**IN THE UNITED STATES DISTRICT COURT**
**FOR THE WESTERN DISTRICT OF TEXAS**
**AUSTIN DIVISION**

| | |
|---|---|
| ARTURO BRUNO, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>ROBERT DONOHOE, as TRUSTEE OF THE TEXAS MEDICAL LIABILITY TRUST,<br><br>Defendant. | CASE NO. 1:23-cv-01183<br><br>CLASS ACTION COMPLAINT<br><br>JURY TRIAL DEMANDED |

Plaintiff Arturo Bruno ("Plaintiff"), individually and on behalf of all others similarly situated, upon personal knowledge of all facts pertaining to himself and on information and belief as to all other matters, by and through the undersigned counsel, bring this Class Action Complaint against Defendant Robert Donohoe, as Trustee of the Texas Medical Liability Trust ("TMLT" and/or "Defendant").

## NATURE OF THE ACTION

1. Plaintiff brings this action, individually and on behalf of all others similarly situated, whose private and confidential personal identifying information ("PII") and/or protected health information ("PHI")—including their name, Social Security numbers, drivers' license numbers, financial account information, protected health information, EIN/Tax Identification Numbers, and dates of birth—was compromised in a massive security breach of TMLT's computer servers (the "Data Breach").

2. The HIPAA Journal—the leading provider of news, updates, and independent advice for HIPAA compliance—reports that TMLT's Data Breach affected 59,901 individuals.[1]

3. As alleged herein, TMLT's failure to implement adequate data security measures to protect its consumers' sensitive PII/PHI and proximately caused injuries to Plaintiff and the class members.

4. The Data Breach was the inevitable result of TMLT's inadequate data security measures and cavalier approach to data security. Despite the well-publicized and ever-growing threat of security breaches involving PII/PHI, TMLT failed to ensure that it maintained adequate data security measures to protect PII/PHI from unauthorized third parties.

5. By collecting, using, and deriving a benefit from the PII/PHI of Plaintiff and Class Members, TMLT assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

6. TMLT had legal obligations and duties created by HIPAA, contract, industry standards, common law, and representations made to Class Members, to keep Class Members' PII/PHI confidential and to protect it from unauthorized access and disclosure.

7. TMLT failed to adequately protect Plaintiff's and Class Members' PII/PHI and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII/PHI was compromised due to TMLT's negligent and/or careless acts and omissions and its utter failure to protect the sensitive data it collected for its own pecuniary gain.

8. Had TMLT adequately designed, implemented, and monitored its network and servers, the Data Breach would have been prevented.

---

[1]Steve Alder, *60,000 Individuals Affected by Texas Medical Liability Trust Data Breach*, The HIPAA Journal (Sep. 12, 2023), *accessible at* https://www.hipaajournal.com/60000-individuals-affected-by-texas-medical-liability-trust-data-breach/.

9. Had Plaintiff and Class Members known that TMLT's data security was below industry standards, Plaintiff and Class Members would not have provided their PII/PHI to TMLT or relied on TMLT to protect that information.

10. As a result of TMLT's inadequate data security practices that resulted in the Data Breach, Plaintiff and Class Members are at an imminent risk of identity theft and have suffered numerous actual and concrete injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain; (d) diminution of value of their PII/PHI; and (e) the continued risk to their PII/PHI, which remains in the possession of TMLT, and which is subject to further breaches, so long as TMLT fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII/PHI.

11. TMLT failed to offer any meaningful assistance to consumers to help deal with the fraud that has and will continue to result from the Data Breach. In contrast to what has been frequently made available to consumers in other data breaches, TMLT has not offered or provided any fraud insurance and only offered basic identity monitoring services for one year.

12. Moreover, The Data Breach was a direct result of TMLT's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect consumers' PII/PHI. Despite discovering the Data Breach on October 13, 2022, TMLT inexplicably failed to provide notice to impacted customers until September 6, 2023. As a result, TMLT left a significant gap of time in which, unbeknownst to its customers, TMLT knew of and could have notified its customers of the Data Breach and advised its customers to take immediate remedial steps. Instead, TMLT left its customers exposed for an entire year.

13. TMLT has admitted that it knew of the Data Breach as early as October 12, 2022, but failed to immediately close off this unauthorized actor from access to its customers' PII/PHI– leaving the door open for this unauthorized actor to continue to collect TMLT's customers' PII/PHI for an entire day.

