his privacy, especially while receiving medical services, and would not have paid the amount that he did to receive medical services had he known that Saint Francis Health's data processor, Advent Health, would negligently maintain his Private Information as it did.

B. Defendant Advent Health

14. Defendant Advent Health Partners is an outsourced healthcare claims review vendor. Advent Health Partners offers a number of medical claims review services, including billing, records review solutions, and medical record retrieval. Advent Health Partners has a principal place of business at 301 Plus Park Boulevard, Suite 500 in Nashville, Tennessee. Advent Health Partners' corporate policies and practices, including those used for data privacy, are established in, and emanate from Tennessee.

JURISDICTION AND VENUE

15. 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 citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

16. The Court has personal jurisdiction over Defendant because Defendant's principal place of business is located in this District.

17. Venue is proper in this district under 28 U.S.C. § 1391(b)(1) because Defendant maintains its principal place of business in this District and therefore resides in this District

pursuant to 28 U.S.C. § 1391(c)(2). A substantial part of the events or omissions giving rise to the Class's claims also occurred in this District.

FACTS

18. Defendant provides a wide variety of healthcare billing claims review services to hospitals and medical offices across the country, including in Tennessee and Oklahoma. As part of its business, Defendant was entrusted with, and obligated to safeguard and protect the Private Information of, Plaintiff and the Class in accordance with all applicable laws.

19. In September of 2021, Defendant first learned of an unauthorized activity on its employees' email accounts, which contained customers' Private Information including first and last names, Social Security numbers, drivers' license information, dates of birth, health insurance information, medical treatment information, and financial account information. Defendant posted the following notice on its website:[1]

> Advent Health Partners is providing notice of a recent incident that may affect the security of some information pertaining to individuals. The confidentiality, privacy, and security of information in Advent Health Partners' care is one of the highest priorities and Advent Health Partners takes this incident very seriously. Please note, we have no indication that anyone's information has been subject to actual or attempted misuse in relation to this incident.
>
> **What Happened?** In early September 2021, Advent Health Partners detected suspicious activity on employee email accounts involving data provided to Advent Health Partners. Advent Health Partners immediately commenced an investigation to determine the nature and scope of the incident. While the investigation is ongoing, on December 2, 2021, Advent Health Partners determined that certain files containing information of individuals were potentially accessed by an unauthorized third party. Advent Health Partners started providing notice of this incident on January 6, 2022.

[1] *Advent Health Partners Provides Notice of Security Incident*, https://adventhp.com/security-incident-notice/ (last visited Apr. 14, 2022) [hereinafter *Data Breach Notice*].

What Information Was Involved? The potentially accessed information varies by individual, but may include first and last names, Social Security numbers, drivers' license information, dates of birth, health insurance information, medical treatment information, and financial account information.

What Are We Doing? We take this incident and the security of personal information in our care very seriously. Upon learning of this incident, we moved quickly to investigate and respond to this incident, assess the security of our systems, and notify potentially affected individuals. As part of our ongoing commitment to the security of information, we are reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event. We will also be notifying state and federal regulators, as required.

For More Information. We understand that you may have questions that are not addressed. If you have additional questions, please call the dedicated assistance line at (855)-604-1735, which is available Monday through Friday, between the hours of 8:00 a.m. and 8:00 p.m. Central Time, or write to Advent Health Partners at 301 Plus Park Boulevard, Suite 500, Nashville, TN 37217. Advent Health Partners recommends that potentially impacted individuals follow the recommendations in the letter they received and contact the call center with any questions.

What You Can Do. Advent Health Partners sincerely regrets any inconvenience this incident may have caused. Advent Health Partners encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make

> regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

20. Upon learning of the Data Breach that occurred in September of 2021, Defendant investigated and began sending notification of the incident to its hospital and medical provider customers.[2] Plaintiff was not notified that his information was affected in the Data Breach until late March of 2022.

