COMMONWEALTH OF MASSACHUSETTS

HAMPDEN, ss.

SUPERIOR COURT DEPARTMENT
CIVIL ACTION NO. 2479CV00652

EUGENE MITCHELL, WANDA DELRIO, and RAFFAELE SANTANIELLO, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

GANDARA MENTAL HEALTH CENTER, INC.,

Defendant.

AMENDED CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

AMENDED CLASS ACTION COMPLAINT

Plaintiffs Eugene Mitchell, Wanda DelRio and Raffaele Santaniello ("Plaintiffs") bring this Amended Class Action Complaint against Defendant Gandara Mental Health Center, Inc. ("Defendant"), in their individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard Plaintiffs' and other similarly situated current and former patients' ("Class Members," defined *infra*) sensitive information, including personally identifiable information ("PII") including names, addresses, dates of birth, driver's license numbers, Social Security

numbers, and protected health information ("PHI") including medical treatment / diagnosis information, and health insurance information (together "PII/PHI" or "Private Information").[1]

2. Defendant provides behavioral health, substance abuse and preventative services at 100 locations throughout the Commonwealth of Massachusetts, including to a bilingual community.[2]

3. Defendant received Plaintiffs and Class Members' Private Information in its provision of health services to Plaintiffs and Class Members.

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

5. On or about October 24, 2024, Defendant announced that certain systems in its network had been accessed by an unauthorized third party ("Data Breach"). The Private Information of tens of thousands of individuals is believed to have been exposed by the Data Breach.[3]

6. Defendant failed to adequately protect Plaintiffs' and Class Members' Private Information—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect its patients' sensitive data. Hackers targeted and obtained Plaintiffs' and Class Members' Private Information because of its value in

[1] Gandara Mental Health Center, Notice of Data Security Incident (Oct. 24, 2024), https://www.gandaracenter.org/general-4 (last visited Nov. 1, 2024).

[2] https://www.gandaracenter.org/about-gandara (last visited Nov. 1, 2024).

[3] *See* Notice Letter sent to Plaintiff by Defendant (Oct. 24, 2024), attached hereto as ***Exhibit A***.

exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

7. Plaintiffs bring this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure its network containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal statutes.

8. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the Private Information of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the Private Information of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party.

9. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

10. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) an increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse;

and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Private Information. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose Private Information was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

PARTIES

11. Plaintiff Eugene Mitchell is and was, at all times material hereto, a resident and citizen of Sandwich, Massachusetts, where he intends to remain. Plaintiff Raffaele Santaniello is and was, at all times material hereto, a resident and citizen of Massachusetts, where he intends to remain. Wanda DelRio is and was, at all times material hereto, a resident and citizen of Massachusetts, where she intends to remain.

12. Defendant is a Massachusetts corporation with its principal place of business located at 933 E. Columbus Ave., Springfield, MA 01105.

JURISDICTION AND VENUE

13. The Court has jurisdiction pursuant to M.G.L. c. 212, § 4, c. 223A, §§ 2 and 3. Further, the amount in controversy exceeds $50,000.00, exclusive of interest and costs.

14. This action does not qualify for federal jurisdiction under the Class Action Fairness Act because the home-state controversy exception under 28 U.S.C. § 1332(d)(4)(B) applies to this action because (1) more than two-thirds of the members of the proposed Class are citizens of the Commonwealth of Massachusetts, and (2) Defendant is a citizen of the Commonwealth of Massachusetts.

15. This Court has personal jurisdiction over Defendant because it is headquartered in Massachusetts and Defendant's conduct occurred in Massachusetts.

16. Venue is proper in this Court pursuant to M.G.L. c. 223, § 1 because some of the parties reside or transact business in this county.

FACTUAL ALLEGATIONS

Background

17. Since 1977, Defendant has been providing mental and behavioral health services to diverse communities, including Hispanics and African Americans. Today, Defendant has more than 100 locations throughout the state.[4]

18. Plaintiffs provided their Private Information to Defendant in connection with health care services they received from Defendant.

19. The information held by Defendant in its computer systems at the time of the Data Breach included the unencrypted Private Information of Plaintiffs and Class Members.

20. