12/30/2021 3:07 PM
Marilyn Burgess - District Clerk Harris County
Envelope No. 60406414
By: Maria Rodriguez
Filed: 12/30/2021 3:07 PM

CAUSE NO. _____

CLIFF LEE, individually and on behalf of all others similarly situated,	:	IN THE DISTRICT COURT OF
Plaintiff,	:	HARRIS COUNTY, TEXAS
v.	:	
TEXAS EAR, NOSE & THROAT SPECIALISTS, PLLC	:	
Defendant.	:	JUDICIAL DISTRICT

PLAINTIFF'S ORIGINAL CLASS ACTION PETITION

1. Plaintiff, CLIFF LEE, individually and on behalf of all others similarly situated, bring this action against Defendant TEXAS EAR, NOSE & THROAT SPECIALISTS, PLLC. ("Texas ENT" or "Defendant") to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction over this action because the contract between Plaintiff and Defendant was established in Houston (Harris County), Texas.

3. This Court has personal jurisdiction over Defendant because it is a resident of the State of Texas.

4. Venue is proper in this County under Tex. Civ. Prac. & Rem. Code § 15.002 because a substantial part of the events or omissions giving rise to the claim occurred in this County, and also under § 15.032 because the loss occurred in this County.

NATURE OF THE ACTION

5. This class action arises out of the recent data security incident and data breach that was perpetrated against Defendant Texas ENT, which held in its possession certain personally identifiable information ("PII") and protected health information ("PHI") (collectively, "the Private Information") of Plaintiff and the putative Class Members (the "Data Breach").

6. The Private Information compromised in the Data Breach included certain personal or protected health information for patients, including individuals' full names, dates of birth, medical record numbers, procedure codes, and Social Security numbers.

7. The Private Information compromised in the Data Breach was exfiltrated by the cyber-criminals who perpetrated the attack and remains in the hands of those cyber-criminals.

8. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect consumers' Private Information.

9. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

10. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant Texas ENT's computer network in a

condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

11. Defendant disregarded the rights of Plaintiff and Class Members (defined below) by, inter alia, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff's and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members with prompt and accurate notice of the Data Breach.

12. In addition, Defendant Texas ENT and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Texas ENT properly monitored its property, it would have discovered the intrusion sooner.

13. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant Texas ENT collected and maintained is now in the hands of data thieves.

14. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims using Class Members' information, obtaining driver's licenses in Class Members'

names but with another person's photograph, and giving false information to police during an arrest.

15. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

16. Plaintiff and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

17. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

18. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

19. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) negligence *per se*, (iii) breach of implied contract, (iv) breach of fiduciary duty; (v) intrusion upon seclusion/invasion of privacy; and (vi) unjust enrichment.

PARTIES

20. Plaintiff Cliff Lee is and at all times mentioned herein was an individual citizen of the State of Texas, residing in the city of Katy, and was a patient of Defendant. Mr. Lee received notice of the Data Breach on or around December 17, 2021, attached as Exhibit A.

21. Defendant Texas Ear, Nose & Throat Specialists, PLLC. is a Texas professional association with its principal place of business at 10740 North Gessner Drive, Suite 310, Houston, Texas 77064. Defendant Texas ENT may be served by serving its Registered Agent, C T Corporation System, 1999 Bryan St., Suite 900, Dallas, TX 75201-3136.

DEFENDANT'S BUSINESS

22. Defendant Texas ENT is a comprehensive ear, nose, throat, hearing, and allergy health care provider with its business headquarters located at 10740 North Gessner Drive, Suite 310, Houston, Texas 77064 and fifteen or more treatment locations. Texas ENT includes more than 30 board-certified otolaryngologists in these fifteen locations that are spread across four counties of the Greater Houston Area. [1]

23. In addition to the medical practice it refers to as "Texas ENT Specialists," it does business as "Texas Allergy & Sinus Center," "Texas Ear Center," "Texas Facial Plastic Surgery," "Hearing Specialists of Texas," and "Texas Center for Voice and Swallowing."[2] For the purposes of this Class Action Complaint, all of its associated will be referred to collectively as "Texas ENT."

