UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

JOE LARA and **LAURIE COOK**, on behalf of themselves and all others similarly situated, Plaintiffs, v. **ERNEST HEALTH, INC.**, Defendant.	Case No. 3:24-cv-00883 **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Joe Lara and Laurie Cook ("Plaintiffs"), through their attorneys, individually and on behalf of all others similarly situated, bring this Class Action Complaint against Defendant Ernest Health, Inc. ("Ernest Health" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiffs allege the following on information and belief—except as to their own actions, counsel's investigations, and facts of public record.

NATURE OF ACTION

1. This class action arises from Defendant's failure to protect highly sensitive data.

2. Defendant is a "network of rehabilitation and long-term acute care hospitals" with location throughout Arizona, California, Colorado, Idaho, Indiana, Montana, New Mexico, Ohio, South Carolina, Texas, Utah, Wisconsin, and Wyoming.[1]

[1] *About Us*, ERNEST HEALTH, https://ernesthealth.com/about-us/ (last visited April 9, 2024).

3. As such, Defendant stores a litany of highly sensitive personal identifiable information ("PII") and protected health information ("PHI")—together "PII/PHI"—about its current and former patients. But Defendant lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the "Data Breach").

4. It is unknown for precisely how long the cybercriminals had access to Defendant's network before the breach was discovered. In other words, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to its current and former patients' PII/PHI.

5. On information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's PII/PHI. In short, Defendant's failures placed the Class's PII/PHI in a vulnerable position—rendering them easy targets for cybercriminals.

6. Plaintiffs are Data Breach victims, having received breach notices. They bring this class action on behalf of themselves, and all others harmed by Defendant's misconduct.

7. The exposure of one's PII/PHI to cybercriminals is a bell that cannot be unrung. Before this data breach, its current and former patients' private information was exactly that—private. Not anymore. Now, their private information is forever exposed and unsecure.

PARTIES

8. Plaintiff, Laurie Cook, is a natural person and citizen of Idaho. She resides in Post Falls, Idaho where she intends to remain.

9. Plaintiff, Joe Lara, is a natural person and citizen of Texas. He resides in Lubbock, Texas where he intends to remain.

10. Defendant, Ernest Health, Inc., is a corporation incorporated in Delaware with its principal place of business at 1024 N Galloway Ave, Mesquite, Texas 75149. Defendant is a citizen of Texas.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Plaintiff Laurie Cook and Defendant are citizens of different states. And there are over 100 putative Class members.

12. This Court has personal jurisdiction over Defendant because it is headquartered and has its principal place of business in Dallas Division of the Northern District of Texas, regularly conducts business in Texas, and has sufficient minimum contacts in Texas.

13. Venue is proper in this Court because Defendant's principal office is in the Dallas Division of the Northern District of Texas, and because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

BACKGROUND

Defendant Collected and Stored the PII/PHI of Plaintiffs and the Class

14. Defendant is a "network of rehabilitation and long-term acute care hospitals" with location throughout Arizona, California, Colorado, Idaho, Indiana, Montana, New Mexico, Ohio, South Carolina, Texas, Utah, Wisconsin, and Wyoming.[2]

15. As part of its business, Defendant receives and maintains the PII/PHI of thousands of its current and former patients.

[2] *About Us*, ERNEST HEALTH, https://ernesthealth.com/about-us/ (last visited April 9, 2024).

16. In collecting and maintaining the PII/PHI, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiffs and Class members themselves took reasonable steps to secure their PII/PHI.

17. Under state and federal law, businesses like Defendant have duties to protect its current and former patients' PII/PHI and to notify them about breaches.