21. In February of 2022, nearly five (5) months after the Data Breach, Defendant first announced that it learned of suspicious activity that allowed one or more cybercriminals to access its employees' email accounts containing patient information.[3] The February 2022 Notice disclosed that an attack enabled a threat actor to access AHP employees' email accounts.

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

23. Defendant's delay in notifying its customers affected by the Data Breach violated the provisions of Tennessee Code Annotated, § 47-18-2107 and, in particular, the reporting provisions of § 47-18-2107(b) requiring Defendant to provide prompt and direct notice of a data security breach to any affected Tennessee residents once it knew or had reason to know of any such breach involving personal information and affecting Tennessee residents.

---

[2] The total number of affected patients still has not been reported to the Health and Human Services Healthcare Data Breach Portal. *See Cases Currently Under Investigation*, U.S. DEP'T OF HEALTH & HUMAN SERVS.: BREACH PORTAL, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf [hereinafter *Breach Portal*] (last visited Apr. 14, 2021).

[3] Defendant's Data Breach notice is not dated. The earliest record of this page being posted on Defendant's website through internet archive records, however, is on February 8, 2022.

24. AHP's notice of the Data Breach 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 customers were affected by the Data Breach. Even worse, AHP offered only one year of identity monitoring to Plaintiff and Class members, which required the disclosure of additional PII that AHP had just demonstrated it could not be trusted with.

25. In light of the types of personal 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' PII is being sold on the dark web, meaning that unauthorized parties have accessed, viewed, and exfiltrated Plaintiff's and Class members' unencrypted, unredacted, sensitive personal information, including names, addresses, email addresses, dates of birth, Social Security numbers, member ID numbers, policyholder names, employer names, policy numbers, and more.

26. The Breach occurred because Defendant failed to take reasonable measures to protect the PII 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.

27. 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's and Class members' PII was safeguarded, failing to take available steps to prevent an 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 PII of Plaintiff and Class members was compromised through unauthorized access by an unknown third party and has already been fraudulently misused. Plaintiff and Class members have a continuing interest in ensuring that their information is and remains safe.

A. Defendant's Privacy Promises

28. Advent Health Partners made, and continues to make, various promises to its customers, including Plaintiff, that it will maintain the security and privacy of their Private Information.

29. In its Notice of Privacy Practices, which was applicable to Plaintiff, Defendant stated under a section bolded and titled "Personal Information," the following:

> "Personally Identifiable Information" (PII), as described in United States privacy law and information security, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. Please read Advent Health Partner's Privacy Policy below carefully to understand how we collect, use, protect, and handle your PII in accordance with our website.
> **Personal Information**
>
> **What personal information do we collect from the people that visit our website(s)?**
> When registering on our site, as appropriate, we may request your name, email address, company name, job title, phone number, or other details.
>
> **When do we collect information?**
> We collect information from you when you complete a website form, utilize our live chat functionality, or otherwise provide information on our site.
>
> **How do we use your information?**
> We may use the information we collect when you respond to a marketing communication, visit pages of our website, or use specific site features in the following ways:

- To improve our website in order to better serve you,
- To send periodic emails regarding relevant technologies and services, and
- To follow up after correspondence (live chat, email, or phone inquiries).

How do we protect your information?

- We do not use vulnerability scanning and/or scanning to Payment Card Industry (PCI) standards.
- We only provide articles and information. We never ask for credit card numbers.
- We use regular malware scanning.
- Your PII is contained behind secured networks and is only accessible by a limited number of persons who have special access rights to such systems and are required to keep the information confidential. In addition, all sensitive information you supply is encrypted via Secure Socket Layer (SSL) technology.
- We implement a variety of security measures when a user enters, submits, or accesses their information to maintain the safety of your personal information.
- All transactions are processed through a gateway provider and are not stored or processed on our servers.

Do we use "cookies"?

