D-1-GN-23-007662

CAUSE NO. _____

CURTIS WILSON, EBONY WRIGHT, and CARLA MOLINELLI individually and on behalf of all others similarly situated,	§	IN THE DISTRICT COURT
Plaintiffs,	§	261ST, DISTRICT COURT
v.	§	_____ JUDICIAL DISTRICT
LONGHORN IMAGING CENTER, LLC,	§	
Defendant.		TRAVIS COUNTY, TEXAS

PLAINTIFFS' ORIGINAL CLASS ACTION PETITION

TO THE HONORABLE JUDGE OF SAID COURT:

COME NOW, Plaintiffs Curtis Wilson, Ebony Wright, and Carla Molinelli, individually and on behalf of all others similarly situated, upon personal knowledge of all facts pertaining to themselves and on information and belief as to all other matters, by and through the undersigned counsel, bring this Class Action Complaint against Defendant Longhorn Imaging Center, LLC ("Defendant" and/or "Longhorn Imaging").

I. NATURE OF THE ACTION

1. Plaintiffs bring this action, individually and on behalf of all others similarly situated, whose private and confidential protected health information ("PHI")—including their name, medical information, and health insurance information—was compromised in a massive security breach of Longhorn Imaging's computer servers (the "Data Breach").

2. As alleged herein, Longhorn Imaging's failure to implement adequate data security measures to protect its consumers' sensitive PHI and proximately caused injuries to Plaintiffs and the class members.

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

4. By collecting, using, and deriving a benefit from the PHI of Plaintiffs and Class Members, Longhorn Imaging assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

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

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

7. Had Longhorn Imaging adequately designed, implemented, and monitored its network and servers, the Data Breach would have been prevented.

8. Had Plaintiffs and Class Members known that Longhorn Imaging's data security was below industry standards, Plaintiffs and Class Members would not have provided their PHI to Longhorn Imaging or relied on Longhorn Imaging to protect that information.

9. As a result of Longhorn Imaging's inadequate data security practices that resulted in the Data Breach, Plaintiffs 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 PHI; (e) the continued risk to their health; and (f) the continued risk to their PHI, which remains in the possession of Longhorn Imaging, and which is subject to further breaches, so long as Longhorn Imaging fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PHI.

10. The Data Breach was a direct result of Longhorn Imaging's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect consumers' PHI.

11. Longhorn Imaging 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, Longhorn Imaging has not offered or provided any fraud insurance.

12. Despite discovering the Data Breach in June of 2023, Longhorn Imaging inexplicably failed to provide notice to impacted customers until September 28, 2023. As a result, Longhorn Imaging left a significant gap of time in which, unbeknownst to its customers, Longhorn Imaging knew of and could have notified its customers of the Data Breach and advised its customers to take immediate remedial steps. Instead, Longhorn Imaging left its customers exposed.

13. Plaintiffs and Class Members seek to recover damages caused by Longhorn Imaging's negligence, negligence per se, breach of fiduciary duty, breach of implied contract, and

unjust enrichment. Additionally, Plaintiffs seek declaratory and injunctive relief as a result of Longhorn Imaging's conduct, as discussed herein.

II. PARTIES

14. Plaintiff Curtis Wilson is an individual residing in Guadalupe County, Texas.

15. Plaintiff Ebony Wright is an individual residing in Bell County, Texas.

16. Plaintiff Carla Molinelli is an individual residing in Williamson County, Texas.

17. Defendant Longhorn Imaging Center, LLC is a limited liability company organized and existing under the laws of the State of Texas. Longhorn Imaging's principal office is located in Travis County, Texas. Longhorn Imaging may be served by and through its registered agent, Patricio Guadiano, at 4316 James Casey, Bldg. F, Suite 110, Austin, TX 78745, or wherever else he may be found.

III. JURISDICTION & VENUE

18. This Court has subject matter jurisdiction, as the amount in controversy exceeds the minimum jurisdictional limits of this Court.