14. Plaintiff and the class members seek to recover damages caused by TMLT's negligence, negligence per se, breach of fiduciary duty, breach of implied contract, and unjust enrichment. Additionally, Plaintiff seeks declaratory and injunctive relief as a result of TMLT's conduct, as discussed herein.

## PARTIES

### A. Plaintiff

15. Plaintiff Arturo Bruno is a natural person and citizen and resident of Bloomingdale, Georgia.

16. Plaintiff was a customer of TMLT, which is an association of affiliated providers of medical malpractice insurance coverage.

17. In exchange for receiving medical malpractice insurance, Plaintiff provided TMLT with his PII/PHI as a regular part of TMLT's business operations.

18. On September 6, 2023, TMLT mailed Plaintiff a letter to notify him of the Data Breach and the impact to his PI/PHI. This Notice Letter stated that unauthorized actors gained access to and acquired files on TMLT's network, which included Plaintiff's PII. The comprised files contained his name, Social Security number, EIN/Tax Identification number, and date of birth.

19. Since learning of the Data Breach, Plaintiff has spent significant time in response to the Data Breach, heeding TMLT's warnings to remain vigilant. He has spent time changing passwords on his accounts and monitoring his credit reports for unauthorized activity, which may take years to discover and detect.

20. Plaintiff plans on taking additional time-consuming but reasonable and necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his credit reports for unauthorized activity.

21. As a result of TMLT's conduct and omissions, Plaintiff suffered actual damages including, without limitation, time and expenses related to monitoring his financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of his personal information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time to review their credit reports and monitor their medical records for fraud or identify theft – particularly since the compromised information includes Social Security numbers.

22. The Data Breach has also caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that TMLT has not been forthright about the cause and full scope of the PII/PHI compromised in the Data Breach.

23. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

24. Plaintiff has a continuing interest in ensuring that his PII/PHI, which, upon information and belief, remains in TMLT's possession, is protected and safeguarded from future breaches.

**B. Defendant**

25. Defendant Robert Donohoe is a citizen and resident of Texas. Upon information and belief, Robert Donohoe is the Trustee or Co-Trustee of TMLT. Defendant Robert Donohoe may be served at his residence, located at 111 Cedar Glen Cv., Austin, TX 78734.

26. TMLT is a not-for-profit trust domiciled in Texas which provides medical professional and general liability insurance to physicians, physician partnerships, ancillary providers, and healthcare facilities.

## JURISDICTION AND VENUE

27. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5 million, exclusive of interests and costs, and is a class action in which some members of the class are citizens of states different than Defendant Robert Donohoe, as Trustee of TMLT.

28. This Court has general personal jurisdiction over Defendant Robert Donohoe, as Trustee of TMLT, because Defendant Robert Donohoe is an individual domiciled in Texas. Further, TMLT is headquartered in Austin, Texas.

29. Venue properly lies in this district pursuant to 28 U.S.C. § 1391(b) because this district is the judicial district in which a substantial part of the property that is the subject of the action is situated.

## FACTUAL ALLEGATIONS

30. Plaintiff and the proposed Class are consumers of TMLT. TMLT is a private healthcare insurance trust that provide medical malpractice insurance.

31. As noted above, Plaintiff brings this class action against TMLT for its failure to properly secure and safeguard personally indefinable information, for failing to comply with industry standards to protect and safeguard that information, and for failing to provide timely, accurate, and adequate notice to Plaintiff and other members of the class that such information has been compromised.

### A. TMLT was obligated to safely protect its customers PII/PHI.

32. Plaintiff and Class Members provided their PII/PHI to TMLT with the reasonable expectation and mutual understanding that TMLT would comply with its obligations to keep such information confidential and secure from unauthorized access.

33. Plaintiff and Class Members' PII/PHI was provided to TMLT in conjunction with the type of work TMLT does in providing medical malpractice insurance. Upon information and belief, as a condition of providing medical malpractice insurance to its customers, TMLT required that each customer sign a form authorizing the use and/or disclosure of their protected health information, pursuant to HIPAA.

34. In receiving the PII/PHI as part of its services, TMLT assented and undertook legal duties to safeguard and protect the PII/PHI entrusted to them by Plaintiff and Class Members, in compliance with all applicable laws, including HIPAA.

