IN THE CIRCUIT COURT FOR
ANDERSON COUNTY AT
CLINTON TENNESSEE

K.B. (minor) through Joan Blank, next friend; J.M. (minor) through Mary Murray, next friend; T.D. (minor) through Shelbie Dempsey, next friend; Jacob Mason; Whitney Sprouls; Meagan Jones; Miguel Cadenas; M.C. and T.C. (minors) through Lynne Cadenas, next friend; B.P., J.P. and C.P. (minors) through Judi Parris, next friend; C.J.J. (minor) through Craig Juneau, next friend; Michael McCarter; C.G.C. (minor) through Beth Catron, next friend; and K.C.U. (minor) through Robert Ulucan, next friend, individually and on behalf of all others similarly situated, Plaintiffs, v. EAST TENNESSEE CHILDREN'S HOSPITAL ASSOCIATION, INC., Defendant.	Case No. C2LA0081 **AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs K.B., a minor child through parent/legal guardian Joan Blank, next friend; J.M., a minor child through parent/legal guardian Mary Murray, next friend, T.D., a minor child through parent/legal guardian Shelbie Dempsey, next friend; Jacob Mason; Whitney Sprouls; Meagan Jones; Miguel Cadenas; M.C. and T.C., minor children through parent/legal guardian Lynne Cadenas, next friend; B.P., J.P., and C.P., minor children through parent/legal guardian Judi Parris, next friend; C.J.J., a minor child through parent/legal guardian Craig Juneau, next friend; Michael McCarter; C.G.C., a minor child through parent/legal guardian Beth Catron, next friend; and

K.C.U., a minor child through parent/legal guardian Robert Ulucan, next friend (collectively "Plaintiffs") bring this Class Action Complaint on behalf of themselves, and all others similarly situated against Defendant, East Tennessee Children's Hospital Association, Inc., ("ETCH" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities, and alleges as follows:

INTRODUCTION

1. On or about March 13, 2022, ETCH, a Comprehensive Regional Pediatric Center in Tennessee serving primarily minors as patients, identified unusual activity on its networks.

2. On or about March 18, 2022, ETCH discovered that it had lost control over at least 422,531 former and current patients' highly sensitive personal records in a data breach by cybercriminals ("Data Breach").

3. On information and belief, the Data Breach occurred between March 11, 2022, and March 14, 2022.

4. On or around May 19, 2022—over two months after discovering the Data Breach—ETCH began to notify breach victims that hackers had gained unauthorized access to former and current patients' confidential personal identifying information and/or personal health information (together "PII").

5. On information and belief, the stolen PII included, at least, patients' names, contact information, dates of birth, medical records, and Social Security numbers.

6. On information and belief, cybercriminals were able to breach ETCH's systems because ETCH did not maintain reasonable security safeguards or protocols to protect its minor patients' PII, leaving it an unguarded target for theft and misuse.

7. After the Data Breach ended on March 14, 2022, ETCH did not notify the Data

Breach victims about the breach within 45 days as required by Tennessee law, depriving them an opportunity to mitigate the Data Breach's impact on them and to secure their identities from theft.

8. When ETCH finally admitted to the Data Breach in May 2022 with a breach notice ("Breach Notice"), it obfuscated the nature of the breach and the threat it posed—refusing to tell its patients how many people were impacted, how the breach happened, or why it took over two months for ETCH to send a bare-bones notice.[1]

9. Despite the lifelong harm that the Data Breach poses to its current and former patients, on information and belief, ETCH offered them only a 12-month credit monitoring service, which does not adequately address the harm ETCH's patients and their families have and will continue to suffer.

10. ETCH's failure to safeguard patients' PII and adequately warn them about the Data Breach violates Tennessee law, harming thousands of individuals.

11. Each of the Plaintiffs, as captioned above, received ETCH's Breach Notice and are Data Breach victims causing them to seek relief on a class wide basis.

12. ETCH knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

13. ETCH's misconduct has injured the Plaintiffs and members of the proposed Class, including: (i) the lost or diminished value of their PII; (ii) costs associated with the prevention, detection, and recovery from identity theft, tax fraud, and other unauthorized use of their data; (iii) lost opportunity costs to mitigate the Data Breach's consequences, including lost time; and (iv) emotional distress associated with the loss of control over their highly sensitive PII.

[1] A true and accurate copy of the Breach Notice is attached to this complaint as **Exhibit A**.