19. Venue is proper in Travis County, Texas pursuant to Texas Civil Practice & Remedies Code § 15.002(a)(3), as Travis County is the county of the Defendant's principal office in the State of Texas.

IV. FACTS

20. Plaintiffs and the proposed Class are consumers of Longhorn Imaging. Longhorn Imaging is a prominent medical imaging service.

21. As noted above, Plaintiffs bring this class action against Longhorn Imaging for its failure to properly secure and safeguard PHI, for failing to comply with industry standards to protect and safeguard that information, and for failing to provide timely, accurate, and adequate notice to Plaintiffs and other members of the class that such information has been compromised.

A. Longhorn Imaging was obligated to safely protect its consumers' PHI.

22. Plaintiffs' and Class Members' PHI was provided to Longhorn Imaging in conjunction with the type of work Longhorn Imaging does in providing medical imaging. Upon information and belief, as a condition of providing its services to its customers, Longhorn Imaging required that each customer sign a form authorizing the use and/or disclosure of their protected health information, pursuant to HIPAA.

23. Plaintiffs and Class Members provided their PHI to Longhorn Imaging with the reasonable expectation and mutual understanding that Longhorn Imaging would comply with its obligations to keep such information confidential and secure from unauthorized access.

24. In receiving the PHI as part of its services, Longhorn Imaging assented and undertook legal duties to safeguard and protect the PHI entrusted to them by Plaintiffs and Class Members, in compliance with all applicable laws, including HIPAA.

25. These duties included the obligation to mitigate cybersecurity risks and enhance data breach resilience through a tailored cybersecurity program. This required Longhorn Imaging to, at very least, perform a risk assessment to identify areas for improvement and to provide security responses and recommended controls for each stage of a ransomware attack, including phishing prevention, multi-factor authentication, endpoint detection and response, and network segmentation.

26. Longhorn Imaging's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting medical facilities preceding the date they disclosed the incident. According to the 2023 State of Ransomware in Healthcare report

by Sophos, 66% of surveyed healthcare organizations fell victim to a ransomware attack in 2023; and ransomware is arguably the biggest cyber risk facing the healthcare sector today.[1]

27. 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."[2]

28. 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.[3]

29. Longhorn Imaging was on notice that the FBI has recently been concerned about data security regarding entities that store certain amounts of PHI, as Longhorn Imaging 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 malicious actors targeting healthcare related systems, perhaps for the purpose of

---

[1]*The State of Ransomware in Healthcare in 2023*, SOPHOS (Aug. 2023) (last accessed Oct. 17, 2023), *available at* https://www.sophos.com/en-us/whitepaper/state-of-ransomware-in-healthcare.

[2]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.

[3]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.

obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[4]

30. However, Longhorn Imaging ignored these warnings and failed to ensure security for the PHI of the individuals that provided them with this sensitive information. Its loose data protection policies and practices left its patients' data exposed.

B. The Longhorn Imaging Data Breach exposed thousands of patients' PHI.

31. According to Longhorn Imaging's Notice of Data Security Incident letter, in June of 2023, it was notified of a cyber incident impacting its internal patient portal.

32. Longhorn Imaging was not forthcoming about any specifics. In Plaintiffs' Notice of Data Security Incident Letter, dated September 28, 2023, Longhorn Imaging merely identified that her name, medical information, and health insurance information was subjected to the attack.

33. Moreover, Longhorn Imaging did not reveal the details or the root cause of the Data Breach, the vulnerabilities exploited, whether Longhorn Imaging's system is still unsecured, or any remedial measures Longhorn Imaging was taking to ensure such a breach does not occur again. Longhorn Imaging still has not explained or clarified these details to Plaintiffs or the Class Members who have a vested interest in ensuring that their PHI remains protected.