18. Defendant recognizes these duties, declaring in its "Notice of Privacy Practices" that:

a. "This notice describes how medical information about you may be used."[3]

b. "We are required by law to maintain the privacy and security of your protected health information."[4]

c. "We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information."[5]

d. "We must follow the duties and privacy practices described in this notice and give you a copy of it."[6]

e. "We will not use or share your information other than as described here unless you tell us we can in writing."[7]

Defendant's Data Breach

19. From January 16, 2024, until February 4, 2024, Defendant was hacked.[8]

[3] *Notice of Privacy Practices*, ERNEST HEALTH, https://lsh.ernesthealth.com/wp-content/uploads/sites/34/2023/05/HIPPA_LSH_Digital.pdf (last visited April 9, 2024).
[4] *Id*.
[5] *Id*.
[6] *Id*.
[7] *Id*.
[8] *Notice of Data Security Incident*, ERNEST HEALTH, https://wrrh.ernesthealth.com/wp-content/uploads/sites/30/2024/03/Sub-notice-Weslaco-Regional-Rehabilitation-Hospital.pdf (last visited April 9, 2024).

20. Worryingly, Defendant already admitted that "an unauthorized party gained access to our IT network" and "accessed and/or acquired files that contain information pertaining to [] patients."[9]

21. And Defendant was unable to detect its Data Breach until February 1, 2024—giving cybercriminals free reign to peruse and exfiltrate PII/PHI for 16 uninterrupted days.[10]

22. Because of Defendant's Data Breach, at least the following types of PII/PHI were compromised:

a. names;

b. addresses;

c. dates of birth;

d. medical record numbers;

e. health insurance plan member IDs;

f. claims data;

g. medical diagnoses;

h. prescription information;

i. Social Security numbers; and

j. driver's license numbers.[11]

23. Currently, the precise number of persons injured is unclear. But upon information and belief, the size of the putative class can be ascertained from information in Defendant's custody and control. And upon information and belief, the putative class is over one hundred members—as it includes its current and former patients.

[9] *Id.*
[10] *Id.*
[11] *Id.*

24. And yet, Defendant waited over until March 29, 2024, before it began notifying the class—a full 73 days after the Data Breach began.

25. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

26. And when Defendant did notify Plaintiffs and the Class of the Data Breach, Defendant acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiffs and the Class:

a. "we recommend reviewing the statements you receive from your health plan and contacting your health insurer immediately if you see services that you did not receive;" and

b. "[i]f an individual believes their information was involved . . . please call 844-563-2187[.]"[12]

27. Defendant failed its duties when its inadequate security practices caused the Data Breach. In other words, Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII/PHI. And thus, Defendant caused widespread injury and monetary damages.

28. Since the breach, Defendant promises that "we have implemented, and will continue to adopt, additional safeguards and technical security measures to further protect and monitor our systems."[13]

29. But this is too little too late. Simply put, these measures—which Defendant now recognizes as necessary—should have been implemented *before* the Data Breach.

[12] *Id*.
[13] *Id*.

30. On information and belief, Defendant failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

31. Further, the Notice of Data Breach shows that Defendant cannot—or will not—determine the full scope of the Data Breach, as Defendant has been unable to determine precisely what information was stolen and when.

32. Defendant has done little to remedy its Data Breach. True, Defendant has offered some victims credit monitoring and identity related services. But upon information and belief, such services are wholly insufficient to compensate Plaintiffs and Class members for the injuries that Defendant inflicted upon them.

33. Because of Defendant's Data Breach, the sensitive PII/PHI of Plaintiffs and Class members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiffs and Class members.

34. Stunningly, this Data Breach is only part and parcel of Defendant's *pattern* of negligent data security. After all, Defendant also experienced a data breach in October 2018, which exposed the following types of PII:

a. names;

b. dates of birth;

c. Social Security numbers;

d. bank account information;

e. and driver's license numbers.[14]

LockBit & the Dark Web

[14] *Ernest Health*, DEPT JUSTICE MONTANA (April 15, 2019) https://dojmt.gov/wp-content/uploads/CON-2019.04.15-MT-AG-Notice-Ernest.pdf.