14. Plaintiffs and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiffs and members of the proposed Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

15. Plaintiffs and members of the proposed Class therefore bring this lawsuit seeking damages and relief for Defendant's actions.

PARTIES

16. Plaintiff Joan Blank, parent, legal guardian and next friend of K.B. (a minor), is a natural person and citizen of Tennessee. They reside in Tennessee, where they both intend to remain. Minor K.B. is a current ETCH patient and Data Breach victim. The minor's parent/legal guardian and next friend received ETCH's Breach Notice on behalf of the minor child in late May 2022.

17. Plaintiff Mary Murray, parent, legal guardian and next friend of J.M. (a minor), is a natural person and citizen of Tennessee. They reside in Tennessee, where they both intend to remain. Minor K.B. is a former ETCH patient and Data Breach victim. The minor's parent/legal guardian and next friend received ETCH's Breach Notice on behalf of the minor child in late May 2022.

18. Plaintiff Shelbie Dempsey, parent, legal guardian and next friend of T.D. (a minor), is a natural person and citizen of Tennessee. They reside in Tennessee, where they both intend to remain. Minor T.D. is a past ETCH patient and Data Breach victim. The minor's parent/legal guardian and next friend received ETCH's Breach Notice on behalf of the minor child in late May 2022.

19. Plaintiff Jacob Mason is a natural person and citizen of Tennessee, residing in

Tennessee and intends to remain in Tennessee. Plaintiff Mason is a past ETCH patient and Data Breach victim who received ETCH's Breach Notice in late May 2022.

20. Plaintiff Whitney Sprouls is a natural person and citizen of Tennessee, residing in Tennessee and intends to remain in Tennessee. Plaintiff Sprouls is a past ETCH patient and Data Breach victim who received ETCH's Breach Notice in late May 2022.

21. Plaintiff Meagan Jones is a natural person and citizen of Tennessee, residing in Tennessee and intends to remain in Tennessee. Plaintiff Jones is a current ETCH patient and Data Breach victim who received ETCH's Breach Notice in late May 2022.

22. Plaintiff Miguel Cadenas is a natural person and citizen of Tennessee, residing in Tennessee and intends to remain in Tennessee. Plaintiff Miguel Cadenas is a past ETCH patient and Data Breach victim who received ETCH's Breach Notice in late May 2022.

23. Plaintiff Lynne Cadenas, parent, legal guardian and next friend of M.C. and T.C. (minors), is a natural person and citizen of Tennessee. They reside in Tennessee and intend to remain in Tennessee. Minors M.C. and T.C. are current ETCH patients and Data Breach victims. The minors' parent/legal guardian and next friend received ETCH's Breach Notices on behalf of the minor children in late May 2022.

24. Plaintiff Judi Parris, parent, legal guardian and next friend of B.P., J.P. and C.P. (minors), is a natural person and citizen of Tennessee. They reside in Tennessee and intend to remain in Tennessee. Minors B.P., J.P. and C.P. are current ETCH patients and Data Breach victims. The minors' parent/legal guardian and next friend received ETCH's Breach Notices on behalf of the minor children in late May 2022.

25. Plaintiff Craig Juneau, parent, legal guardian and next friend of C.J.J. (a minor), is a natural person and citizen of Tennessee. They reside in Tennessee, where they both intend to

remain. Minor C.J.J. is a current ETCH patient and Data Breach victim. The minor's parent/legal guardian and next friend received ETCH's Breach Notice on behalf of the minor child in late May 2022.

26. Plaintiff Michael McCarter is a natural person and citizen of Tennessee, residing in Tennessee and intends to remain in Tennessee. Plaintiff McCarter is a past ETCH patient and Data Breach victim who received ETCH's Breach Notice in late May 2022.

27. Plaintiff Beth Catron, parent, legal guardian and next friend of C.G.C. (a minor), is a natural person and citizen of Tennessee. They reside in Tennessee, where they both intend to remain. Minor C.G.C. is a current ETCH patient and Data Breach victim. The minor's parent/legal guardian and next friend received ETCH's Breach Notice on behalf of the minor child in late May 2022.

28. Plaintiff Robert Ulucan, parent, legal guardian and next friend of K.C.U. (a minor), is a natural person and citizen of Tennessee. They reside in Tennessee, where they both intend to remain. Minor K.C.U. is a current ETCH patient and Data Breach victim. The minor's parent/legal guardian and next friend received ETCH's Breach Notice on behalf of the minor child in late May 2022

29. Defendant ETCH, is a Tennessee corporation, with its principal place of business at 2018 Clinch Ave., Knoxville, Tennessee 37916.