34. However, according to Cyber Express, a leading cybersecurity news provider, the Longhorn Imaging Data Breach was far more injurious than Longhorn Imaging admitted: it

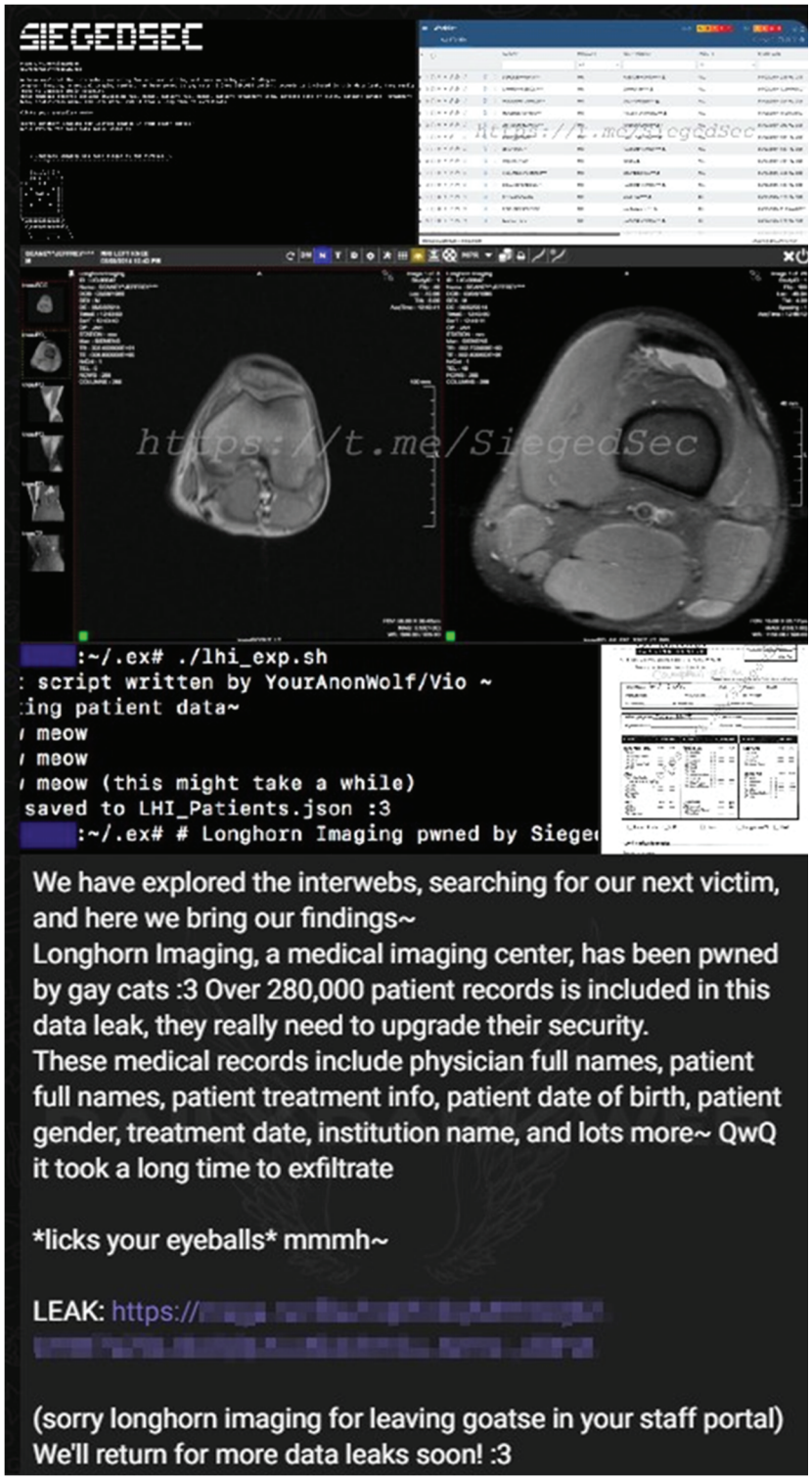
[4]Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820.

resulted in a successful infiltration of the company's extensive database containing more than 280,000 patient records.[5]

35. The notorious hacker group SiegedSec claimed responsibility. In a twitter post, Daily Dark Web (a dark web forum typically used by cybercriminals to share stolen data and boast

[5]Ashish Khaitan, *Longhorn Cyber Attack Puts Data of 28000 Patients at Risk*, The Cyber Express (Jun. 7, 2023) (last accessed Oct. 17, 2023), *available at* https://thecyberexpress.com/longhorn-cyber-attack-data-28000-patients-risk/.

about their exploits), shared a screenshot of the statement made by the threat actor responsible for the data breach:



36. The leaked data reportedly included a vast range of sensitive information such as full names of physicians and patients, patient treatment details, dates of birth, genders, treatment dates, institution names, and various other details pertaining to patient healthcare.