Yes. Cookies are small files that a site or its service provider transfers to your computer's hard drive through your web browser (if you allow) that enables the site's or service provider's systems to recognize your browser and capture and remember certain information (e.g., information you submit through a form). They are also used to help us understand your preferences based on previous or current site activity, which enables us to provide you with improved services.

Advent Health Partners uses cookies to:

- Keep track of advertisements.
- Compile aggregate data about site traffic and interactions to offer improved future site experiences. We may also use trusted third-party services that track this information on our behalf.

Through your browser settings, you can choose to have your computer warn you each time a cookie is sent, or you can turn off all cookies. Since each browser is a little different, look at your browser's Help Menu to learn the correct way to modify your cookies. If you turn cookies off, some of the features that make your site experience more efficient may not function properly.

30. AHP describes how it may use and disclose medical information for each category of uses or disclosures, none of which provide it a right to expose customers' Private Information in the manner in which it was exposed to unauthorized third parties in the Data Breach.

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

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

32. AHP acquires, collects, and stores a massive amount of its customers' protected PII, including health information and other personally identifiable data.

33. As a condition of engaging in health-related services, AHP requires that its customers entrust them with their patients' highly confidential Private Information.

34. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class members' Private Information, AHP 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.

35. Defendant had obligations created by the Health Insurance Portability and Accountability Act (42 U.S.C. § 1320d *et seq.*) ("HIPAA"), Tennessee law (Tenn. Code Ann. § 47-18-2107, *et seq.*), industry standards, common law, and representations made to Class members, to keep Class members' Private Information confidential and to protect it from unauthorized access and disclosure.

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

37. 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.

38. Prior to and during the Data Breach, Defendant promised customers that their Private Information would be kept confidential.

39. Defendant's failure to provide adequate security measures to safeguard customers' 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 customers' highly confidential Private Information.

40. 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.

41. 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 Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[4]

42. The American Medical Association ("AMA") has also warned healthcare companies about the important 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.[5]

43. 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.[6] In 2017, a new record high of 1,579 breaches were reported—representing a 44.7 percent increase.[7] That trend continues.

44. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[8] 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

---

[4] 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.

[5] 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.

[6] 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.

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

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

out-of-pocket costs for healthcare they did not receive in order to restore coverage.[9] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[10]

45. 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.

46. Healthcare related data breaches continued to rapidly increase into 2021 when AHP was breached.[11]

47. 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."[12]

48. 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."[13]

---

[9] 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/.
[10] *Id.*
[11] *2019 HIMSS Cybersecurity Survey*, https://www.himss.org/2019-himsscybersecurity-survey.
[12] 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.
[13] *See How to Protect Your Networks from RANSOMWARE*, FBI (2016) https ://www. fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

49. 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:

- 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.

50. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants 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 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]

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 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;

- **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**

[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.

- 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]

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

53. Charged with handling sensitive PII including healthcare information, AHP knew, or should have known, the importance of safeguarding its customers' 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 AHP's customers as a result of a breach. AHP failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

54. With respect to training, AHP specifically failed to:

- Implement a variety of anti-ransomware training tools, in combination, such as computer-based training, classroom

[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/.

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.

55. The PII was also maintained on AHP'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' PII was a known risk to AHP, and thus AHP was on notice that failing to take reasonable steps necessary to secure the PII from those risks left the PII in a vulnerable position.

C. The Monetary Value of Privacy Protections and Private Information

56. 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.

57. At all relevant times, Defendant was well aware that 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.

58. 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 PII including sensitive health information on multiple underground Internet websites, commonly referred to as the dark web.

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

59. 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]

60. 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]

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

62. 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

---

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*].

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.

make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

63. 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]

64. 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.

65. 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 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]

---

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/.
23 Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER (Feb. 7, 2014) https://khn.org/news/rise-of-indentity-theft/.

66. The ramifications of AHP's failure to keep its customers' 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 6 to 12 months or even longer.

67. Approximately 21% of victims do not realize their identify 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]

68. Breaches are particularly serious in healthcare industries. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[26] Indeed, when compromised, healthcare related data is among the most private 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.[27] Almost 50% of the surveyed victims lost their healthcare coverage as a result of the incident, while nearly 30% said their insurance premiums went up after the event. Forty percent of the victims were never able to resolve their identity theft at all. Seventy-four percent said that the effort to resolve the crime and restore their identity was significant or very

[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] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, (2019) https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.
[27] 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/.

significant. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[28]

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

70. 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 customers' Private Information.

71. 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."[29] For example, different PII 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.[30] Based upon information and belief, the unauthorized parties utilized the Private Information they

---

[28] *Id.*

[29] *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.

[30] *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").

obtained through the Data Breach to obtain additional information from Plaintiff and Class members that was misused.

72. 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."

73. 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 were 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.

74. Given these facts, any company that transacts business with customers and then compromises the privacy of customers' Private Information has thus deprived customers of the full monetary value of their transaction with the company.

75. Acknowledging the damage to Plaintiff and Class members, Defendant instructed customers like Plaintiff to "remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft." Plaintiff and the other Class members now face a greater risk of identity theft.

76. 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. Advent Health Partners' Conduct violated HIPPA

77. HIPAA requires covered entities like AHP 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.[31]

78. 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.

79. 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."[32]

80. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations. AHP'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);

[31] *What is Considered Protected Health Information Under HIPAA*?, HIPPA JOURNAL, https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/.
[32] *Breach Notification Rule*, U.S. DEP'T HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

- 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);

- 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 their 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 their workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their 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. Advent Health Partners Failed to Comply with FTC Guidelines

81. AHP 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).

82. 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.[33]

83. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[34] 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.

84. 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.[35]

85. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and

[33] *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*].
[34] *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.
[35] *Start with Security*, *supra* note 32.

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

86. AHP was at all times fully aware of its obligation to protect the Private Information of patients because of its position as a trusted healthcare provider. AHP was also aware of the significant repercussions that would result from its failure to do so.

87. 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. AHP Failed to Comply with Healthcare Industry Standards

88. 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.[36]

89. 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.

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

90. 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.[37] They too have promulgated similar best practices for bolstering cybersecurity and protecting against the unauthorized disclosure of Private Information.

91. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, AHP chose to ignore them. These best practices were known, or should have been known by AHP, 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

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

93. The ramifications of AHP's failure to keep 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.[38]

94. In addition to their obligations under state and federal laws and regulations, Defendant owed a common law duty to Plaintiff and Class members to protect Private Information 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.

---

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

[38] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

95. 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.

96. 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 have already suffered, and are at a heightened and increased substantial risk of suffering, identity theft and fraud.

97. 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.

98. Some of the injuries and risks associated with the loss of personal information have already manifested themselves in Plaintiff and other Class members' lives. Plaintiff McHenry received a cryptically written notice letter from Defendant stating that his information was released, and that he should remain vigilant for fraudulent activity on his accounts, with no other explanation of where this information could have gone, or who might have access to it. He was subsequently denied benefits he never applied for, has already spent hours on the phone trying to determine what additional negative effects may occur from the loss of his personal information, and now faces a certainly impending and substantial risk of a slew of future harms.

99. Plaintiff and the Class have suffered or 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, and identity theft.

100. 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.

101. 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, which healthcare institutions entered into agreements with AHP that were made solely for the benefit of Plaintiff and Class members. 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.

102. 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.

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

104. The theft of Social Security Numbers, which were purloined as part of the 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."[39] The SSA has stated that "[i]dentity thieves can use your number and your good credit to apply for more credit in your 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."[40] In short, "[s]omeone illegally using your Social Security number and assuming your identity can cause a lot of problems."[41]

105. 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."[42]

106. 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

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

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.