24. In the ordinary course of receiving health care services from Defendant Texas ENT, each patient must provide (and Plaintiff did provide) Defendant Texas ENT with sensitive, personal, and private information such as their own:

- Name, address, phone number, and email address;
- Date of birth;
- Social Security number;
- Information relating to the individual's medical and family history;

[1] https://texasent.com/ (last visited Dec. 29, 2021).
[2] *Id.*

- Medical record information;
- Insurance information and coverage; and
- Treatment details.

25. Defendant also creates and stores medical records and other protected health information for its patients, including records of treatments and diagnoses.

26. All of Defendant Texas ENT's employees, staff, entities, sites, and locations may share patient information with each other for various purposes, as disclosed in the HIPAA compliant privacy notice ("Privacy Policy") that Defendant Texas ENT is required to maintain.[3]

27. The Privacy Policy is provided to every patient on Texas ENT's website and upon request.

28. Defendant Texas ENT agreed to and undertook legal duties to maintain the protected health information entrusted to it by Plaintiff and Class Members safely, confidentially, and in compliance with all applicable laws, including the Health Insurance Portability and Accountability Act ("HIPAA").

29. The patient information held by Defendant Texas ENT in its computer system and network included the Private Information of Plaintiff and Class Members.

THE DATA BREACH

30. A Data Breach occurs when cyber criminals intend to access and steal Private Information that has not been adequately secured by a business entity like Texas ENT.

31. Between August 9, 2021, and August 15, 2021, according to the Data Breach Notice letters that Texas ENT sent to affected Plaintiff and the Class, unauthorized cyber criminals were able to infiltrate its patient information computer systems. According to its Data Breach letters

[3] https://texasent.com/privacy-policy/ (last visited December 29, 2021).

sent to Plaintiff and Class members, Texas ENT learned of the Data Breach from "law enforcement."[4]

32. On its website called "Notice of Security Incident," Texas ENT states that it hired a third-party cybersecurity firm that determined that unauthorized parties gained access to our computer systems and took copies of Texas ENT files between August 9, 2021, and August 15, 2021."[5]

33. Texas ENT determined the accessed files "contained patient names, dates of birth, medical record numbers, and procedure codes used for billing purposes. [And a] limited number of files also contained patient Social Security numbers."[6] Texas ENT does not publicly state how many patients' Social Security numbers were stolen.

34. Defendant's investigation further determined that, as a result of this incident, certain personal or protected health information was compromised, including names, Social Security number, date of birth, medical record number, and procedure codes (the "Private Information").

35. By October 19, 2021, Texas ENT knew that this "data security incident" resulted in the access to and theft of patient files.

36. As reported to Department of Health and Human Services Office for Civil Rights ("DHH Report") on or about December 10, 2021, Texas ENT's investigation revealed that the private health information (PHI) of 535,489 individuals was accessed by the Data Breach.[7]

---

[4] *See, e.g.,* Lee Notice of Data Breach (Dec. 10, 2021).
[5] https://texasent.com/wp-content/uploads/2021/12/Texas_ENT_Specialists_Substitute_Notice.pdf (last visited Dec. 29, 2021).
[6] *Id.*
[7] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Dec. 29, 2021).

37. As reported to the Texas Attorney General Data Security Breach ("AG Report") site on or about December 13, 2021, Texas ENT's investigation showed that cyber criminals accessed the "Name of Individual; Social Security Information; Medical Information" of 529,623 individuals.[8] No explanation is given to explain the 5,866 fewer records that appear on the AG Report as compared to the DHH Report.

38. Despite Texas ENT's Data Breach occurring between August 9 and 15, 2021, notification letters were not sent to affected patients until almost exactly 4 months later, on or around December 10, 2021.

39. Defendant openly admits that the Personal Information of Plaintiff and Class Members that was accessed without authorization and exfiltrated by the cyberthieves who perpetrated the Data Breach.[9]

40. Though Defendant claims that it "received assurances" from the attacker that "any potential exfiltrated data had been destroyed,"[10] computer experts have definitively stated that "Proof of deletion is not a thing."[11]

41. Defendant had obligations created by HIPAA, contract, industry standards, common law, and representations made to Class Members, to keep Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

[8] https://oagtx.force.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited Dec. 29, 2021).
[9] *See* Exhibit A- the Lee Letter
[10] *Id.*
[11] *See* Keith Mukai, *ArbiterSports Was Hacked. Don't Use Them Ever Again*, Medium (Aug. 29, 2020), https://medium.com/@kdmukai_64726/arbitersports-was-hacked-dont-use-them-ever-again-fddea92bcd21 (last visited Dec. 29, 2021).

