UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

MARIE SNOW and GAIL LEDGERWOOD, individually and on behalf of all others similarly situated, Plaintiffs, v. ERNEST HEALTH, INC., Defendant.	**Case No.: 3:24-cv-01019** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Marie Snow and Gail Ledgerwood ("Plaintiffs"), individually and on behalf of all others similarly situated, by their attorneys, file this class action complaint against Defendant Ernest Health, Inc. ("Defendant" or "Ernest Health"), and in support thereof allege, upon personal knowledge as to their own actions and their counsel's investigation, and upon information and belief as to all other matters, the following:

NATURE OF THE ACTION

1. This class action arises out of a recent cyberattack and data breach ("Data Breach") caused by Defendant's failure to implement reasonable and industry standard data security practices.

2. According to its website, "Ernest Health is a network of rehabilitation and long-term acute care hospitals. Ernest Health hospitals see patients who are often recovering from disabilities caused by injuries or illnesses, or from chronic or complex medical conditions. Ernest Health hospitals are located throughout the United States in Arizona, California, Colorado, Idaho,

Indiana, Montana, New Mexico, Ohio, South Carolina, Texas, Utah, Wisconsin, and Wyoming. Each hospital is managed locally to best meet the needs of each community which is served. Ernest Health hospitals share information, knowledge, and resources — so they can continually evaluate and improve the delivery of care to their patients."[1]

3. Plaintiffs bring this Complaint against Defendant for its failure to properly secure and safeguard the sensitive information that it collected and maintained as part of its regular business practices. Such information included, but was not limited to names, Social Security numbers, driver's license numbers, addresses, dates of birth, ("personally identifying information" or "PII") amd medical record numbers, health insurance plan member IDs, claims data, diagnoses, and prescription information, which is protected health information ("PHI", and collectively with PII, "Private Information") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[2]

4. Upon information and belief, former and current Ernest Health, Inc. patients and employees are required to entrust Defendant with sensitive, non-public Private Information, without which Defendant could not perform its regular business activities, in order to obtain medical services from Defendant. Defendant retains this information for at least many years and even after the patient-physician or employee-employer relationship has ended.

5. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

[1] https://ernesthealth.com/about-us/ (last visited Apr. 21, 2024).
[2] https://www.jdsupra.com/legalnews/patients-of-several-ernest-health-2477780/ (last visited Apr. 21, 2024).

6. According to the letters that Defendant sent to Plaintiffs and other impacted Class Members (the "Notice Letter")[3] on or about February 1, 2024, Defendant became aware of "unusual activity in [its] Information Technology environment," prompting an investigation wherein it was "determined that an authorized party gained access to [Defendant's] IT network between the dates of January 16, 2024 and February 4, 2024. While in [Defendant's] IT network, the unauthorized party accessed and/or acquired files that contain" Private Information pertaining to former and current patients and employees, including but not limited to Social Security numbers.[4]

7. Defendant failed to adequately protect Plaintiffs' and Class Members' Private Information—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and an utter failure to protect its patients' sensitive data. Hackers targeted and obtained Plaintiffs' and Class Members' Private Information because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes. By their Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose PII and PHI was accessed during the Data Breach.

8. In breaching their duties to properly safeguard Private Information and provide timely, adequate notice of the Data Breach's occurrence, Defendant's conduct amounts to negligence and/or recklessness and violates federal and state statutes.

[3] Each member hospital within Defendant's network sent slightly varied letters to affected individuals, but in sum and substance the contents therein were consistent throughout. *Compare* letter addressed to Plaintiff Snow from Mountain Valley Regional Rehabilitation Hospital (attached as Ex. A) with letter addressed to Plaintiff Ledgerwood from Lafayette Regional Rehabilitation Hospital (attached as Ex. B).
[4] *See* Exs. A & B.

9. Plaintiffs bring this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents.

10. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the Private Information of Plaintiffs and Class Members 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 Private Information of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

11. Plaintiffs and Class Members have suffered injuries as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third

parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

12. Plaintiffs seeks to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

PARTIES

13. Plaintiff Marie Snow is and has been, at all relevant times, a resident and citizen of Yavapai County, Arizona. Plaintiff Snow was treated as a patient at Defendant's Mountain Valley Regional Rehabilitation Hospital in or around 2022.

14. Plaintiff Gail Ledgerwood is and has been, at all relevant times, a resident and citizen of Clinton County, Indiana. Plaintiff Ledgerwood worked as an employee at Defendant's Lafayette Regional Rehabilitation Hospital between 2016 and 2024.

15. Defendant Ernest Health, Inc. is a corporation formed under the state laws of Delaware, with its principal place of business located 1024 N. Galloway Ave. Suite 102, Mesquite, Texas 75149. Ernest Health, Inc. is a citizen of Texas. Defendant Ernest Health's registered agent for service of process is Corporate Creations Network, Inc., 5444 Westheimer, St. 1000, Houston, Texas 77056.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and

minimal diversity exists because many putative class members are citizens of a different state than Defendant. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

17. This Court has personal jurisdiction over Defendant because it operates and maintains its principal place of business in the Dallas Division of the Northern District of Texas.

18. Venue is proper in the Dallas Division of the Northern District of Texas under 28 U.S.C. § 1391(a) through (d) because Defendant's principal place of business is located in Dallas Division of the Northern District of Texas and Defendant maintains Class Members' Private Information in this District.