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

108. 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 information about Plaintiff and the Class that was of an extremely personal and sensitive nature as a direct result of its inadequate security measures.

109. 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.

110. 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.

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

112. 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.

113. 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.

114. 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."[43]

115. Other than offering 12 months of credit monitoring, Defendant did not take any measures to assist Plaintiff and Class members other than telling them to simply do the following:

- remain vigilant for incidents of fraud and identity theft;
- review account statements and monitor credit reports for unauthorized activity;
- obtain a copy of free credit reports;
- contact the FTC and/or the state Attorney General's office;
- enact a security freeze on credit files; and
- create a fraud alert.

None of these recommendations, however, require Defendant to expend any effort to protect Plaintiff and Class members' Private Information.

116. 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

[43] *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*].

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 AHP's Data Breach Notice indicates, it is putting the burden on Plaintiff and Class members to discover possible fraudulent activity and identity theft.

117. While Defendant offered one year of credit monitoring, the credit monitoring offered from Transunion 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.

118. Moreover, the offer of 12 months of identity monitoring to Plaintiff and Class members 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.[44] This is especially true for many kinds of medical identity theft, for which most credit monitoring plans provide little or no monitoring or protection.

119. 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. Plaintiff and Class members have

[44] *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.

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.

120. 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 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.

121. 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.

122. 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

123. 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).

124. Specifically, Plaintiff proposes the following Nationwide Class and Oklahoma 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 September of 2021 and who were sent notice of the Data Breach.

Oklahoma Subclass
All persons residing in Oklahoma whose Private Information was compromised as a result of the Data Breach discovered on or about September 2021 and who were sent notice of the Data Breach.

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.

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

126. 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.

127. **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. On information and belief, the Class numbers in the thousands. Moreover, the Class and Oklahoma Subclass are composed of an easily ascertainable set of individuals and entities who were patients of Defendant and who were impacted by the Data Breach. 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.

128. **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.

129. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of himself 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.

130. **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 Plaintiff.

131. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class he seeks to represent, he has 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 his counsel.

132. **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).

133. **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.

134. 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.

135. 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).

136. 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 State Subclass)

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

138. Upon Defendant's accepting and storing 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.

139. 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.

140. 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.

141. 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 and potentially misuse the Private Information and intentionally disclose it to others without consent.

142. 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.

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

144. 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.

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

146. 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.

147. 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.

148. 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.

149. Furthermore, Defendant had a duty under Tenn. Code Ann. § 47-18-101, *et seq* to ensure that all customers' medical records and communications were kept confidential.

150. 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.

151. 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.

152. 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

153. 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.

154. Defendant's conduct was grossly negligent and departed from all 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.

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

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

157. 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 THID PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the State Subclass)

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

159. Plaintiff brings this claim for breach of third-party beneficiary contract against AHP in the alternative to Plaintiff's claim for breach of implied contract

160. Advent Health Partners entered into a contract to provide medical claims and billing review services to Saint Frances Health. Upon information and belief, this contract is virtually identity to the contracts entered into between Advent Health Partners and its other medical provider customers around the country whose patients were affected by the Data Breach.

161. The contracts were made expressly for the benefit of Plaintiff and the Class, as it was their confidential medical information that AHP agreed to collect and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties.

162. AHP knew that if it were to breach these contracts with its customers, the customers' patients, including Plaintiff and the Class, would be harmed by, among other harms, fraudulent transactions.

163. AHP breached its contracts with the medical providers affected by this Data Breach when it failed to use reasonable data security measures that could have prevented the Data Breach.

164. As foreseen, Plaintiff and the Class were harmed by AHP's failure to use reasonable security measures to store patient information, including but not limited to the risk of harm through the loss of their personal information.

165. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class)

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

167. Plaintiff and Class Members conferred a monetary benefit on Defendant in the form of their PII.

168. Defendant collected, maintained, and stored the PII of Plaintiff and Class Members and, as such, Defendant had knowledge of the monetary benefits conferred by them.