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

43. Defendant's data security obligations were particularly important given the substantial increase in Data Breaches in the healthcare industry preceding the date of the breach.

44. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[12] Of the 1,473 recorded data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry.[13] The 525 reported breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.[14]

45. In 2021 alone there have been over 220 data breach incidents.[15] These approximately 220 data breach incidents have impacted nearly 15 million individuals.[16]

46. Indeed, data breaches such as the one experienced by Defendant Texas ENT have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.

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

---

[12] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last visited Dec. 29, 2021).
[13] *Id*.
[14] *Id*. at 15.
[15] *See* Kim Delmonico, Another (!) Orthopedic Practice Reports Data Breach, Orthopedics This Week (May 24, 2021), https://ryortho.com/breaking/another-orthopedic-practice-reports-data-breach/ (last visited on Dec. 29, 2021).
[16] *Id*.
[17] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited on Dec. 29, 2021).

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

Defendant Fails to Comply with FTC Guidelines

49. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

50. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[18] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[19]

51. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity

[18] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Dec. 29, 2021).
[19] *Id*.

on the network; and verify that third-party service providers have implemented reasonable security measures.

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

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

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

55. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

56. Defendant was at all times fully aware of its obligation to protect the PII and PHI of its patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

57. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

58. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees; utilizing strong passwords; creating multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; using multi-factor authentication; protecting backup data, and; limiting which employees can access sensitive data.

59. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

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

61. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

Defendant's Conduct Violates HIPAA and Evidences Its Insufficient Data Security

62. HIPAA requires covered entities such as Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information.

63. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

64. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

65. A Data Breach such as the one Defendant experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40.

66. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate it failed to comply with safeguards mandated by HIPAA regulations.

DEFENDANT'S BREACH

67. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard Texas ENT's

computer systems and Texas ENT's data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that vendors with access to Defendant's protected health data employed reasonable security procedures;

e. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

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

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

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

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

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

k. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

l. Failing to train all members of Defendant's workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); and/or

m. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).

n. Failing to notify Plaintiff of the Data Breach within 60 days after originally determining that a breach had occurred in violation of Texas Bus. & Com. Code § 521.002 and 521.053 (2007); as amended (2019), and Texas Bus. & Com. Code § 17.46.

68. As the result of computer systems in need of security upgrading, inadequate procedures for handling emails containing ransomware or other malignant computer code, and

inadequately trained employees who opened files containing the ransomware virus, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

69. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft.

DATA BREACHES PUT CONSUMERS AT AN INCREASED RISK OF FRAUD AND IDENTIFY THEFT

70. Data Breaches such as the one experiences by Texas ENT's patients are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

71. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[20]