30. Defendant ETCH has other clinic or hospital locations in Tennessee, including, but not limited to locations in Alcoa, Clinton, and Oak Ridge, Tennessee.

JURISDICTION & VENUE

31. This Court has general jurisdiction over this action under T.C.A. § 16-10-101.

32. This Court has personal jurisdiction over Defendant because it operates in

Anderson County, and some of the conduct at-issue occurred in Anderson County.

33. Venue is proper in this Court under T.C.A. § 20-4-101 because the cause of action arose in this county and Defendant resides or is found in this county.

BACKGROUND FACTS

A. ETCH's Failure to Safeguard Patients' PII

34. ETCH offers pediatric medical care in Tennessee. In doing so, ETCH collects highly sensitive PII from its patients, most of whom are minor children. Indeed, ETCH requires that patients disclose their personal information in order to receive ETCH's services.

35. On information and belief, the PII collected from patients includes first and last names, dates of birth, addresses, patient identification numbers, insurance card numbers, their guardians' credit card information, Social Security numbers, and medical information.

36. When ETCH collects this sensitive information, it promises to use reasonable measures to safeguard the PII from theft and misuse.

37. In fact, ETCH informs its patients and their guardians that it collects and maintains their PII through the Privacy Policy (the "Privacy Policy").[2] A true and correct copy of the Privacy Policy is attached hereto as **Exhibit B.**

38. The Privacy Policy highlights ETCH's legal obligations under federal and state law "to maintain the privacy of [children's] health information" and to notify patients if they are "affected by a breach of unsecured [PII]." Ex. B.

39. ETCH represented to its patients that their PII would be secure. Plaintiffs and members of the proposed Class relied on such representations when they agreed to provide their PII to ETCH.

[2] *See* ETCH Website: https://www.etch.com/privacy/ (last visited Jan. 10, 2023).

40. Despite its alleged commitments to securing sensitive patient data, ETCH does not follow industry standard practices in securing patients' PII.

41. In March 2022, hackers bypassed ETCH's security safeguards and infiltrated its systems, giving them unfettered access to patients' PII.

42. On information and belief, the Data Breach was undetected for at least two days.

43. In response to the Data Breach, ETCH contends that it is "reviewing and strengthening [its] existing policies, procedures, and safeguards related to cyber security and [has] already taken additional steps to further enhance the security of [its] systems." Exh. A. These measures should have been in place *before* the Data Breach.

44. ETCH's Breach Notice omits the size and scope of the breach. ETCH has demonstrated a pattern of providing inadequate notices and disclosures about the Data Breach.

45. On information and belief, the Data Breach has impacted at least 422,531 former and current ETCH patients.

46. On information and belief, ETCH does not adequately train its employees on cybersecurity policies, enforce those policies, or maintain reasonable security practices and systems.

47. ETCH's negligent conduct caused the Data Breach. ETCH violated its obligation to implement best practices and comply with industry standards concerning computer system security. ETCH failed to comply with security standards and allowed its patients' PII to be accessed and stolen by failing to implement security measures that could have prevented, mitigated, or timely detected the Data Breach.

48. On information and belief, ETCH has offered breach victims one year of complimentary identity theft protection services through IDX.

49. As more fully articulated below, Plaintiffs and the members of the proposed Class's personal data may exist on the dark web and in the public domain for months, or even years, before it is used for ill gains and actions. With only one year of monitoring, and no form of insurance or other protection, Plaintiffs, their minor children, and other members of the proposed Class remain unprotected from the real and long-term threats against their personal, sensitive, and private data.

50. Therefore, the "protection services" offered by ETCH are inadequate, and Plaintiffs and the members of the proposed Class have a real and cognizable interest in obtaining equitable relief, in addition to the monetary relief requested herein.

B. Plaintiffs' Experiences

51. Each minor child captioned above is a current or former ETCH patient, who received medical services and provided PII to ETCH. Each adult Plaintiff captioned above is either a former ETCH patient who received medical services and provided PII to ETCH, or alternatively, the parent, legal guardian, and next friend of a current or former ETCH patient (or patients) who received medical services and provided PII to ETCH.

52. As a condition of receiving ETCH's medical services, ETCH required that its minor patients, through their parents and/or legal guardians, to provide the children's PII. Each of the Plaintiffs, as parents and/or legal guardians provided the minor children's PII to ETCH.

53. Plaintiffs believed that, as part of the payments to ETCH for medical treatment and services, that those payments included amounts for data security. Had Plaintiffs' known that ETCH did not utilize reasonable data security measures, they would have paid less for those treatments and services.

54. In late May 2022, each Plaintiff, individually or on behalf of their minor child(ren) received a notice letter from ETCH confirming that their or their child(ren)s' PII was compromised

as a result of the Data Breach.

55. Had each Plaintiff, as a parent and legal guardian, known that ETCH does not adequately protect PII, they would not have transacted with ETCH. Furthermore, each Plaintiff's and their family's sensitive PII remains in ETCH's possession without adequate protection against known threats, exposing them to the prospect of additional harm in the event ETCH suffers another data breach.

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

56. Plaintiffs, their minor children, and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

57. The ramifications of Defendant's failure to keep the Class's PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

58. According to experts, one out of four data breach notification recipients become a victim of identity fraud. [3]

59. As a result of Defendant's failure to prevent the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

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

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

[3] *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims*, ThreatPost.com (Feb. 21, 2013), https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/ (last visited Jan. 9, 2023).

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in their possession.

60. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained. [4]

61. The value of the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

62. Of particular importance here, a minor's information can be stolen and used until the minor turns eighteen years old before the minor even realizes he or she has been victimized.

63. It can take victims years to spot identity or PII theft, giving criminals plenty of time

[4] *See* Here's How Much Your Personal Information Is Selling for on the Dark Web, Experian, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Jan. 9, 2023).

to use that information for cash.

64. One such example of criminals using PII for profit is the development of "Fullz" packages. [5]

65. Cyber-criminals can cross-reference multiple sources of PII 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. These dossiers are known as "Fullz" packages.

66. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's 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 PII 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, their children, and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

---

[5] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited 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 can be made off 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), *available at* https://krebsonsecurity.com/tag/fullz/ (last visited Jan. 9, 2023).

67. Defendant disclosed the PII of Plaintiffs, their children, and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of members of the proposed Class 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.

68. The risk to Plaintiffs, as well as the affected minor children, and other potential minor Class members is substantial given the children's ages and lack of established credit because their information can be used to create a "clean identity slate." It is not surprising, then, that one report found that children are 51% more likely be victims of identity theft than adults. Cybercriminals on the dark web have been caught selling Social Security numbers of infants for $300 per number to be used on fraudulent tax returns.[6]

69. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the PII of potentially thousands of members of the proposed Class to unscrupulous operators, con artists and outright criminals.

70. Defendant's failure to properly notify members of the proposed Class of the Data Breach exacerbated their injuries by depriving them of the earliest ability to take appropriate measures to protect their family's PII and take other necessary steps to mitigate the harm caused by the Data Breach.

CLASS ACTION ALLEGATIONS

[6] Avery Wolfe, *How Data Breaches Affect Children*, Axion Cyber Sols. (Mar. 15, 2018) (last visited Jan. 10, 2023), https://axiomcyber.com/data-breach/how-data-breaches-affect-children/.

71. Plaintiffs sue on behalf of themselves and the proposed Class ("Class"), defined as follows:

> All individuals whose PII was compromised in the Data Breach disclosed by ETCH in May 2022.

72. The following people are excluded from the Class: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or its parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

73. The Class defined above is identifiable through Defendant's business records.

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

75. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Tenn. R. Civ. P. 23.01.

a. **Numerosity**. Plaintiffs are representatives of the proposed Class, consisting of thousands of members, far too many to join in a single action;

b. **Typicality**. Plaintiffs' claims are typical of Class member's 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.

c. **Adequacy**. Plaintiffs will fairly and adequately protect the proposed Class's interests. Plaintiffs' interests do not conflict with Class members' interests, and Plaintiffs have retained counsel experienced in complex class action litigation and data privacy to

prosecute this action on the Class's behalf, including as lead counsel. Defendant has no defenses unique to Plaintiffs.

d. **Commonality**. Plaintiffs' and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Common questions for the Class include, but are not necessarily limited to the following:

i. Whether Defendant had a duty to use reasonable care in safeguarding the PII of Plaintiffs, their minor children, and the Class;

ii. 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;

iii. Whether Defendant was negligent in maintaining, protecting, and securing PII;

iv. Whether Defendant breached contractual promises to safeguard the Class's PII;

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

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether Defendant's conduct was likely to deceive the public;

viii. Whether Defendant is liable for negligence or gross negligence;

ix. Whether Defendant's practices and representations related to the Data Breach breached implied warranties;

x. Whether the Data Breach caused Plaintiffs and the Class injuries;

xi. What the proper damages measure is; and

xii. Whether Plaintiffs and the Class are entitled to damages, treble damages, or injunctive relief.

76. Further, this action satisfies Tenn. R. Civ. P. 23.02 because: (i) common questions of law and fact predominate over any individualized questions; (ii) prosecuting individual actions would create a risk of inconsistent or varying adjudications, risking incompatible standards of conduct for Defendant, and a risk of adjudications with respect to individual members of the Class which would as a practical matter be dispositive of the interests of the other members not parties to the adjudications or would substantially impair or impede their ability to protect their interest; and (iii) the Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

77. Plaintiffs and members of the Class incorporate all previous paragraphs as if fully set forth herein.

78. Plaintiffs and members of the Class entrusted their and their minor children's PII to Defendant. Defendant owed to members of the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

79. Defendant owed a duty of care to Plaintiffs and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard the PII in accordance with state-

of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of the PII of Plaintiffs and members of the Class by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

80. Defendant owed to Plaintiffs and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of the PII. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiffs and members of the Class to take appropriate measures to protect the PII, 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.

81. Defendant owed these duties to Plaintiffs and members of the Class 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 protocols. Defendant actively sought and obtained Plaintiffs' and members of the Class's personal information and PII.

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

83. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing of the PII of Plaintiffs and members of the Class,

particularly because most of ETCH's patients are minors, and the importance of exercising reasonable care in handling it.

84. 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 of Plaintiffs and members of the Class which actually and proximately caused the Data Breach and Plaintiffs' and members of the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

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

COUNT II
Negligence Per Se
(On Behalf of Plaintiffs and the Class)

86. Plaintiffs and members of the Class incorporate all previous paragraphs as if fully set forth herein.

87. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard the PII of Plaintiffs and members of the Class.

88. 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 customers or, in this case, patients' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect the PII of Plaintiffs and members of the Class.

89. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect the PII of Plaintiffs and members of the Class 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 Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to its employees and applicants in the event of a breach, which ultimately came to pass.

90. 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.

91. Defendant had a duty to Plaintiffs and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard the PII of Plaintiffs and members of the Class.

92. Defendant breached its respective duties to Plaintiffs and members of the Class

under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII of Plaintiffs and members of the Class.

93. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

94. Further, Tennessee's Identity Theft Deterrence Act ("ITDA"), under T.C.A § 47-18-2107, required Defendant to notify all Tennessee residents whose "personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made no later than forty-five (45) days from the discovery or notification of the breach of system security[.]"

95. In other words, the ITDA imposed a statutory duty on Defendant to notify Plaintiffs and the Class about the Data Breach within the statute's timeframe.

96. Plaintiffs and the Class belong to the class of persons the ITDA was designed to protect because they are Data Breach victims entitled to timely notice of the Data Breach.

97. Plaintiffs' and the Class's injuries, including those caused by Defendants' untimely notice, are the types of injuries the ITDA was designed to protect against in requiring timely notice. Indeed, the ITDA's timing requirements are designed to give Data Breach victims an opportunity to mitigate the Data Breach's impact on them and safeguard their identities from theft.

98. On information and belief, Defendant's two-month delay in notifying Plaintiffs and the Class about the Data Breach was not "due to the legitimate needs of law enforcement" as defined by ITDA.

99. Defendant failed to disclose the Data Breach to Plaintiffs and the Class within 45 days of discovering it, meaning it violated the ITDA and its statutory duty to give timely notice.

100. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs

and members of the Class, Plaintiffs and members of the Class would not have been injured.

101. The injury and harm suffered by Plaintiffs and members of the Class were 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.

102. Had Plaintiffs and members of the Class known that Defendant did not adequately protect their PII, Plaintiffs and members of the Class would not have entrusted Defendant with their PII.

103. As a direct and proximate result of Defendant's negligence per se, Plaintiffs and members of the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

COUNT III
Breach of an Implied Contract
(On Behalf of Plaintiffs and the Class)

104. Plaintiffs and members of the Class incorporate all previous paragraphs as if fully set forth herein.

105. Defendant offered to provide medical services to Plaintiffs, their minor children, and members of the Class in exchange for their PII and in exchange for amounts paid for medical treatment and services that included payment for data security.

106. In turn, and through internal policies, Defendant agreed it would not disclose the

PII it collects to unauthorized persons. Defendant also promised to safeguard patient PII.

107. Plaintiffs and the members of the Class accepted Defendant's offer by providing PII to Defendant in exchange for medical services.

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

109. Plaintiffs and the members of the Class would not have entrusted their and their children's PII to Defendant in the absence of such agreement with Defendant.

110. Defendant materially breached the contract(s) it had entered with Plaintiffs and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant further breached the implied contracts with Plaintiffs and members of the Class by:

a. Failing to properly safeguard and protect the PII of Plaintiffs and members of the Class;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PII that Defendant created, received, maintained, and transmitted.

111. The damages sustained by Plaintiffs and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

112. Plaintiffs and members of the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

113. The covenant of good faith and fair dealing is an element of every contract. All

such contracts impose upon each party a duty of good faith and fair dealing. The 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—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

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

115. Defendant failed to advise Plaintiffs and members of the Class of the Data Breach promptly and sufficiently.

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

117. Plaintiffs and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

118. Plaintiffs and members of the Class incorporate all previous paragraphs as if fully set forth herein.

119. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

120. Plaintiffs and members of the Class conferred a benefit upon Defendant in the form of monies paid for treatment services and by providing their PII to Defendant in order to receive

such services.

121. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiffs and members of the Class.

122. As a result of Defendant's conduct, Plaintiffs and members of the Class suffered actual damages in an amount equal to the difference in value between the purchases made with reasonable data privacy and security practices and procedures that Plaintiffs and members of the Class paid for, and the purchases without unreasonable data privacy and security practices and procedures that they received.

123. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the proposed Class's payments and their PII because Defendant failed to adequately protect their PII. Plaintiffs and the proposed Class would not have provided their PII, nor used and paid for Defendant's services, had they known Defendant would not adequately protect their PII.

124. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and members of the Class all unlawful or inequitable proceeds received by it because of its misconduct and the Data Breach alleged herein.

COUNT V
Violation of the Tennessee Consumer Protection Act,
Tenn. Code Ann. § 47-18-101, *et seq.*
(On Behalf of Plaintiffs and the Class)

125. Plaintiffs and members of the Class incorporate all previous paragraphs as if fully set forth herein.

126. Tennessee's Identity Theft Deterrence Act ("ITDA"), under T.C.A § 47-18-2106, states that any violation of the ITDA "constitutes a violation of the Tennessee Consumer Protection Act[,]" ("CPA"). The ITDA further states: "For the purpose of application of the [CPA], any

violation of this part shall be construed to constitute an unfair or deceptive act or practice affecting trade or commerce and subject to the penalties and remedies as provided in that act, in addition to the penalties and remedies set forth in this part."

127. Defendant violated the ITDA because Defendant did not follow its provisions in notifying Plaintiffs and the Class about the Data Breach.

128. Defendant suffered a "Breach of system security" as the ITDA defines that term during the Data Breach. On information and belief, Defendant maintained the PII of Plaintiffs and members of the Class according to § 47-18-2107(a)(1)(i).

129. The ITDA defines "information holder" to include Defendant because Defendant conducts business in Tennessee.

130. The ITDA defines "personal information" to include Plaintiffs' and the Class's PII, including their names in combination with the Social Security numbers, driver's license numbers, or any "Account, credit card, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account[.]"

131. Following discovery of the Data Breach caused by unauthorized actors, the ITDA required Defendant to notify all Tennessee residents whose "personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made no later than forty-five (45) days from the discovery or notification of the breach of system security[.]" On information and belief, Defendant's two-month delay in notifying Plaintiffs and the Class about the Data Breach was not "due to the legitimate needs of law enforcement" as defined by ITDA.

132. Defendant failed to disclose the Data Breach to Plaintiffs and the Class within 45 days of discovering it, meaning it violated the CPA.

133. As a direct and proximate cause of Defendant's ITDA and CPA violations, Plaintiffs and the Class have suffered damages, including (i) the compromise, publication, and/or theft of the PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (iii) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (iv) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession, and (v) future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class.

134. Plaintiffs and the Class are entitled to damages as well as injunctive relief, including, but not limited to, ordering Defendant to: (i) strengthen its data security systems, monitoring procedures, and data breach notification procedures; and (ii) immediately provide adequate credit monitoring to Plaintiffs and the Class.

COUNT VI
Violation of the ITDA under Tenn. Code Ann. § 47-18-2104
(On behalf of Plaintiffs and the Class)

135. Plaintiffs and members of the Class incorporate all previous paragraphs as if fully set forth herein.

136. As explained in this Complaint, Defendant violated the ITDA in failing to give notice of the Data Breach according to its provisions, including failure to notify all Tennessee residents whose "personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made no later than forty-five (45) days from the

discovery or notification of the breach of system security[.]"

137. Under Tenn. Code Ann. § 47-18-2104(f), "[w]ithout regard to any other remedy or relief to which a person is entitled, anyone affected by a violation of this part may bring an action to obtain a declaratory judgment that the act or practice violates this part and to enjoin the person who has violated, is violating, or who is otherwise likely to violate this part[.]"

138. Defendant has, is, and is likely to violate the ITDA because Defendant failed to give Plaintiffs and the Class notice of the Data Breach according to the ITDA's terms, its Breach Notice is and was inadequate, and Defendant has not developed or maintained adequate policies and procedures to comply with the ITDA's terms.

139. Further, under § 47-18-2104(f), "Upon a finding by the court that a provision of this part has been violated, the court may award to the person bringing such action reasonable attorneys' fees and costs."

140. Plaintiffs and the Class are thus entitled to a declaratory judgment that Defendant violated the ITDA, and entitled to an injunction ordering Defendant to: (i) strengthen its data security systems, monitoring procedures, and data breach notification procedures; and (ii) immediately provide adequate credit monitoring to Plaintiffs and the Class.

PRAYER FOR RELIEF

Plaintiffs and members of the Class demand a trial on all claims so triable and request 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 representatives, and appointing their counsel to represent the Class;

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

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

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiffs and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

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

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

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

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

J. Granting such other or further relief as may be appropriate under the circumstances.

K. JURY DEMAND

L. Plaintiffs demand a trial by jury on all issues so triable.

Dated: March 9th, 2023

Respectfully submitted,

J. Gerard Stranch, IV (BPR 23045)
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Avenue, Ste. 200
Nashville, TN 37203
Telephone: 615-254-8801
Facsimile: 615-255-5419
gstranch@stranchlaw.com

David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW
Suite 440
Washington, DC 20015-2052
dlietz@milberg.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: (866) 252-0878 / Fax: (865) 522-0049
gklinger@milberg.com

Nicholas A. Migliaccio
Jason Rathod
Tyler Bean
MIGLIACCIO & RATHOD, LLP
412 H Street NE
Washington, D.C. 20002
202.470.3520
nmigliaccio@classlawdc.com

Nathan D. Prosser
HELLMUTH & JOHNSON, PLLC
8050 West 78th Street
Edina, MN 55439
Telephone: (952)941-4005
Fax: (952) 941-2337
nprosser@hjlawfirm.com

Joseph Lyon
THE LYON FIRM, LLC
2754 Erie Ave
Cincinnati, Ohio 45208
Phone: (513) 381-2333
jlyon@thelyonfirm.com

Lynn A. Toops*
Lisa LaFornara*
Amina A. Thomas*
COHEN & MALAD, LLP
One Indiana Square, Ste. 1400
Indianapolis, IN 46204
Telephone: (317) 636-6481
Facsimile: (317) 636-2593
ltoops@cohenandmalad.com
llafornara@cohenandmalad.com
athomas@cohenandmalad.com

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

Lisa A. White (TN BPR # 026658)
lwhite@masonllp.com
Gary E. Mason*
gmason@masonllp.com
Danielle L. Perry*
dperry@masonllp.com
MASON LLP
5335 Wisconsin Ave. NW Ste. 640
Washington DC 20015
Phone: 202.640.1160
Fax: 202.429.2294

**Pro Hac Vice* forthcoming

Attorneys for Plaintiffs and the Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that on the 9th day of March, 2023, I served via U.S. Mail and/or electronic mail a copy of the forgoing Amended Complaint to the following:

Rocklan W. King III (#30643)
Sam D. Jones (#038436)
ADAMS AND REESE LLP
1600 West End Avenue, Suite 1400
Nashville, Tennessee 37203
Tel: 615-259-1450
Fax: 615-259-1470
rocky. king@arlaw.com
sam.jones@arlaw.com

Counsel for Defendant

J. Gerard Stranch, IV