35. Worryingly, the cybercriminals that obtained Plaintiffs' and Class members' PII/PHI appear to be the notorious cybercriminal group "LockBit."[15]

36. Arising in Russia during early 2020, "LockBit" is now "the most deployed ransomware variant across the world and continues to be prolific in 2023."[16]

37. Thus, the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), the Multi-State Information Sharing and Analysis Center (MS-ISAC) have warned that:

a. "LockBit affiliates have employed double extortion by first encrypting victim data and then exfiltrating that data while threatening to post that stolen data on leak sites."[17]

b. "Up to the Q1 2023, a total of 1,653 alleged victims were observed [i.e., published] on LockBit leak sites."[18]

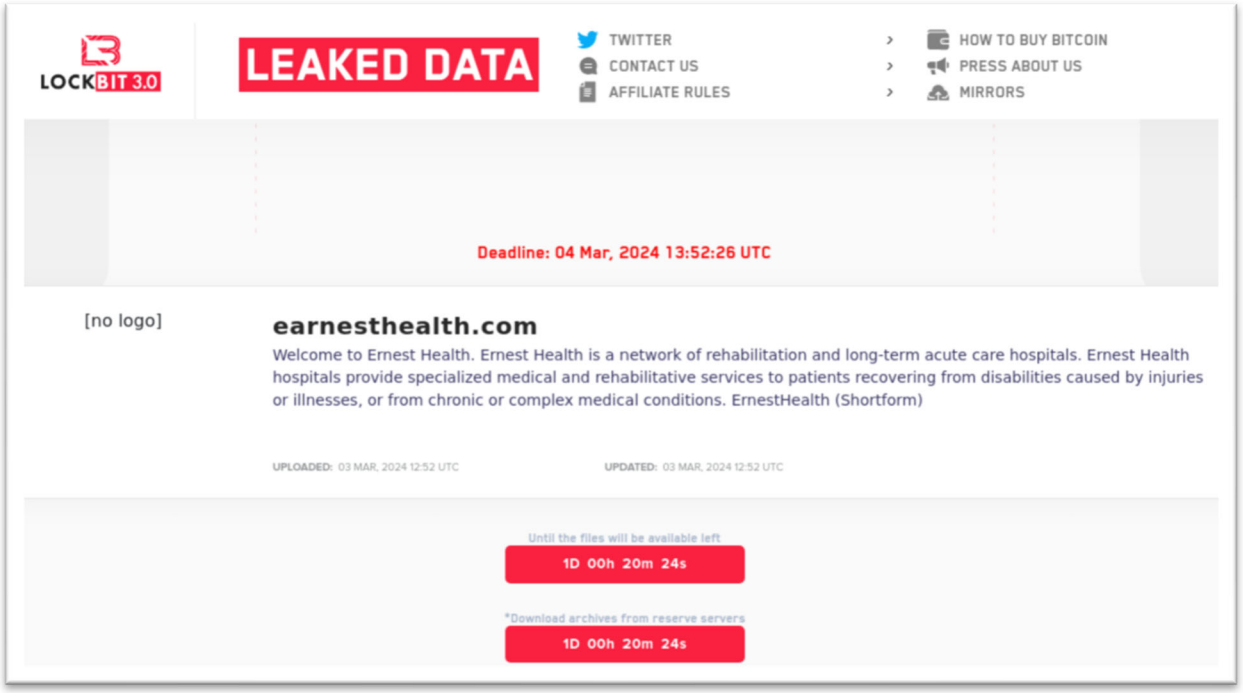
38. And Reuters reports that:

a. "On the dark web, Lockbit's blog displays an ever-growing gallery of victim organisations that is updated nearly daily."[19]

[15] *Id*.
[16] *Cybersecurity Advisory*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (June 14, 2023) https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a.
[17] *Id*.
[18] *Id*.
[19] Zeba Siddiqui & James Pearson, *Explainer: What is Lockbit? The digital extortion gang on a cybercrime spree*, REUTERS (Nov. 10, 2023) https://www.reuters.com/technology/cybersecurity/what-is-lockbit-digital-extortion-gang-cybercrime-spree-2023-11-10/.

b. "Next to their names are digital clocks showing the number of days left to the deadline given to each organisation to provide ransom payment, failing which, the gang publishes the sensitive data it has collected."[20]