37. Longhorn Imaging failed to take appropriate or even the most basic steps to protect the PHI of Plaintiffs and other Class Members from being disclosed. Upon information and belief, Longhorn Imaging failed to adequately perform a risk assessment to identify areas for improvement or put in place adequate security responses, phishing prevention, multi-factor authentication, endpoint detection and response, or network segmentation.

38. Further, upon information and belief, the PHI contained in the files accessed by cybercriminals was not encrypted or inadequately encrypted, as the threat actors were able to acquire and steal Plaintiffs' and Class Members' PHI.

39. Unfortunately, Longhorn Imaging has not reported this data breach to 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 30th 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.

C. Plaintiffs and the Class Members have suffered as a result of the Data Breach.

40. Personally Identifying Information ("PII") is a valuable property right.[6] Its value as a commodity is measurable.[7] "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."[8] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[9] 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.

41. Personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[10] 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

[6]*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...").

[7]*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).

[8]*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.

[9]*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/.

[10]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/.

$1,200 to $1,300 each on the black market.[11] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[12]

42. Stolen PHI is one of the most valuable commodities on the criminal information black market. According to both a report released by the Federal Bureau of Investigation's Cyber Division[13] and ClearDATA Chief Privacy and Security Officer and Founder Chris Bowen, a medical record is 50 times more valuable than a credit card number.[14] As Mr. Bowen explains: "[i]t is not just the credit card. You can build an entire persona around a health record. You can create or seek medical treatment, abuse drugs, or get prescriptions. The lifespan is so much longer than a credit card."[15]

43. Moreover, according to the National Association of Healthcare Access Management, stolen PHI can result in medical identity theft which can pose a threat to not just a person's finances, but also their health – it has been referred to "the privacy crime that can

[11] 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.

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

[13] *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.

[14] Will Maddox, *Why Medical Data is 50 Times More Valuable Than a Credit Card*, D. Magazine (Oct. 15, 2019) (last accessed Oct. 17, 2023), *available at* https://www.dmagazine.com/healthcare-business/2019/10/why-medical-data-is-50-times-more-valuable-than-a-credit-card/.

[15] *Id.*

kill."[16]Thieves have the potential to alter personal medical records, including blood type, allergies, or medicine, which can have a potentially fatal outcome.[17]

44. Moreover, criminals can use stolen PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[18] 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."[19]

45. It can take victims years to spot or identify PHI theft and is easily concealed, giving criminals plenty of time to milk that information for cash. Only ten (10) percent of victims report receiving a satisfactory resolution to their stolen PHI, and those who found a resolution spent more than 200 working hours to do so.[20]

46. 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

[16]Laurie Zabel, CHC, CPC, *The Value of Personal Medical Information: Protecting Against Data Breaches*, National Association of Healthcare Access Management (last accessed Oct. 17, 2023), *available at* https://www.naham.org/page/ConnectionsThe-Value-of-Personal-Medical-Information.

[17]*Id.*

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

[19] *Id.*

[20]Zabel, *supra* n.16.

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."[21]

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

48. Plaintiffs 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.

49. Once 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, Plaintiffs and the Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Longhorn Imaging's conduct. Further, the value of Plaintiffs' and Class Members' PHI has been diminished by its exposure in the Data Breach.

50. As a result of Longhorn Imaging's failures, Plaintiffs and Class Members are at substantial risk of suffering identity theft and fraud or misuse of their PHI.

51. Plaintiffs and the Class Members suffered actual injury from having PHI compromised as a result of Longhorn Imaging's negligent data management and resulting Data

[21] 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.