35. TMLT's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches preceding the date they disclosed the incident.

36. However, TMLT failed to secure the PII/PHI of the individuals that provided them with this sensitive information.

**B. The TMLT Data Breach**

37. According to TMLT's press release, on October 12, 2022, TMLT identified suspicious activity.

38. According to the press release, TMLT's subsequent investigation revealed that certain personal and health information maintained on their systems was potentially accessed by an unauthorized party between October 2, 2022, and October 13, 2022. The information involved includes Social Security numbers, driver's license number/government issued identification numbers, financial account information, medical treatment and diagnosis information, and health insurance information.

39. What TMLT did not reveal were the details of the root cause of the Data Breach, the vulnerabilities exploited, whether TMLT's system is still unsecured, why TMLT decided to wait almost a year to inform impacted individuals after TMLT first detected the Data Breach, and the remedial measures TMLT was taking to ensure such a breach does not occur again. TMLT still has not explained or clarified these details to Plaintiff or the Class Members who have a vested interest in ensuring that their PII/PHI remains protected.

40. Though TMLT claimed in their notice that they "immediately took steps to secure our network, and launched an investigation" of the Data Breach, TMLT failed to secure its network for an entire day while the unauthorized user continued to exploit TMLT's network vulnerabilities.

41. Moreover, TMLT failed report the Data Breach to the Texas Attorney General until March 6, 2023. TMLT did not submit a report on the Data Breach to the Office of the Texas Attorney General as required by Texas law. Texas law specifically requires that any business that experiences a data breach "notify the attorney general of that breach not later than the 60$^{th}$ day after the date on which the person determines that the breach occurred if the breach involves at least 250 [Texas] residents." Tex. Bus. & Com. Code Ann. § 521.053.

42. According to TMLT's official filing with the Texas Attorney General, the Data Breach resulted in an unauthorized party gaining access to consumers' names, social security numbers, drivers' license numbers, financial account information, and protected health information. However, at that time, TMLT had not yet posted notice of the incident on its website, and the information provided on the Texas Attorney General's "Data Security Breach Reports" website was minimal.

43. Further, TMLT failed to report the Data Breach to the U.S. Department of Health and Human Services ("HHS") until more than 60 calendar days from discovery of the breach, in violation of HHS requirements.

44. Upon information and belief, the PII/PHI contained in the files accessed by cybercriminals was not encrypted or inadequately encrypted, as the threat actors were able to acquire and steal Plaintiff's and Class Members' PII/PHI.

45. TMLT failed to take appropriate or even the most basic steps to protect the PII/PHI of Plaintiff and other class members from being disclosed.

**C. Plaintiff and the class members have suffered as a result of the Data Breach.**

46. PII/PHI is a valuable property right.[2] The value of PII/PHI as a commodity is measurable.[3] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[4] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[5] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

---

[2] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible...").

[3] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192 (last visited January 16, 2023).

[4] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[5] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

47. Personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[6] All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[7] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[8] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[9]

48. 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.[10]

49. The value of Plaintiff's and 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

---

[6] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[7] Adam Greenberg, *Health insurance credentials fetch high prices in the online black market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

[8] *In the Dark*, VPNOverview.com, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed on January 16, 2023).

[9] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI CYBER DIVISION (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[10] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017) https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

50. It can take victims years to spot or identify PII theft, giving criminals plenty of time to milk that information for cash.

51. One such example of criminals using PII for profit is the development of "Fullz" packages.[11]

52. Cyber-criminals can cross-reference two 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.

53. 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

[11] "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) https://krebsonsecurity.com/tag/fullz/.

telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

54. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[12] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[13]

55. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[14]

56. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

---

[12] *See* https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html.

[13] *Id.*

[14] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), https://www.jstor.org/

stable/23015560?seq=1.

57. Indeed, cyberattacks against the healthcare industry have been common for over ten years with the Federal Bureau of Investigation ("FBI") warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[15]

58. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[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.[16]

59. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[17]

60. TMLT was on notice that the FBI has recently been concerned about data security regarding entities that store certain amounts of PHI, as TMLT does. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed

[15] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

[16] 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.

[17] *See* Maria Henriquez, *Iowa City Hospital Suffers PIIshing Attack,* SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-PIIshing-attack.

malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[18]

61. Plaintiff and members of the Class, as a whole, must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

62. Once PII/PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and the class members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of TMLT's conduct. Further, the value of Plaintiff's and class members' PI/PHI has been diminished by its exposure in the Data Breach.