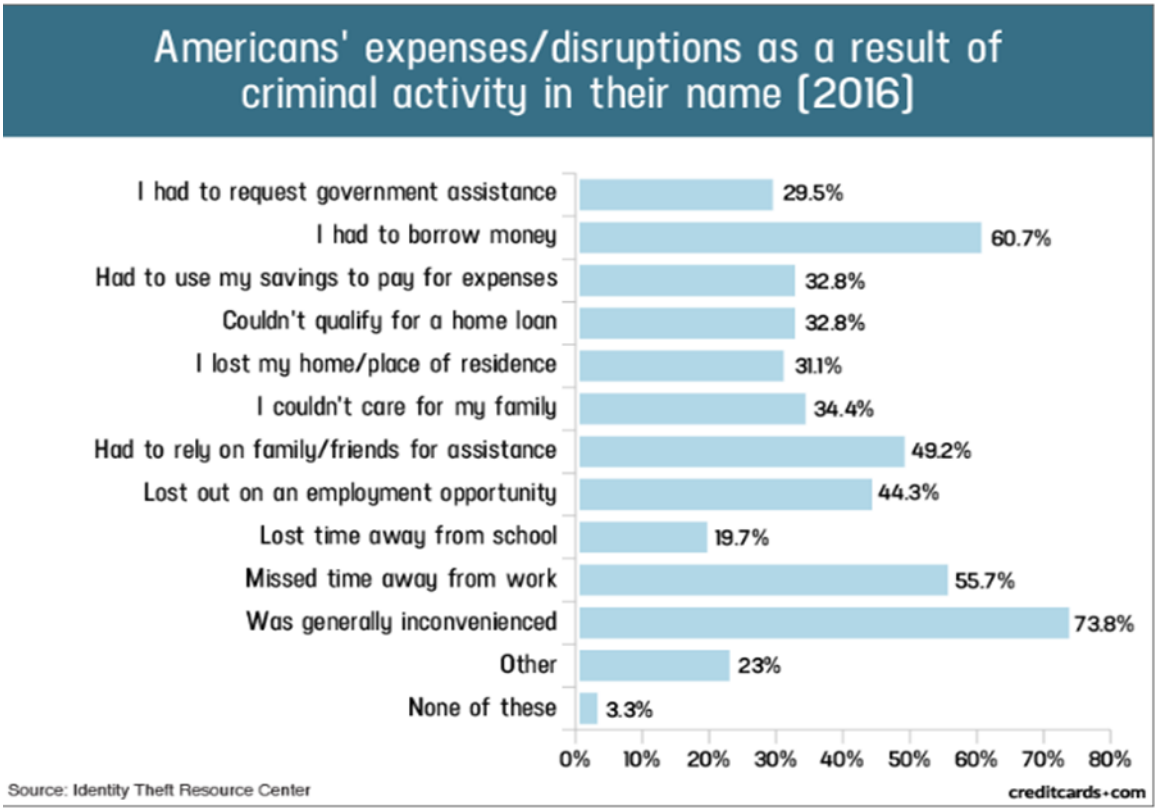
72. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[21]

73. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

[20] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Dec. 29, 2021) ("GAO Report").
[21] *See* https://www.identitytheft.gov/Steps (last visited Dec. 29, 2021).

74. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

75. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[22]



[22] "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Dec. 29, 2021).

76. Furthermore, theft of Private Information is also gravely serious. PII/PHI is a valuable property right.[23] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

77. Theft of PHI, in particular, is gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[24] Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

78. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

---

[23] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[24] *See* Federal Trade Commission, Medical Identity Theft, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited December 29, 2021).

See GAO Report, at p. 29.

79. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

80. There is a strong probability that the entirety of the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

81. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[25] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

82. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[26] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[27] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number

[25] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Dec. 29. 2021).
[26] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Dec. 29, 2021).
[27] *Id* at 4.

was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

83. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

84. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[28]

85. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[29]

86. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account. That pales in comparison with the asking price for medical data, which was selling for $50 and up.[30]

[28] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Dec. 29, 2021).
[29] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Dec. 29, 2021).
[30] https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last visited Dec. 29, 2021)

87. In recent years, the medical and financial services industries have experienced disproportionally higher numbers of data theft events than other industries. Defendant therefore knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

PLAINTIFF'S EXPERIENCES

88. Plaintiff Cliff Lee is and at all times mentioned herein was an individual citizen of the State of Texas, residing in the city of Katy.

89. Mr. Lee is currently a patient and, at all times relevant to this Complaint, was a patient of Defendant.

90. Mr. Lee received notice of the Data Breach on or around December 17, 2021, attached as Exhibit A, and was especially alarmed by the fact that his Social Security number was stolen from the Defendant's computer system. As an IT professional, he is well-aware of the risks associated with failing to protect your Social Security number. Although certain reputable types of businesses, including medical and financial organizations, require that consumers provide this information, he expected these types of organizations to secure their computers to ward off cyberattacks and exfiltration of Private Information from their systems.

91. Since he received notice of the Data Breach, he has suffered from anxiety about the Data Breach and has been forced to expend a significant amount of time verifying the security of his financial information. In addition, he has experienced an increase in spam emails, texts, and phone calls. He is aware that cybercriminals often sell Private Information, and that it could be abused months or even years after a data breach.

PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

92. To date, Defendant Texas ENT has done absolutely nothing to compensate Plaintiff Lee and Class Members for the damages they sustained in the Data Breach.

93. Defendant Texas ENT has merely offered identity monitoring services for a paltry 12 months through Experian Identity Works, but *only to those patients who, according to Texas ENT, had their Social Security Number stolen*, like Plaintiff Lee and certain other Class Members.[31]

94. This one-year limitation is inadequate when victims are likely to face many years of identity theft.

95. The Texas ENT offer is wholly inadequate as it fails to compensate all victims of the Data Breach, who commonly face multiple years of ongoing identity theft and it entirely fails to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' Private Information.

96. Furthermore, Defendant Texas ENT's credit monitoring offer to Plaintiff and Class Members squarely places the burden on Plaintiff and Class Members, rather than on the Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff and Class Members in credit monitoring services upon discovery of the breach, Defendant merely sent instructions to Plaintiff and Class Members about actions they can affirmatively take to protect themselves.[32]

97. Plaintiff and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

[31] *See* Lee Notice Letter, attached as Exhibit A.
[32] *See id.*

98. Plaintiff's Private Information was compromised and exfiltrated by cyber-criminals as a direct and proximate result of the Data Breach.

99. Plaintiff Lee was damaged in that their Private Information is in the hands of cyber criminals.

100. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an actual, present, immediate, and continuing increased risk of harm from fraud and identity theft.

101. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

102. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

103. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

104. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

105. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

106. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

107. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

108. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

109. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

110. Plaintiff and the Class Members were also injured in that they were deprived of rights they possess under Texas Bus. & Com. Code § 521.002 and 521.053 (2007); as amended (2019), for notice of the Data Breach within sixty days from when the Defendant determined the data beach occurred.

111. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

112. Defendant's delay in identifying and reporting the Data Breach caused additional harm. It is axiomatic that "[t]he quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a

victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act."[33]

113. Indeed, once a Data Breach has occurred, "[o]ne thing that does matter is hearing about a Data Breach quickly. That alerts consumers to keep a tight watch on credit card bills and suspicious emails. It can prompt them to change passwords and freeze credit reports. And notifying officials can help them catch cybercriminals and warn other businesses of emerging dangers. If consumers don't know about a breach because it wasn't reported, they can't take action to protect themselves" (internal citations omitted).[34]

114. Although their Private Information was improperly exposed between about August 9 and August 15, 2021, affected patients were not notified of the Data Breach until December 10, 2021, depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

115. As a result of Defendant's delay in detecting and notifying consumers of the Data Breach, the risk of fraud for Plaintiff and Class Members has been driven even higher.

CLASS ACTION ALLEGATIONS

116. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated.

---

[33] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, Business Wire, https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million.

[34] Consumer Reports, The Ransomware Attack Next Door Security breaches don't just hit giants like Equifax and Marriott. Breaches at small companies put consumers at risk, too, January 31, 2019, https://www.consumerreports.org/data-theft/the-data-breach-next-door/

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

> All persons whose Private Information was compromised as a result of the Data Breach announced by Texas ENT on or about December 10, 2021 (the "Class").

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

119. 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. The proposed Class meets the criteria for certification under Rule 42(a), (b)(2), and (b)(3).

120. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of approximately 535,489 individuals whose data was compromised in the Data Breach.

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

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

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

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

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

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

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

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

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

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

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's conduct was per se negligent;

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

m. Whether Defendant was unjustly enriched;

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

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

122. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class member, was compromised in the Data Breach.

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

124. Predominance. Defendant 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 Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

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

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

127. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

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

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

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

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

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

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

CAUSES OF ACTION

FIRST COUNT
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

129. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

130. Defendant Texas ENT required Plaintiff and Class Members to submit non-public personal information in order to obtain medical services.

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

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

133. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant Texas ENT and its patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach or data breach.

134. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

135. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

136. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

137. Defendant breached its duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

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

c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

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

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

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

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

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

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

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

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

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

SECOND COUNT
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and All Class Members)

143. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

144. When Plaintiff and Class Members provided their Private Information to Defendant Texas ENT in exchange for Defendant Texas ENT's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

145. Defendant Texas ENT solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

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

147. Plaintiff and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

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

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

150. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

151. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

152. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged herein, including the loss of the benefit of the bargain.

153. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

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

THIRD COUNT
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and All Class Members)

155. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

156. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

157. Pursuant to HIPAA, 42 U.S.C. § 1302d, et seq., Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

158. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which

there is a low probability of assigning meaning without use of a confidential process or key." See definition of encryption at 45 C.F.R. § 164.304.

159. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

160. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

161. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

162. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that they failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

163. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

FOURTH COUNT
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and All Class Members)

164. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

165. In light of the special relationship between Defendant Texas ENT and Plaintiff and Class Members, whereby Defendant became guardian of Plaintiff's and Class Members' Private

Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

166. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Texas ENT's relationship with its patients, in particular, to keep secure their Private Information.

167. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discovery, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

168. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Private Information.

169. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

170. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

171. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) 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; (v) the continued risk to their Private Information, 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 Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

172. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

FIFTH COUNT
INTRUSION UPON SECLUSION / INVASION OF PRIVACY
(On Behalf of Plaintiff and All Class Members)

173. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

174. The State of Texas recognizes the tort of Intrusion upon Seclusion, and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 652B (1977).

175. Plaintiff and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

176. Defendant's conduct as alleged above intruded upon Plaintiff's and Class Members' seclusion under common law.

177. By intentionally failing to keep Plaintiff's and Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiff's and Class Members' privacy by:

a. Intentionally and substantially intruding into Plaintiff's and Class Members' private affairs in a manner that identifies Plaintiff and Class Members and that would be highly offensive and objectionable to an ordinary person; and

b. Intentionally publicizing private facts about Plaintiff and Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiff and Class Members.

178. Defendant knew that an ordinary person in Plaintiff's or Class Members' position would consider Defendant's intentional actions highly offensive and objectionable.

179. Defendant invaded Plaintiff's and Class Members' right to privacy and intruded into Plaintiff's and Class Members' private affairs by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

180. Defendant intentionally concealed from and delayed reporting to Plaintiff and Class Members a security incident that misused and/or disclosed their Private Information without their informed, voluntary, affirmative, and clear consent.

181. The conduct described above was at or directed at Plaintiff and the Class Members.

182. As a proximate result of such intentional misuse and disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct amounted to a substantial and serious invasion of

Plaintiff's and Class Members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

183. In failing to protect Plaintiff's and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private. Plaintiff, therefore, seeks an award of damages on behalf of himself and the Class.

SIXTH COUNT
UNJUST ENRICHMENT
(On Behalf of Plaintiff and All Class Members)

184. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein. Plaintiff brings this claim individually and on behalf of all Class Members. This count is plead in the alternative to the breach of contract count above.

185. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

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

187. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and/or its agents and in so doing provided Defendant with their Private Information. In exchange, Plaintiff and Class Members

should have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

188. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

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

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

191. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

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

193. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

194. Plaintiff and Class Members have no adequate remedy at law.

195. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts 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; (f) the continued risk to their Private Information, 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 Private Information in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Class;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

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

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

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

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

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

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

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

JURY TRIAL DEMANDED

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

Dated: December 30, 2021

Respectfully submitted,

/s/ Jarrett L. Ellzey
Jarrett L. Ellzey
Texas Bar No. 24040864
Leigh Montgomery
Texas Bar No. 24052214
Ellzey & Associates, PLLC
1105 Milford Street
Houston, Texas 77066
Telephone: (713) 554-2377
Facsimile: (888) 276-3455
jarett@ellzeyaw.com
leigh@ellseylaw.com

Gary E. Mason*
David K. Lietz*
MASON LIETZ & KLINGER LLP
5301 Wisconsin Avenue, NW
Suite 305
Washington, DC 20016
Tel: (202) 429-2290
gmason@masonllp.com
dlietz@masonllp.com

and

Gary M. Klinger*
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60630
Tel.: (312) 283-3814
gklinger@masonllp.com

**pro hac vice to be filed*

Attorneys for Plaintiff