169. The money that Defendant received from Plaintiff's and Class Members' PII should have been used to pay, at least in part, for the administrative costs and implementation of data

security adequate to safeguard and protect the confidentiality of Plaintiff's and Class Members' PII.

170. Defendant failed to implement—or adequately implement—those data security practices, procedures, and programs to secure sensitive PII, as evidenced by the Data Breach.

171. As a result of Defendant's failure to implement data security practices, procedures, and programs to secure sensitive PII, Plaintiff and Class Members suffered actual damages in an amount of the savings and costs Defendant reasonably and contractually should have expended on data security measures to secure Plaintiffs' PII.

172. Under principles of equity and good conscience, Defendant should not be permitted to retain the money it received from Plaintiff's and Class Members' PII that should have been used to implement the data security measures necessary to safeguard and protect the confidentiality of Plaintiff's and Class Members' PII.

173. As a direct and proximate result of Defendant's decision to profit rather than provide adequate security, and Defendant's resultant disclosures of Plaintiff's and Class Members' PII, Plaintiff and Class Members suffered and continue to suffer considerable injuries in the forms of time and expenses mitigating harms, diminished value of PII, loss of privacy, and a present increased risk of harm.

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

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

175. 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.

176. 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' PII, 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 further compromises of their PII will occur in the future.

177. 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.

178. Defendant still possesses the PII of Plaintiff and the Class.

179. To Plaintiff's knowledge, Defendant has made no announcement that it has changed its data storage or security practices relating to the PII.

180. 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.

181. 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 AHP. The risk of another such breach is real, immediate, and substantial.

182. 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 AHP, Plaintiff and Class members will likely continue to be subjected to 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.

183. 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 AHP, thus eliminating the additional injuries that would result to Plaintiff and Class members, along with other consumers whose PII would be further compromised.

184. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Advent Health Partners 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 AHP's systems on a periodic basis, and ordering AHP 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 his 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 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: April 20, 2022

Respectfully submitted,

/s/Adam A. Edwards

Adam. A. Edwards (BPR No. 23253)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
800 S. Gay Street, Suite 1100
Knoxville, TN 37929
Telephone: (865) 247-0080
Facsimile: (865) 522-0049
aedwards@milberg.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
gklinger@milberg.com

David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW
Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
dlietz@milberg.com

Nicholas A. Migliaccio*
Jason S. Rathod, Esquire*
MIGLIACCIO & RATHOD, LLP
412 H Street, NE, Suite 302

Washington, DC 20002
Phone: 202-470-520
Fax: 202-800-2730
Email: nmigliaccio@classlawdc.com

**Pro Hac Vice forthcoming*

JS 44 (Rev. 04/21)

CIVIL COVER SHEET

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

I. (a) PLAINTIFFS

J. PAUL McHENRY individually and on behalf of all others similarly situated

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

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

Adam A. Edwards, Milberg, 800 S. Gay Street, Suite 1100, Knoxville, TN 37929

DEFENDANTS

ADVENT HEALTH PARTNERS, INC.

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

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

Attorneys *(If Known)*

not known

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

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

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

(For Diversity Cases Only)

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

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

Click here for: Nature of Suit Code Descriptions.

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

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

TORTS

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

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

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

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

PRISONER PETITIONS

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

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

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

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

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

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

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

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

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

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

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

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

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
Class Action Fairness Act, 28 U.S.C. § 1332(d)(2); 28 U.S.C. §1391(b)(1)

Brief description of cause:
Data Breach of defendant's computer system

VII. REQUESTED IN COMPLAINT:

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

DEMAND $

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
Apr 20, 2022

SIGNATURE OF ATTORNEY OF RECORD
/s/Adam A. Edwards

FOR OFFICE USE ONLY

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

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. Origin. Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

ClassAction.org