63. As a result of TMLT's failures, Plaintiff and Class Members are at substantial risk of suffering identity theft and fraud or misuse of their PII/PHI.

64. Plaintiff and the Class suffered actual injury from having PII/PHI compromised as a result of TMLT's negligent data management and resulting Data Breach including, but not limited to (a) damage to and diminution in the value of their PII/PHI, a form of property that TMLT obtained from Plaintiff; (b) violation of their privacy rights; (c) present and increased risk arising from the identity theft and fraud; (d) loss of time and loss of productivity incurred mitigating the

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

materialized risk and imminent threat of identity theft risk; (e) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; and (f) invasion of privacy.

65. For the reasons mentioned above, TMLT's conduct, which allowed the Data Breach to occur, caused Plaintiff and members of the Class these significant injuries and harm.

66. Plaintiff brings this class action against TMLT for TMLT's failure to properly secure and safeguard PII/PHI and for failing to provide timely, accurate, and adequate notice to Plaintiff and other class members that their PII/PHI had been compromised.

## CLASS ACTION ALLEGATIONS

67. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons whose Personal Information or PHI was compromised in the Data Breach occurring in October 2022, including all individuals who Defendant mailed notice to on or around September 6, 2023.

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

69. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

70. Numerosity. The Members of the Classes are so numerous that joinder of all of them is impracticable. As noted above, there are approximately 60,000 Members.

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

a. Whether TMLT unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII/PHI;

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

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

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

e. Whether TMLT owed a duty to Class Members to safeguard their PII/PHI;

f. Whether TMLT breached their duty to Class Members to safeguard their PII/PHI;

g. Whether computer hackers obtained Class Members' PII/PHI in the Data Breach;

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

i. Whether TMLT's conduct was negligent;

j. Whether TMLT's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

k. Whether TMLT's acts breaching an implied contract they formed with Plaintiff and the Class Members;

l. Whether TMLT violated the Federal Trade Commission Act ("FTC Act");

m. Whether TMLT violated the Health Insurance Portability and Accountability Act ("HIPAA");

n. Whether TMLT was unjustly enriched to the detriment of Plaintiff and the Class;

o. Whether TMLT failed to provide notice of the Data Breach in a timely manner; and

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

72. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII/PHI, like that of every other Class Member, was compromised in the Data Breach.

73. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including data privacy litigation of this kind.

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

75. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual

Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for TMLT. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

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

77. Likewise, particular issues under are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether TMLT owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, storing, using, and safeguarding their PII/PHI;

b. Whether TMLT's data security practices were reasonable in light of best practices recommended by data security experts;

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

d. Whether TMLT failed to take commercially reasonable steps to safeguard consumer PII/PHI; and

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

78. Finally, all members of the proposed Classes are readily ascertainable. TMLT has access to Class Members' names and addresses affected by the Data Breach. At least some Class Members have already been preliminarily identified and sent notice of the Data Breach by TMLT.

## CAUSES OF ACTION

### COUNT I
### NEGLIGENCE

79. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

80. TMLT owed a duty to Plaintiff and all other Class members to exercise reasonable care in safeguarding and protecting their PII/PHI in their possession, custody, or control.

81. TMLT knew, or should have known, the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining secure systems. TMLT knew, or should have known, of the vast uptick in data breaches in recent years. TMLT had a duty to protect the PII/PHI of Plaintiff and Class Members.

82. Given the nature of TMLT's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, TMLT should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring, which TMLT had a duty to prevent.

83. TMLT breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiff's and Class members' PII/PHI.

84. It was reasonably foreseeable to TMLT that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt,

implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

85. But for TMLT's negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised.

86. As a result of TMLT's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) actual or attempted fraud.

## COUNT II
## NEGLIGENCE PER SE

87. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

88. TMLT's duties arise from, in part due to its storage of certain medical information, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule

("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

89. TMLT's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as TMLT, of failing to employ reasonable measures to protect and secure PII/PHI.

90. TMLT's duties further arise from the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. § 1302(d), *et seq.*

91. TMLT is an entity covered under HIPAA, which sets minimum federal standards for privacy and security of PHI.

92. TMLT violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class members' PII/PHI and not complying with applicable industry standards. TMLT's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

93. TMLT's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

94. Plaintiff and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

95. The harm occurring because of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

96. It was reasonably foreseeable to TMLT that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

97. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of TMLT's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiffs and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) actual or attempted fraud.