STATEMENT OF FACTS

Defendant's Business

19. Defendant operates a network of rehabilitation and long-term acute care hospitals numbering in the dozens throughout 13 states.[5] Its hospitals "have been ranked in the top 10% nationally by the Uniform Data System for Medical Rehabilitation."[6]

20. In order to obtain medical services from Defendant, Defendant requires its patients to provide sensitive and confidential Private Information, including their names, insurance information, dates of birth, and other personal information.

21. Similarly, as a condition of employment, prospective employees are required to provide sensitive and confidential Private Information, including social security numbers.

22. The information held by Defendant in its computer systems included the unencrypted Private Information of Plaintiffs and Class Members.

[5] https://ernesthealth.com/about-us/ (last visited Apr. 21, 2024).
[6] *See supra* fn. 1.

23. Upon information and belief, Defendant made promises and representations to its patients and employees that their information would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

24. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

25. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiffs and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

26. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep Plaintiffs' and Class Members' Private Information safe and confidential.

27. Defendant had obligations created by the FTC Act, HIPAA, contract, and industry standards, to keep its patients' and employees' Private Information confidential and to protect it from unauthorized access and disclosure.

28. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform the services it provides, and in turn generate the revenue it does.

29. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

The Data Breach

30. On or about March 29, 2024, Defendant began sending Plaintiffs and other victims of the Data Breach the "Notice Letter", informing them, in relevant part, that:

> On February 1, 2024, we were alerted to unusual activity in our Information Technology ("IT") environment. In response, we promptly secured and isolated our IT systems. We also commenced an investigation with assistance from a third-party cybersecurity firm and have been in communication with law enforcement ….
>
> Through our ongoing investigation, we determined that an unauthorized party gained access to our IT network between the dates of January 16, 2024 and February 4, 2024. While in our IT network, the unauthorized party accessed and/or acquired files that contain information pertaining to certain patients, including their names and one or more of the following: addresses, dates of birth, medical record numbers, health insurance plan member IDs, claims data, diagnosis, and/or prescription information. For some patients, this information may have included their Social Security and/or driver's license numbers.[7]

31. Omitted from the Notice Letter were the dates of Defendant's investigation, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

32. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach's critical facts. Without

[7] *See* Ex. A. Victims of the Data Breach who were employees rather than patients received slightly different letters, however the pertinent details did not vary from those received by pateints. *See* Ex. B.

these details, the ability to mitigate the harms resulting from the Data Breach is severely diminished.

33. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

34. The attacker accessed and acquired files in Defendant's computer systems containing unencrypted Private Information of Plaintiffs and Class Members, including their names, dates of birth, PHI, and other sensitive information. Plaintiffs' and Class Members' Private Information was accessed and stolen in the Data Breach.

35. Plaintiffs further believe that their Private Information and that of Class Members was or will be sold on the dark web, as that is the modus operandi of cybercriminals that commit cyber-attacks of this type.

Data Breaches Are Preventable

36. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[8]

37. To prevent and detect cyber-attacks and/or ransomware attacks 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.

[8] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

- 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 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.[9]

[9] *Id.* at 3-4.

38. To prevent and detect cyber-attacks or ransomware attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

> **Secure internet-facing assets**
>
> - Apply latest security updates
> - Use threat and vulnerability management
> - Perform regular audit; remove privileged 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**
>
> - 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
> - Analyze logon events
> - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[10]

[10] *See* Human-operated ransomware attacks: A preventable disaster (Mar. 5, 2020), *available at:*

39. Given that Defendant was storing the sensitive Private Information of its patients (and its employees), Defendant could and should have implemented the above measures to prevent and detect cyberattacks.

40. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of a large number of people, including that of Plaintiffs and Class Members.

Defendant Acquires, Collects, & Stores Plaintiffs' and Class Members' Private Information

41. As a condition to obtain medical services from Defendant, Defendant requires its patients to give their sensitive and confidential Private Information to Defendant

42. Similarly, as a condition of employment to work for Defendant, Defendant requires prospective employees to give their sensitive and confidential Private Information to Defendant.

43. Defendant retains and stores this information and derives a substantial economic benefit from the Private Information that it collects. But for the collection of Plaintiffs' and Class Members' Private Information, Defendant would be unable to perform its services.

44. By obtaining, collecting, and storing the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the Private Information from disclosure.

45. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private

https://microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

46. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiffs and Class Members.

47. Upon information and belief, Defendant made promises to its patients (and employees) to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

48. Defendant's negligence in safeguarding the Private Information of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Defendant Knew, Or Should Have Known, of the Risk Because Healthcare Entities in Possession of Private Information Are Particularly Susceptible to Cyber Attacks

49. Data thieves regularly target health care providers like Defendant due to the highly sensitive information that they keep. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

50. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare entities that collect and store Private Information and other sensitive information, like Defendant, preceding the date of the breach.

51. In the third quarter of the 2023 fiscal year alone, 7,333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[11]

52. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

53. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[12]

54. Additionally, as companies became more dependent on computer systems to run their business,[13] *e.g.*, working remotely as a result of the COVID-19 pandemic, and the Internet of

[11] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/
[12] https://www.law360.com/articles/1220974/ (last accessed Apr. 21, 2024).
[13] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html (last accessed Apr. 21, 2024).

Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[14]

55. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being compromised.

56. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

57. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

58. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on its server(s), and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

59. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

[14] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022 (last accessed Apr. 21, 2024).

60. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen—particularly PHI—fraudulent use of that information and damage to victims may continue for years.

61. As a healthcare entity in possession of its patients' and other individuals' Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

Value of Private Information

62. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[15] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's

[15] 17 C.F.R. § 248.201 (2013).

license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[16]

63. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[17]

64. For example, Private Information can be sold at a price ranging from $40 to$200.[18] Criminals can also purchase access to entire company data breaches from $900 to $4,500.19.[19]

65. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected." [20]

66. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information (e.g., patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, Private Information is a valuable commodity for which a "cyber black market" exists where criminals openly post stolen payment card numbers, Social Security numbers, and other

---

[16] *Id.*
[17] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/
[18] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/
[19] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/
[20] https://efraudprevention.net/home/education/?a=187#:%7E:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected

personal information on several underground internet websites. Unsurprisingly, the pharmaceutical industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

67. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[21] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[22] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[23]

68. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[24]

69. A study by Experian found that the average cost of medical identity theft is "about $20,000" per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.[25] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-

[21] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/
[22] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/
[23] https://www.tenabhle.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches/
[24] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/
[25] *See* Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/

third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[26]

70. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible to change – names, dates of birth, and PHI.

71. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[27]

72. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

73. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may

[26] Id.; *see also* Healthcare Data Breach: What to Know About them and What to Do After One, EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-toknow-about-them-and-what-to-do-after-one/

[27] Tim Greene, Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers, IT World, (Feb. 6, 2015), available at: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html

> continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[28]

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

Defendant Fails to Comply with FTC Guidelines

75. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which 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.

76. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal patient 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.[29]

77. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[30]

---

[28] Report to Congressional Requesters, GAO, at 29 (June 2007), available at: https://www.gao.gov/assets/gao-07-737.pdf

[29] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

[30] *Id.*

78. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive 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.

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

80. These FTC enforcement actions include actions against healthcare entities, like Defendant. *See, e.g., In the Matter of LabMD, Inc., a corp*, 2016-2 Trade Cas. (MMRGH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

81. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

82. Defendant failed to properly implement basic data security practices.

83. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Private Information it stored or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

84. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Private Information of its patients and employees. Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

Defendant Fails to Comply with HIPAA Guidelines

85. Defendant is a business associate under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

86. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[31] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

87. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

[31] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

88. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

89. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

90. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

91. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

92. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]mplement 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." 45 C.F.R. § 164.312(a)(1).

93. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. See 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); see also 42 U.S.C. §17902.

94. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[32]

95. HIPAA requires a business associate to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the business associate or the requirements of 45 C.F.R. Part 164, Subparts D or E. See 45 C.F.R. § 164.530(e).

96. HIPAA requires a business associate to mitigate, to the extent practicable, any harmful effect that is known to the business associate of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

97. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. See 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the

[32] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[33] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[34]

Defendant Fails to Comply with Industry Standards

98. As noted above, experts studying cyber security routinely identify healthcare entities in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

99. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities like Defendant in possession of Private Information, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

100. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems;

[33] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.
[34] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

protection against any possible communication system; and training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

101. Upon information and belief Defendant failed to meet the minimum standards of one or more of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

102. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and upon information and belief, Defendant failed to comply with at least one––or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

COMMON INJURIES & DAMAGES

103. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for

unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

The Data Breach Increases Victims' Risk of Identity Theft

104. The unencrypted Private Information of Plaintiffs and Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

105. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class Members. Simply, unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

106. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

107. Plaintiffs' and Class Members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and Class Members and to profit off their misfortune.

108. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[35]

[35] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited

109. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

110. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

111. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiffs and the other Class Members.

112. Thus, even if certain information was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

---

to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. See, e.g., Brian Krebs, Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/.

113. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss Of Time to Mitigate the Risk of Identity Theft and Fraud

114. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

115. Thus, due to the actual and imminent risk of identity theft, Defendant offers, in its Notice Letter, one year of complimentary credit to Plaintiffs and Class Members whose Social Security and/or driver's license numbers were involved in the Data Breach.[36] Moreover, Defendant reminds victims "to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity."[37]

116. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach, replacing credit cards, and monitoring their financial accounts for any indication of fraudulent activity, which may take years to detect.

117. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in

[36] *See* Exs. A & B.
[37] *Id.*

which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[38]

118. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[39]

119. And for those Class Members who experience actual identity theft and fraud, GAO Report notes that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[40]

Diminution Of Value of PII and PHI

120. PII and PHI are valuable property rights.[41] Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy

[38] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.
[39] *See* Federal Trade Commission, Identity Theft.gov, https://www.identitytheft.gov/Steps
[40] *See* GAO Report, p. 2
[41] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

121. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[42]

122. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[43]

123. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[44] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[45]

124. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[46]

125. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

---

[42] See Ashiq Ja, Hackers Selling Healthcare Data in the Black Market, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/
[43] https://www.latimes.com/business/story/2019-11-05/column-data-brokers
[44] https://datacoup.com/
[45] https://digi.me/what-is-digime/
[46] Lisa Vaas, Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content

126. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

127. The fraudulent activity resulting from the Data Breach may not come to light for years.

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

129. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendants network, amounting to a large number of individual's detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

130. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

131. Given the type of targeted attack in this case, sophisticated criminal activity, and the type of Private Information involved, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes–e.g.,

opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

132. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

133. Consequently, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

134. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach.