Breach including, but not limited to (a) damage to and diminution in the value of their PHI, a form of property that Longhorn Imaging obtained from Plaintiffs; (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 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.

52. For the reasons mentioned above, Longhorn Imaging's conduct, which allowed the Data Breach to occur, caused Plaintiffs and members of the Class these significant injuries and harm.

53. Plaintiffs bring this class action against Longhorn Imaging for Longhorn Imaging's failure to properly secure and safeguard PHI and for failing to provide timely, accurate, and adequate notice to Plaintiffs and other Class Members that their PHI had been compromised.

V. CLASS ALLEGATIONS

54. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> All persons whose PHI was compromised in the Data Breach occurring in June of 2023, including all individuals to whom Longhorn Imaging mailed notice to on or around September 28, 2023.

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

56. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

57. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. As noted above, there are approximately 280,000 Members.

58. 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 Longhorn Imaging unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PHI;

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

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

e. Whether Longhorn Imaging owed a duty to Class Members to safeguard their PHI;

f. Whether Longhorn Imaging breached their duty to Class Members to safeguard their PHI;

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

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

i. Whether Longhorn Imaging's conduct was negligent;

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

k. Whether Longhorn Imaging's acts breaching an implied contract they formed with Plaintiffs and the Class Members;

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

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

n. Whether Longhorn Imaging was unjustly enriched to the detriment of Plaintiffs and the Class;

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

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

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

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

61. Predominance. Longhorn Imaging has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Longhorn Imaging'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.

62. 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 Longhorn Imaging. 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.

63. Longhorn Imaging 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.

64. Likewise, particular issues 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 Longhorn Imaging owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, using, and safeguarding their PHI;

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

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

d. Whether Longhorn Imaging failed to take commercially reasonable steps to safeguard consumer PHI; and

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

65. Finally, all members of the proposed Class are readily ascertainable. Longhorn Imaging 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 Longhorn Imaging.

VI. CAUSES OF ACTION

A. Count I - Negligence

66. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

67. Longhorn Imaging owed a duty to Plaintiffs and all other Class Members to exercise reasonable care in safeguarding and protecting the PHI in their possession, custody, or control.

68. Longhorn Imaging knew, or should have known, the risks of collecting and storing Plaintiffs' and all other Class Members' PHI and the importance of maintaining secure systems. Longhorn Imaging knew, or should have known, of the vast uptick in data breaches in recent years. Longhorn Imaging had a duty to protect the PHI of Plaintiffs and Class Members.

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

70. Longhorn Imaging breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' 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 PHI entrusted to it—including Plaintiffs' and Class Members' PHI.

71. It was reasonably foreseeable to Longhorn Imaging that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' 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 Plaintiffs' and Class Members' PHI to unauthorized individuals.

72. But for Longhorn Imaging's negligent conduct or breach of the above-described duties owed to Plaintiffs and Class Members, their PHI would not have been compromised.

73. As a result of Longhorn Imaging's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs 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 PHI; (iii) breach of the confidentiality of their PHI; (iv) deprivation of the value of their 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.

B. Count II – Negligence Per Se

74. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

75. Longhorn Imaging'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").

76. Longhorn Imaging'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 Longhorn Imaging, of failing to employ reasonable measures to protect and secure PHI.

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

78. Longhorn Imaging is an entity covered under HIPAA, which sets minimum federal standards for privacy and security of PHI.

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

80. Longhorn Imaging's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

81. Plaintiffs 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.

82. 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.

83. It was reasonably foreseeable to Longhorn Imaging that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' 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 Plaintiffs' and Class Members' PHI to unauthorized individuals.

84. The injury and harm that Plaintiffs and the other Class Members suffered was the direct and proximate result of Longhorn Imaging'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 PHI; (iii) breach of the confidentiality of their PHI; (iv) deprivation of the value of their 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.

C. Count III – Breach of Fiduciary Duty

85. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

86. Plaintiffs and Class Members either directly or indirectly gave Longhorn Imaging their PHI in confidence, believing that Longhorn Imaging – a healthcare provider – would protect that information. Plaintiffs and Class Members would not have provided Longhorn Imaging with this information had they known it would not be adequately protected. Longhorn Imaging's acceptance and storage of Plaintiffs' and Class Members' PHI created a fiduciary relationship between Longhorn Imaging and Plaintiffs and Class Members. In light of this relationship, Longhorn Imaging must act primarily for the benefit of its customers, which includes safeguarding and protecting Plaintiffs' and Class Members' PHI.

87. Longhorn Imaging has a fiduciary duty to act for the benefit of Plaintiffs 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 Plaintiffs' and Class Members' PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard the PHI of Plaintiffs and Class Members it collected.

88. As a direct and proximate result of Longhorn Imaging's breaches of its fiduciary duties, Plaintiffs 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 PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their 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 PHI which remains in Longhorn Imaging'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 PHI compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

D. Count IV – Unjust Enrichment

89. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

90. Plaintiffs and Class Members conferred a monetary benefit upon Longhorn Imaging in the form of monies paid for healthcare services or other services.

91. Longhorn Imaging accepted or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members. Longhorn Imaging also benefitted from the receipt of Plaintiffs' and Class Members' PHI.

92. As a result of Longhorn Imaging's conduct, Plaintiffs 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 Plaintiffs and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

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

94. Longhorn Imaging should be compelled to provide for the benefit of Plaintiffs and Class Members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

E. Count V – Breach of Implied Contract

95. Plaintiffs reallege and incorporate by reference all allegations of the preceding factual allegations as though fully set forth herein.

96. Longhorn Imaging required Plaintiffs and Class Members to provide, or authorize the transfer of, their PHI in order for Longhorn Imaging to provide services. In exchange, Longhorn Imaging entered into implied contracts with Plaintiffs and Class Members in which Longhorn Imaging agreed to comply with its statutory and common law duties to protect Plaintiffs' and Class Members' PHI and to timely notify them in the event of a data breach.

97. Plaintiffs and Class Members would not have provided their PHI to Longhorn Imaging had they known that Longhorn Imaging would not safeguard their PHI, as promised, or provide timely notice of a data breach.

98. Plaintiffs and Class Members fully performed their obligations under their implied contracts with Longhorn Imaging.

99. Longhorn Imaging breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' PHI and by failing to provide them with timely and accurate notice of the Data Breach.

100. The losses and damages Plaintiffs and Class Members sustained (as described above) were the direct and proximate result of Longhorn Imaging's breach of its implied contracts with Plaintiffs and Class Members.

VII. JURY DEMAND

101. Plaintiffs demand a jury trial and tender the appropriate fee contemporaneously with this Petition.

VIII. PRAYER

WHEREFORE, Plaintiffs, individually and on behalf of the Class, pray for judgment as

follows:

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

b. For equitable relief enjoining Longhorn Imaging from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' PHI;

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

d. For an order requiring Longhorn Imaging to pay for credit monitoring services for Plaintiffs 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: October 20, 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 PLAINTIFFS AND THE PROPOSED CLASS

Automated Certificate of eService

This automated certificate of service was created by the efiling system. The filer served this document via email generated by the efiling system on the date and to the persons listed below. The rules governing certificates of service have not changed. Filers must still provide a certificate of service that complies with all applicable rules.

Jamie Baciak on behalf of Bruce Steckler
Bar No. 785039
jamie@swclaw.com
Envelope ID: 80800684
Filing Code Description: Petition
Filing Description: PLAINTIFFS' ORIGINAL CLASS ACTION PETITION
Status as of 10/24/2023 9:47 AM CST

Case Contacts

Name	BarNumber	Email	TimestampSubmitted	Status
Bruce WilliamSteckler		bruce@swclaw.com	10/20/2023 10:05:15 AM	SENT
Kaitlyn Coker		kcoker@swclaw.com	10/20/2023 10:05:15 AM	SENT
Jamie Baciak		jamie@swclaw.com	10/20/2023 10:05:15 AM	SENT