39. Here, numerous third parties have reported that LockBit (1) successfully hacked Defendant, and (2) promised to ***publish*** the exfiltrated PII/PHI by March 4, 2024.[21]



[20] *Id.*

[21] *See e.g., LockBit3*, RANSOMLOOK, https://www.ransomlook.io/group/lockbit3 (last visited April 9, 2024); *Hacks of Today*, HACKMANAC, https://hackmanac.com/news/hacks-of-today-24-25-26-02-2024 (last visited April 9, 2024); Miklos Zoltan, *Freshly Revived Lockbit Announces 2 Victims*, PRIVACY AFFAIRS (Feb. 26, 2024) https://www.privacyaffairs.com/freshly-revived-lockbit-announces-2-victims/; *Ernest Health*, BREACHSENSE, https://www.breachsense.com/breaches/ernest-health-data-breach/(last visited April 9, 2024).

ERNEST HEALTH

Victim website:	ernesthealth.com
Victim country:	USA
Attacker name:	LockBit 3.0
Attacker class:	Cybercrime
Attack technique:	Ransomware
Ransom demand:	N/A
Exfiltrated data amount:	N/A
Exfiltrated data type:	N/A
Leaked data:	/
Ransom deadline:	28th Feb 24

40. Thus, on information and belief, Plaintiffs' and the Class's stolen PII/PHI has already been published—or will be published imminently—on the Dark Web.

Plaintiff Joe Lara's Experiences and Injuries

41. Plaintiff Joe Lara is a former patient of Defendant—having received medical services for several weeks in or around 2024.

42. Thus, Defendant obtained and maintained Plaintiff's PII/PHI.

43. As a result, Plaintiff was injured by Defendant's Data Breach.

44. As a condition of receiving medical services, Plaintiff provided Defendant with his PII/PHI. Defendant used that PII/PHI to facilitate its provision of medical services and to collect payment.

45. Plaintiff provided his PII/PHI to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

46. Plaintiff reasonably understood that a portion of the funds paid to Defendant would be used to pay for adequate cybersecurity and protection of PII/PHI.

47. Plaintiff received a Notice of Data Breach on April 5, 2024.

48. Thus, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

49. Through its Data Breach, Defendant compromised Plaintiff's:

a. name;

b. Social Security number;

c. health information; and

d. health insurance information.

50. Plaintiff has spent—and will continue to spend—significant time and effort monitoring his accounts to protect themselves from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

51. And in the aftermath of the Data Breach, Plaintiff has suffered from a spike in spam and scam calls.

52. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach.

53. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond

allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

54. Plaintiff suffered actual injury from the exposure and theft of his PII/PHI—which violates his rights to privacy.

55. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII/PHI. After all, PII/PHI is a form of intangible property—property that Defendant was required to adequately protect.

56. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's PII/PHI right in the hands of criminals.

57. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

58. Today, Plaintiff has a continuing interest in ensuring that his PII/PHI—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Laurie Cook's Experiences and Injuries

59. Plaintiff Laurie Cook is a former patient of Defendant—having received medical services in or around 2021.

60. Thus, Defendant obtained and maintained Plaintiff's PII/PHI.

61. As a result, Plaintiff was injured by Defendant's Data Breach.

62. As a condition of receiving medical services, Plaintiff provided Defendant with her PII/PHI. Defendant used that PII/PHI to facilitate its provision of medical services and to collect payment.

63. Plaintiff provided her PII/PHI to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

64. Plaintiff reasonably understood that a portion of the funds paid to Defendant would be used to pay for adequate cybersecurity and protection of PII/PHI.

65. Plaintiff received a Notice of Data Breach on April 8, 2024.

66. Thus, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

67. Through its Data Breach, Defendant compromised Plaintiff's:

a. name;

b. address;

c. date of birth;

d. Social Security number;

e. driver's license number; and

f. medical records.

68. Plaintiff has spent—and will continue to spend—significant time and effort monitoring her accounts to protect themselves from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

69. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach.

70. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond

allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

71. Plaintiff suffered actual injury from the exposure and theft of her PII/PHI—which violates her rights to privacy.

72. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII/PHI. After all, PII/PHI is a form of intangible property—property that Defendant was required to adequately protect.

73. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's PII/PHI right in the hands of criminals.

74. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her injuries.

75. Today, Plaintiff has a continuing interest in ensuring that her PII/PHI—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

76. Because of Defendant's failure to prevent the Data Breach, Plaintiffs and Class members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their PII/PHI is used;

b. diminution in value of their PII/PHI;

c. compromise and continuing publication of their PII/PHI;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII/PHI; and

h. continued risk to their PII/PHI—which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the PII/PHI.

77. Stolen PII/PHI is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII/PHI can be worth up to $1,000.00 depending on the type of information obtained.

78. The value of Plaintiffs and Class's PII/PHI on the black market is considerable. Stolen PII/PHI trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "Dark Web"—further exposing the information.

79. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII/PHI far and wide.

80. One way that criminals profit from stolen PII/PHI is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen PII/PHI, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

81. The development of "Fullz" packages means that the PII/PHI exposed in the Data Breach can easily be linked to data of Plaintiffs and the Class that is available on the internet.

82. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII/PHI stolen by the cyber-criminals in the Data Breach, criminals can 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. That is exactly what is happening to Plaintiffs and Class members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class members' stolen PII/PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

83. Defendant disclosed the PII/PHI of Plaintiffs and Class members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII/PHI of Plaintiffs and Class members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII/PHI.

84. Defendant's failure to promptly and properly notify Plaintiffs and Class members of the Data Breach exacerbated Plaintiffs and Class members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII/PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant Knew—Or Should Have Known—of the Risk of a Data Breach

85. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

86. In 2021, a record 1,862 data breaches occurred, exposing approximately

293,927,708 sensitive records—a 68% increase from 2020.[22] Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[23] Those 330 reported breaches exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[24]

87. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[25]

88. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[26]

89. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant Failed to Follow FTC Guidelines

90. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines

---

[22] *See 2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) https://notified.idtheftcenter.org/s/.
[23] *Id*.
[24] *Id*.
[25] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.
[26] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited Sept. 11, 2023).

identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

91. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[27] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

92. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

93. Furthermore, the FTC explains that companies must:

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

94. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and

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

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

95. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to its current and former patients' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

96. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: 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.

97. Other industry standard best practices 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; protection against any possible communication system; and training staff regarding critical points.

98. 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.

99. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

Defendant Violated HIPAA

100. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[28]

101. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII/PHI and PHI is properly maintained.[29]

102. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

[28] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[29] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

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

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

d. failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

103. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

CLASS ACTION ALLEGATIONS

104. Plaintiffs bring this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII/PHI was compromised in the Data Breach discovered by Ernest Health in February 2024, including all those individuals who received notice of the breach.

105. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

106. Plaintiffs reserve the right to amend the class definition.

107. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

108. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some individuals and sent them data breach notices.

109. Numerosity. The Class members are so numerous that joinder of all Class members is impracticable. Upon information and belief, the proposed Class includes at least 100 members.

110. Typicality. Plaintiffs' claims are typical of Class members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

111. Adequacy. Plaintiffs will fairly and adequately protect the proposed Class's common interests. Their interests do not conflict with Class members' interests. And Plaintiffs have retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

112. Commonality and Predominance. Plaintiffs' and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class members—for which a class wide proceeding can answer for all Class members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's PII/PHI;

b. if 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. if Defendant were negligent in maintaining, protecting, and securing PII/PHI;

d. if Defendant breached contract promises to safeguard Plaintiffs and the Class's PII/PHI;

e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendant's Breach Notice was reasonable;

g. if the Data Breach caused Plaintiffs and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiffs and the Class are entitled to damages, treble damages, and or injunctive relief.

113. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would be practically impossible for Class members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

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

114. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

115. Plaintiffs and the Class entrusted their PII/PHI to Defendant on the premise and with the understanding that Defendant would safeguard their PII/PHI, use their PII/PHI for business purposes only, and/or not disclose their PII/PHI to unauthorized third parties.

116. Defendant owed a duty of care to Plaintiffs and Class members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry

standards for data security—would compromise their PII/PHI in a data breach. And here, that foreseeable danger came to pass.

117. Defendant has full knowledge of the sensitivity of the PII/PHI and the types of harm that Plaintiffs and the Class could and would suffer if their PII/PHI was wrongfully disclosed.

118. Defendant owed these duties to Plaintiffs and Class members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiffs and Class members' PII/PHI.

119. Defendant owed—to Plaintiffs and Class members—at least the following duties to:

a. exercise reasonable care in handling and using the PII/PHI in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiffs and Class members within a reasonable timeframe of any breach to the security of their PII/PHI.

120. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiffs and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiffs and Class members to take appropriate measures to protect their PII/PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

121. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII/PHI it was no longer required to retain under applicable regulations.

122. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII/PHI of Plaintiffs and the Class involved an unreasonable risk of harm to Plaintiffs and the Class, even if the harm occurred through the criminal acts of a third party.

123. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential PII/PHI, a necessary part of obtaining services from Defendant.

124. The risk that unauthorized persons would attempt to gain access to the PII/PHI and misuse it was foreseeable. Given that Defendant hold vast amounts of PII/PHI, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII/PHI —whether by malware or otherwise.

125. PII/PHI is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII/PHI of Plaintiffs and Class members' and the importance of exercising reasonable care in handling it.

126. Defendant improperly and inadequately safeguarded the PII/PHI of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

127. Defendant breached these duties as evidenced by the Data Breach.

128. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class members' PII/PHI by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the PII/PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

129. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII/PHI of Plaintiffs and Class members which actually and proximately caused the Data Breach and Plaintiffs and Class members' injury.

130. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs and Class members' injuries-in-fact.

131. Defendant has admitted that the PII/PHI of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

132. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

133. And, on information and belief, Plaintiffs' PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

134. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and Class members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII/PHI by criminals, improper disclosure of their PII/PHI, lost benefit of their bargain, lost value of their

PII/PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Negligence *per se*
(On Behalf of Plaintiffs and the Class)

135. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

136. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' PII/PHI.

137. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII/PHI entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs and the Class members' sensitive PII/PHI.

138. Defendant breached its respective duties to Plaintiffs and Class members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII/PHI.

139. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII/PHI and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

140. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because 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 members of the Class.

141. But for Defendant's wrongful and negligent breach of its duties owed, Plaintiffs and Class members would not have been injured.

142. The injury and harm suffered by Plaintiffs and Class members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure of their PII/PHI.

143. Similarly, under HIPAA, Defendant had a duty to follow HIPAA standards for privacy and security practices—as to protect Plaintiffs' and Class members' PHI.

144. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect its PHI and by not complying with applicable regulations detailed *supra*. Here too, Defendant's conduct was particularly unreasonable given the nature and amount of PHI that Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

145. Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

146. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

THIRD CAUSE OF ACTION
Breach of Implied Contract

(On Behalf of Plaintiffs and the Class)

147. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

148. Plaintiff and Class members either directly contracted with Defendant or Plaintiff and Class members were the third-party beneficiaries of contracts with Defendant.

149. Plaintiffs and Class members were required to provide their PII/PHI to Defendant as a condition of receiving medical services provided by Defendant. Plaintiffs and Class members provided their PII/PHI to Defendant or its third-party agents in exchange for Defendant's medical services.

150. Plaintiffs and Class members reasonably understood that a portion of the funds they paid Defendant would be used to pay for adequate cybersecurity measures.

151. Plaintiffs and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

152. Plaintiffs and the Class members accepted Defendant's offers by disclosing their PII/PHI to Defendant or its third-party agents in exchange for medical services.

153. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII/PHI to unauthorized persons.

154. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiffs' and Class Member's PII/PHI.

155. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and Class members with prompt and adequate notice of all unauthorized access and/or theft of their PII/PHI.

156. After all, Plaintiffs and Class members would not have entrusted their PII/PHI to Defendant in the absence of such an agreement with Defendant.

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

158. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

159. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

160. Defendant materially breached the contracts it entered with Plaintiffs and Class members by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII/PHI that Defendant created, received, maintained, and transmitted.

161. In these and other ways, Defendant violated its duty of good faith and fair dealing.

162. Defendant's material breaches were the direct and proximate cause of Plaintiffs' and Class members' injuries (as detailed *supra*).

163. And, on information and belief, Plaintiffs' PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

164. Plaintiffs and Class members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

FOURTH CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

165. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

166. Plaintiffs and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII/PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

167. Defendant owed a duty to its current and former patients, including Plaintiffs and the Class, to keep this information confidential.

168. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs and Class members' PII/PHI is highly offensive to a reasonable person.

169. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and the Class disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

170. The Data Breach constitutes an intentional interference with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

171. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

172. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

173. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

174. As a proximate result of Defendant's acts and omissions, the private and sensitive PII/PHI of Plaintiffs and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages (as detailed *supra*).

175. And, on information and belief, Plaintiffs' PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

176. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII/PHI are still maintained by Defendant with their inadequate cybersecurity system and policies.

177. Plaintiffs and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for

monetary damages will not end Defendant's inability to safeguard the PII/PHI of Plaintiffs and the Class.

178. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other Class members, also seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

FIFTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

179. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

180. This claim is pleaded in the alternative to the breach of implied contract claim.

181. Plaintiffs and Class members conferred a benefit upon Defendant. After all, Defendant benefitted from (1) using their PII/PHI to facilitate its provision of services, and (2) receiving payment from Plaintiffs and Class members.

182. Defendant appreciated or had knowledge of the benefits it received from Plaintiffs and Class members.

183. Plaintiffs and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

184. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class members' PII/PHI.

185. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class members by utilizing cheaper, ineffective security measures.

Plaintiffs and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

186. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and Class members' PII/PHI and/or payment because Defendant failed to adequately protect their PII/PHI.

187. Plaintiffs and Class members have no adequate remedy at law.

188. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiffs and Class members—all unlawful or inequitable proceeds that it received because of its misconduct.

SIXTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

189. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

190. Given the relationship between Defendant and Plaintiffs and Class members, where Defendant became guardian of Plaintiffs' and Class members' PII/PHI, Defendant became a fiduciary by its undertaking and guardianship of the PII/PHI, to act primarily for Plaintiffs and Class members, (1) for the safeguarding of Plaintiffs and Class members' PII/PHI; (2) to timely notify Plaintiffs and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

191. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of Defendant's relationship with them—especially to secure their PII/PHI.

192. Because of the highly sensitive nature of the PII/PHI, Plaintiffs and Class members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII/PHI had they known the reality of Defendant's inadequate data security practices.

193. Defendant breached its fiduciary duties to Plaintiffs and Class members by failing to sufficiently encrypt or otherwise protect Plaintiffs' and Class members' PII/PHI.

194. Defendant also breached its fiduciary duties to Plaintiffs and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

195. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

PRAYER FOR RELIEF

Plaintiffs and Class members respectfully request judgment against Defendant and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representative, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as necessary to protect the interests of Plaintiffs and the Class;

D. Awarding Plaintiffs and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

E. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

F. Awarding attorneys' fees and costs, as allowed by law;

G. Awarding prejudgment and post-judgment interest, as provided by law;

H. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

I. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial for all claims so triable.

Dated: April 10, 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
Telephone: 214/744-3000 / 214/744-3015 (fax)
jkendall@kendalllawgroup.com

TURKE & STRAUSS LLP
Samuel J. Strauss*
Raina Borrelli*
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

**Pro hac vice forthcoming*
Attorneys for Plaintiffs and Proposed Class

ClassAction.org