Loss of Benefit of the Bargain

135. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to obtain medical services from Defendant under certain terms (or to become employed with Defendant), Plaintiffs and other reasonable patients understood and expected that Defendant would properly safeguard and protect their Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received medical services (or employment benefits) of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

PLAINTIFFS' EXPERIENCE

136. Plaintiff Snow is a former patient who was treated at Defendant's Mountain Valley Regional Rehabilitation Hospital, which is located in Arizona, in or around 2022.

137. As a condition of obtaining services at Ernest Health, Plaintiff Snow was required to provide Defendant with her Private Information, including her name, social security number, health insurance information, date of birth, and other sensitive information.

138. Plaintiff Ledgerwood is a former employee who worked at Defendant's Lafayette Regional Rehabilitation Hospital, which is located in Indiana, between 2016 and 2024.

139. As a condition of employment with Ernest Health, Plaintiff Ledgerwood was required to provide Defendant with her Private Information, including her name, social security number, date of birth, and other sensitive information.

140. Upon information and belief, at the time of the Data Breach, Defendant had retained Plaintiffs' Private Information on its system.

141. Plaintiffs are very careful about sharing their sensitive Private Information. Plaintiffs store any documents containing their Private Information in a safe and secure location. Had Plaintiffs known that Defendant would fail to implement reasonable and adequate data security safeguards, they would not have provided their Private Information to Ernest Health or any entity that provided their information, directly or indirectly to Defendant.

142. Plaintiffs received the Notice Letter, by U.S. mail in or around late March or early April 2024, informing them that their Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach.

143. In particular, Plaintiff Snow was advised that her Private Information that may have been accessed includes her name, address, date of birth, social security number, driver's license number, medical record number, claims data, diagnosis, and/or prescription information.[47]

144. Similarly, Plaintiff Ledgerwood was advised that her Private Information that may have been accessed includes her social security number.[48]

145. As a result of the Data Breach and at the direction of the Notice Letter, which instructed them "to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity,"[49] Plaintiffs made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach, and monitoring their financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiffs have spent significant time remedying the breach—valuable time Plaintiffs otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

146. Plaintiffs suffered actual injury from having their Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which:

[47] *See* Ex. A.
[48] *See* Ex. B.
[49] *See* Exs. A & B.

(a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

147. Plaintiffs further suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

148. The Data Breach has caused Plaintiffs to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed them of key details about the Data Breach's occurrence.

149. As a result of the Data Breach, Plaintiffs anticipate spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

150. As a result of the Data Breach, Plaintiffs are at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

151. Plaintiffs have a continuing interest in ensuring that their Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

152. Pursuant to Federal Rule of Civil Procedure 23, Plaintiffs proposes the following Class and Sub-Class definitions, subject to amendment as appropriate:

> All persons whose Private Information was maintained on Defendant's computer systems that were compromised in the Data Breach announced by Defendant on or about March 29, 2024 (the "Class").

All members of the Class who either: (i) resided in the State of Arizona at the time of the Data Breach; and/or (ii) provided their Private Information to Defendant at one of its facilities located in the State of Arizona (the "Arizona Sub-Class").
All members of the Class who either: (i) resided in the State of Indiana at the time of the Data Breach; and/or (ii) provided their Private Information to Defendant at one of its facilities located in the State of Indiana (the "Indiana Sub-Class").

153. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

154. Plaintiffs hereby reserve the right to amend or modify the Class definition with greater specificity or division after having had an opportunity to conduct discovery.

155. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. The exact number of Class Members is unknown to Plaintiffs at this time, but can be determined from Defendant's records.

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

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

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

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breached implied contracts for adequate data security with Plaintiffs and Class Members;

l. Whether Defendant was unjustly enriched by retention of the monetary benefits conferred on it by Plaintiffs and Class Members;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and,

n. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

157. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

158. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel is competent and experienced in litigating class actions.

159. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' Private Information was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

160. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

161. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

162. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

b. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

163. Finally, all Members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent the Notice Letter by Defendant.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

164. Plaintiffs repeat, re-allege, and incorporate by reference, all other paragraphs of this complaint.

165. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of its business of soliciting its services, which solicitations and services affect commerce.

166. Plaintiffs and Class Members entrusted Defendant with their Private Information with the understanding that Defendant would safeguard their information.

167. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information were wrongfully disclosed.

168. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

169. Defendant had a duty to employ reasonable security measures under Section 5 of the FTC 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.

170. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

171. For instance, HIPAA required Defendant, *inter alia, to act* promptly. However, despite allegedly learning of the breach on February 1, 2024, Defendant's system continued to be breached up and through February 4, 2024, demonstrating its response to learning of the Data Breach was unreasonable.

172. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

173. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential Private Information, a necessary part of being patients of Defendant.

174. 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.

175. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Class.

176. Defendant also had a duty to exercise appropriate practices to remove former patients' Private Information once it was no longer required to retain pursuant to regulations.

177. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

178. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiffs and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

179. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. 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 their networks and systems;

c. Failing to periodically ensure that its email system had reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

f. Failing to remove former patients' and employees' Private Information it was no longer required to retain pursuant to regulations,

g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

180. Defendant violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

181. Plaintiffs and the Class are within the class of persons that the FTC Act and HIPAA were intended to protect.

182. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against.

183. Defendant's violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

184. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

185. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

186. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

187. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

188. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

189. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

190. Plaintiffs and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

191. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

192. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the

actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

193. Defendant has admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

194. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

195. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The Private Information of Plaintiffs and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

196. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's

possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

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

198. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

199. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

200. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and insecure manner.

201. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE
(On Behalf of Plaintiffs and the Class)

202. Plaintiffs repeat, re-allege, and incorporate by reference, all other paragraphs of this complaint.

203. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

204. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

205. For instance, HIPAA required Defendant, *inter alia*, to act promptly. However, despite allegedly learning of the breach on February 1, 2024, Defendant's system continued to be breached up and through February 4, 2024, demonstrating its response to learning of the Data Breach was unreasonable.

206. Defendant violated Section 5 of the FTC Act, HIPAA, and similar state statutes by failing to use reasonable measures to protect Private Information and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

207. Defendant's violation of Section 5 of the FTC Act, HIPAA, and similar state statutes constitutes negligence *per se*.

208. Class Members are consumers within the class of persons Section 5 of the FTC Act, HIPAA, and similar state statutes were intended to protect.

209. Moreover, the harm that has occurred is the type of harm the FTC Act, HIPAA, and similar state statutes were intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class Members.

210. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered or will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

211. Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

212. Plaintiffs repeat, re-allege, and incorporate by reference, all other paragraphs of this complaint.

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

214. In its member hospitals' Notices of Privacy Practices, Defendant represented that it would not disclose Plaintiffs' and Class Members' Private Information to unauthorized third parties.[50]

215. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

216. When Plaintiffs and Class Members provided their Private Information to Defendant in exchange for Defendant's services, they entered into protect such information and to destroy any Private Information that it was no longer required to maintain.

217. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Defendant on the other, is demonstrated by their conduct and course of dealing.

218. Defendant solicited, offered, and invited Plaintiffs and Class Members to provide their Private Information as part of Defendant's regular business practices.

219. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

[50] *See, e.g.*, https://lrrh.ernesthealth.com/wp-content/uploads/sites/9/2023/04/HIPAA_LRRH_Digital.pdf and https://mvrrh.ernesthealth.com/wp-content/uploads/sites/16/2023/04/HIPAA_MVHH_Digital2.pdf (each last accessed Apr. 21, 2024).

220. In accepting the Private Information of Plaintiffs and Class Members, Defendant understood and agreed that they were required to reasonably safeguard the Private Information from unauthorized access or disclosure.

221. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, the FTC Act, and were consistent with industry standards.

222. As a result of services contracted by Plaintiffs and Class Members, Defendant earned money with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

223. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

224. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

225. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

226. Defendant breached its implied contracts with Plaintiffs and Class Members by failing to safeguard and protect their Private Information or to destroy it once it was no longer necessary to retain the Private Information.

227. As a direct and proximate result of Defendant's breach of the implied promises, Plaintiffs and Class Members are at a current and ongoing risk of identity theft, and Plaintiffs and Class Members sustained incidental and consequential damages including: (a) financial "out of

pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) financial "out of pocket" costs incurred due to actual identity theft; (d) spam and targeted marketing emails; (f) diminution of value of their Private Information; (g) future costs of identity theft monitoring; (h) and the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

228. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach to be determined at trial.

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

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
[In the Alternative]
(On Behalf of Plaintiffs and the Class)

230. Plaintiffs repeat, re-allege, and incorporate by reference, all other paragraphs of this complaint.

231. Plaintiffs brings this claim in the alternative to their breach of implied contract claim.

232. Plaintiffs and Class Members conferred a benefit on Defendant. Specifically, they provided Defendant with their Private Information. In exchange, Plaintiffs and Class Members should have had their Private Information protected with adequate data security.

233. Defendant knew that Plaintiffs and Class Members conferred a benefit on it in the form of their Private Information. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

234. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiff and some Class Members.

235. As such, a portion of the payments made for the benefit of or on behalf of Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

236. Defendant, however, failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide adequate data security in return for the benefit Plaintiffs and Class Members provided.

237. Defendant would not be able to carry out an essential function of its regular business without the Private Information of Plaintiffs and Class Members and derived revenue by using it for business purposes. Plaintiffs and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

238. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

239. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have allowed their Private Information to be provided to Defendant.

240. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

241. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained from Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

242. Plaintiffs and Class Members have no adequate remedy at law.

243. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in

Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

244. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

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

FIFTH CAUSE OF ACTION
VIOLATION OF THE ARIZONA CONSUMER FRAUD ACT (ACFA)
ARIZONA REV. STAT. §§ 44-1521, ET SEQ.
(On Behalf of Plaintiffs and the Arizona Sub-Class)

246. Plaintiffs repeat, re-allege, and incorporate by reference, all other paragraphs of this complaint.

247. The ACFA provides in pertinent part: "The act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in face been misled, deceived or damaged thereby, is declared to be an unlawful practice." Ariz. Rev. Stat. § 44-1522.