## COUNT III
## BREACH OF FIDUCIARY DUTY

98. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

99. Plaintiff and Class members either directly or indirectly gave TMLT their PII/PHI in confidence, believing that TMLT – a healthcare malpractice insurance provider – would protect that information. Plaintiff and Class members would not have provided TMLT with this information had they known it would not be adequately protected. TMLT's acceptance and storage

of Plaintiff's and Class members' PII/PHI created a fiduciary relationship between TMLT and Plaintiff and Class Members. In light of this relationship, TMLT must act primarily for the benefit of its customers, which includes safeguarding and protecting Plaintiff's and Class Members' PII/PHI.

100. TMLT has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard the PII/PHI of Plaintiff and Class Members it collected.

101. As a direct and proximate result of TMLT's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in TMLT's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

## COUNT IV
## UNJUST ENRICHMENT

102. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

103. This claim is pled in the alternative to the implied contract claim pursuant to Fed. R. Civ. P. 8(d).

104. Plaintiff and Class Members conferred a monetary benefit upon TMLT in the form of monies paid for healthcare services or other services.

105. TMLT accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. TMLT also benefitted from the receipt of Plaintiff's and Class Members' PII/PHI.

106. As a result of TMLT's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

107. TMLT should not be permitted to retain the money belonging to Plaintiff and Class Members because TMLT failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state, and local laws. and industry standards.

108. TMLT should be compelled to provide for the benefit of Plaintiff and Class Members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

## COUNT IV
## BREACH OF IMPLIED CONTRACT

109. Plaintiff realleges and incorporates by reference all allegations of the preceding factual allegations as though fully set forth herein.

110. TMLT required Plaintiff and Class Members to provide, or authorize the transfer of, their PII/PHI in order for TMLT to provide services. In exchange, TMLT entered into implied contracts with Plaintiff and Class Members in which TMLT agreed to comply with its statutory

and common law duties to protect Plaintiff's and Class Members' PII/PHI and to timely notify them in the event of a data breach.

111. Plaintiff and Class Members would not have provided their PII/PHI to TMLT had they known that TMLT would not safeguard their PII/PHI, as promised, or provide timely notice of a data breach.

112. Plaintiff and Class Members fully performed their obligations under their implied contracts with TMLT.

113. TMLT breached the implied contracts by failing to safeguard Plaintiff's and Class Members' PII/PHI and by failing to provide them with timely and accurate notice of the Data Breach.

114. The losses and damages Plaintiff and Class Members sustained (as described above) were the direct and proximate result of TMLT's breach of its implied contracts with Plaintiff and Class Members.

## JURY DEMAND

115. Plaintiff demands a trial by jury on all claims so triable.

## PRAYER

WHEREFORE, Plaintiff, individually and on behalf of the Classes, pray for judgment as follows:

a. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class and Subclass;

b. For equitable relief enjoining TMLT from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII/PHI;

c. For equitable relief compelling TMLT to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII/PHI compromised during the Data Breach;

d. For an order requiring TMLT to pay for credit monitoring services for Plaintiff and the Class of a duration to be determined at trial;

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

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

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

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

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

Dated: September 28, 2023

Respectfully submitted,

By: /s/*Bruce W. Steckler*

**Bruce W. Steckler**
TX Bar No. 00785039
bruce@swclaw.com
**Kaitlyn M. Coker**
TX Bar No. 24115264*
kcoker@swclaw.com
**STECKLER WAYNE & LOVE, PLLC**
12720 Hillcrest Road, Suite 1045
Dallas, TX 75230
Tel: (972) 387-4040
Fax: (972) 387-4041

**John G. Emerson, Jr.**
TX Bar No. 06602600
jemerson@emersonfirm.com
**EMERSON FIRM, PLLC**
2500 Wilcrest, Suite 300
Houston, TX 77042
Tel: (800) 551-8649
Fax: (501) 286-4649

**John A. Yanchunis**
TX Bar No. 22121300
jyanchunis@ForThePeople.com
**Ra Amen**
ramen@ForThePeople.com
*Pro Hac Vice Pending*
**MORGAN & MORGAN**
**COMPLEX LITIGATION GROUP**
201 North Franklin Street 7th Floor

Tampa, Florida 33602
T: (813) 223-5505
F: (813) 223-5402

**ATTORNEYS FOR PLAINTIFF AND THE PROPOSED CLASS**

*****_Admission Pending_