248. Plaintiff Snow and Arizona Sub-Class Members are "persons" as defined by Ariz. Rev. Stat. § 44-1521(6).

249. Defendant provides "services" as that term is included in the definition of "merchandise" under Ariz. Rev. Stat. § 44-1521(5), and Defendant is engaged in the "sale" of "merchandise" as defined by Ariz. Rev. Stat. § 44-1521(7).

250. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression and omission of material facts in connection with the sale and advertisement of "merchandise" (as defined in the ACFA) in violation of the ACFA, including but not limited to the following:

a. Failing to maintain sufficient security to keep Plaintiff Snow's and Arizona Sub-Class Members' confidential medical and personal data from being hacked and stolen;

b. Failing to disclose the Data Breach to Plaintiff Snow's and Arizona Sub-Class Members in a timely and accurate manner, in violation of Ariz. Rev. Stat. § 18-552(B);

c. Failing to adequately monitor the security of their networks and systems;

d. Misrepresenting material facts, pertaining to the sale of healthcare services by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff Snow's and Arizona Sub-Class Members' PHI and PII from unauthorized disclosure, release, data breaches, and theft;

e. Misrepresenting material facts, in connection with the sale of healthcare services by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff Snow's and Arizona Sub-Class Members' PHI and PII;

f. Omitting, suppressing, and concealing the material fact of the inadequacy of the data privacy and security protections for Plaintiff Snow's and Arizona Sub-Class Members' PHI and PII;

g. Engaging in unfair, unlawful, and deceptive acts and practices with respect to the sale of healthcare services by failing to maintain the privacy and security of Plaintiff Snow's and Arizona Sub-Class Members' PHI and PII, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws, including HIPAA and Section 5 of the FTC Act;

h. Engaging in unlawful, unfair, and deceptive acts and practices with respect to the sale of healthcare services by failing to disclose the Data Breach to Plaintiff Snow's and Arizona Sub-Class Members in a timely and accurate manner; and

i. Engaging in unlawful, unfair, and deceptive acts and practices with respect to the sale of healthcare services by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff Snow's and Arizona Sub-Class Members' PHI and PII from further unauthorized disclosure, release, data breaches, and theft

251. The above unlawful, unfair, and deceptive acts and practices by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff Snow and Arizona Sub-Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

252. Defendant knew or should have known that their computer systems and data security practices were inadequate to safeguard Plaintiff Snow's and Arizona Sub-Class Members' PHI and PII and that risk of a data breach or theft was high, especially in light of the frequency of Data Breaches in the healthcare industry.

253. Defendant's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Members of the Class.

254. As a direct and proximate result of Defendant's deceptive acts and practices, Plaintiff Snow and Arizona Sub-Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their PHI and PII.

255. Plaintiff Snow, individually and on behalf of Arizona Sub-Class Members, seek reliefs under the ACFA including, but not limited to, injunctive relief, actual damages, treble damages for each willful or knowing violation, and attorneys' fees and costs.

SIXTH CAUSE OF ACTION
VIOLATION OF THE INDIANA DECEPTIVE CONSUMER SALES ACT (IDCSA)
IND. CODE §§ 24-5-0.5-1, ET SEQ.
(On Behalf of Plaintiffs and the Indiana Sub-Class)

256. Plaintiffs repeat, re-allege, and incorporate by reference, all other paragraphs of this complaint.

257. Indiana's Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5-3(a) ("IDCSA") prohibits suppliers from engaging in deceptive, unfair, and abusive acts or omissions in consumer transactions.

258. Defendant is a "person" as defined by Ind. Code § 24-5-05-2(a)(2).

259. Defendant is a "supplier" as defined by § 24-5-0.5-2(a)(1), because it regularly engages in or solicits "consumer transactions," within the meaning of § 24-5-0.5-2(a)(3)(A). As a regular part of its business, Ernest Health sells medical services. In doing so, it requires consumers such as Plaintiff Ledgerwood and Indiana Sub-Class Members to provide their Private

Information. These transactions were directed towards Indiana, and on information and belief, those transactions were processed in Indiana and the information resulting from those transactions was stored in Indiana.

260. In connection with its consumer transactions, Defendant engaged in unfair, abusive or deceptive acts, omissions or practices by, inter alia, engaging in the following conduct: failing to maintain sufficient security to keep sensitive Private Information of Plaintiff Ledgerwood and Indiana Sub-Class Members from being hacked and stolen; misrepresenting and/or omitting material facts to Plaintiff Ledgerwood and Indiana Sub-Class Members in connection with the sale of goods and services, by representing that it would maintain adequate data privacy and security practices and procedures to safeguard their Private Information from unauthorized disclosure, release, data breaches, and theft; and, misrepresenting and/or omitting material facts to Plaintiff Ledgerwood and Indiana Sub-Class Members in connection with the sale of goods and services, by representing that Defendant did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of their Private Information.

261. Defendant knew that its computer systems and data security practices were inadequate to safeguard the Private Information of Plaintiff Ledgerwood and Indiana Sub-Class Members, and that risk of a data breach or theft was highly likely. Nevertheless, it did nothing to warn them about its data insecurities, and instead affirmatively promised that it would maintain adequate security. This was a deliberate effort to mislead consumers, such as Plaintiff Ledgerwood and Indiana Sub-Class Members, in order to encourage them to provide their Private Information in order to obtain medical services even while Defendant knew that sensitive Private Information it came into possession of was vulnerable.

262. Defendant had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the PHI in its possession, and the generally accepted professional standards. This duty arose due to the representations and relationship between Defendant and Plaintiff Ledgerwood and Indiana Sub-Class Members as described herein.

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

264. Plaintiffs and the Class seek all relief allowed by law, including the greater of actual damages or $500 for each violation; the greater of treble damages or $1,000 for each willful violation; restitution; reasonable attorneys' fees and costs; injunctive relief; and punitive damages.

SEVENTH CAUSE OF ACTION
DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and the Class)

265. Plaintiffs repeat, re-allege, and incorporate by reference, all other paragraphs of this complaint.

266. 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 to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious, and which violate the terms of the federal and state statutes described above.

267. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to employing reasonable data security. Plaintiffs alleges Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiffs and the Class continue to suffer injury due to the continued and ongoing threat of new or additional fraud against them or on their accounts using the stolen data.

268. Under its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following: Defendant owed, and continues to owe, a legal duty to employ reasonable data security to secure the PII it possesses, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act; Defendant breached, and continues to breach, its duty by failing to employ reasonable measures to secure its customers' personal and financial information; and Defendant's breach of its legal duty continues to cause harm to Plaintiffs and the Class.

269. The Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect its employees' (i.e., Plaintiffs and the Class's) data.

270. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendant's data systems. If another breach of Defendant's data systems occurs, Plaintiffs and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiffs and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered

by Plaintiffs and the Class, which include monetary damages that are not legally quantifiable or provable.

271. The hardship to Plaintiffs and the Class if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued.

272. 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, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and Class Members, requests judgment against Defendant and that the Court grants the following:

a) For an Order certifying this action as a class action and appointing Plaintiffs and their 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 Plaintiffs' and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs 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 injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members;

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

f) Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiffs and the Class;

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

h) For an award of punitive damages, as allowable by law;

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

j) Pre- and post-judgment interest on any amounts awarded; and

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

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: April 26, 2024

Respectfully Submitted,

s/ Joe Kendall
JOE KENDALL
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 825
Dallas, Texas 75219
Phone:214-744-3000
Fax: 214-744-3015
jkendall@kendalllawgroup.com

Interim Local Counsel for Plaintiff and the Putative Class

Jeffrey S. Goldenberg (*pro hac vice forthcoming*)
GOLDENBERG SCHNEIDER, LPA
4445 Lake Forest Drive, Suite 490
Cincinnati, Ohio 45242
Telephone: (513) 345-8291

jgoldenberg@gs-legal.com

Charles E. Schaffer (*pro hac vice forthcoming*)
LEVIN SEDRAN & BERMAN
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Telephone: (215) 592-1500
cschaffer@lfsblaw.com

LEEDS BROWN LAW, P.C.
Jeffrey K. Brown (*pro hac vice forthcoming*)
Brett R. Cohen (*pro hac vice forthcoming*)
One Old Country Road, Suite 347
Carle Place, NY 11514-1851
Tel: (516) 873-9550
jbrown@leedsbrownlaw.com
bcohen@leedsbrownlaw.com
Counsel for Plaintiff and the Putative Class

EXHIBIT A

Mountain Valley Regional Rehabilitation Hospital
Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Marie L Snow
[redacted]
91080

March 29, 2024

Dear Marie L Snow:

Mountain Valley Regional Rehabilitation Hospital is committed to protecting the confidentiality and security of the information we maintain. We are writing to let you know about a data security incident that may have involved some of your information. This letter explains the incident, measures that have been taken, and some steps you can take in response to protect your information.

On February 1, 2024, we were alerted to unusual activity in our Information Technology ("IT") environment. In response, we promptly secured and isolated our IT systems. We also commenced an investigation with assistance from a third-party cybersecurity firm and have been in communication with law enforcement.

Through our ongoing investigation, we determined that an unauthorized party gained access to our IT network between the dates of January 16, 2024 and February 4, 2024. While in our IT network, the unauthorized party accessed and/or acquired files that contain information pertaining to certain patients. Our investigation cannot rule out the possibility that, as a result of this incident, files containing some of your information may have been subject to unauthorized access. This information may have included your name and one or more of the following: address, date of birth, Social Security number, driver's license number, medical record number, claims data, diagnosis, and/or prescription information.

As a precaution, we are offering you a complimentary one-year membership to Identity Defense Complete, which includes credit monitoring and fraud alerts. **For more information on identity theft prevention and Identity Defense Complete, including instructions on how to activate your complimentary membership, please see the pages following this letter.**

We deeply regret any inconvenience or concern this incident may cause and take this matter seriously. To help prevent something like this from happening again, we have implemented, and will continue to adopt, additional safeguards and technical security measures to further protect and monitor our systems. If you have any questions about this incident, please call 1-844-563-2187, Monday through Friday, between 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely,

Joshua Davis

Joshua Davis
CEO

Identity Defense

Enter your Activation Code: [redacted]
Enrollment Deadline: July 2, 2024
Service Term: 12 months *

Identity Defense Complete

Key Features

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- $1 Million Identity Theft Insurance**

Enrollment Instructions

To enroll in Identity Defense, visit https://app.identitydefense.com/enrollment/activate/erne

1. Enter your unique Activation Code [redacted]
   Enter your Activation Code and click 'Redeem Code'.
2. Create Your Account
   Enter your email address, create your password, and click 'Create Account'.
3. Register
   Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
4. Complete Activation
   Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is July 2, 2024. After July 2, 2024, the enrollment process will close, and your Identity Defense code will no longer be active. **If you do not enroll by July 2, 2024, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.**

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at 1.866.622.9303.

*Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.
**Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report. For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Mountain Valley Regional Rehabilitation Hospital's mailing address is 3700 North Windsong Drive, Prescott Valley, AZ 86314 and its phone number is 928-759-8800.

Additional information for residents of the following states:

Maryland Residents: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.marylandattorneygeneral.gov

New York Residents: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina Residents: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island Residents: Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

West Virginia Residents: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a 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.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

EXHIBIT B

Lafayette Regional Rehabilitation Hospital
Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Gail M Ledgerwood
[redacted]
42037

March 29, 2024

Dear Gail M Ledgerwood:

Lafayette Regional Rehabilitation Hospital is committed to protecting the confidentiality and security of the information we maintain. We are writing to let you know about a data security incident that may have involved some of your information. This letter explains the incident, measures that have been taken, and some steps you can take in response to protect your information.

What Happened: On February 1, 2024, we were alerted to unusual activity in our Information Technology ("IT") environment. In response, we promptly secured and isolated our IT systems. We also commenced an investigation with assistance from a third-party cybersecurity firm and have been in communication with law enforcement. Through our ongoing investigation, we determined that an unauthorized party gained access to our IT network between the dates of January 16, 2024 and February 4, 2024. While in our IT network, the unauthorized party accessed and/or acquired files that contain information pertaining to certain current and former employees.

What Information was Involved: Our investigation cannot rule out the possibility that, as a result of this incident, files containing some of your information may have been subject to unauthorized access. This information may have included your name and one or more of the following: Social Security number.

What We Are Doing: To help prevent something like this from happening again, we have implemented, and will continue to adopt, additional safeguards and technical security measures to further protect and monitor our systems.

What You Can Do: As a precaution, we are offering you a complimentary one-year membership to Identity Defense Complete, which includes credit monitoring and fraud alerts. **For more information on identity theft prevention and Identity Defense Complete, including instructions on how to activate your complimentary membership, please see the pages following this letter.**

For More Information: We deeply regret any inconvenience or concern this incident may cause and take this matter seriously. If you have any questions about this incident, please call 1-844-563-2187, Monday through Friday, between 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely,

Logan Savage

Logan Savage
CEO

Identity Defense

Enter your Activation Code: [redacted]
Enrollment Deadline: July 2, 2024
Service Term: 12 months *

Identity Defense Complete

Key Features

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- $1 Million Identity Theft Insurance**

Enrollment Instructions

To enroll in Identity Defense, visit https://app.identitydefense.com/enrollment/activate/erne [redacted]

1. Enter your unique Activation Code
   Enter your Activation Code and click 'Redeem Code'.
2. Create Your Account
   Enter your email address, create your password, and click 'Create Account'.
3. Register
   Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
4. Complete Activation
   Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is July 2, 2024. After July 2, 2024, the enrollment process will close, and your Identity Defense code will no longer be active. **If you do not enroll by July 2, 2024, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.**

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at 1.866.622.9303.

*Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.
**Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report. For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Lafayette Regional Rehabilitation Hospital's mailing address is 950 Park East Blvd, Lafayette, IN 47905 and its phone number is 765-447-4040.

Additional information for residents of the following states:

Maryland Residents: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.marylandattorneygeneral.gov

New York Residents: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina Residents: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island Residents: This incident involves 7 individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

West Virginia Residents: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a 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.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

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

MARIE SNOW and GAIL LEDGERWOOD, individually and on behalf of all others similarly situated

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Joe Kendall, Kendall Law Group, PLLC, 3811 Turtle Creek Blvd., Suite 825, Dallas, TX 75219, 214/744-3000

DEFENDANTS

ERNEST HEALTH, INC.

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

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

Attorneys *(If Known)*

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

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

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

(For Diversity Cases Only)

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

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

Click here for: Nature of Suit Code Descriptions.

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

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

PROPERTY RIGHTS
- ❒ 820 Copyrights
- ❒ 830 Patent
- ❒ 835 Patent - Abbreviated New Drug Application
- ❒ 840 Trademark

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
- ❒ 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)***:
28 U.S.C. § 1332(d)

Brief description of cause:
Data Breach

VII. REQUESTED IN COMPLAINT:

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

DEMAND $

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ❒ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE SEE ATTACHMENT DOCKET NUMBER

DATE 04/26/2024

SIGNATURE OF ATTORNEY OF RECORD /s/ Joe Kendall

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

ATTACHMENT TO CIVIL COVER SHEET

VIII. RELATED CASE(S) IF ANY:

Docket No. 3:24-cv-00883-X	Judge Brantley Starr
Docket No. 3:24-cv-00923-X	Judge Brantley Starr
Docket No. 3:24-cv-00973-E	Judge Ada Brown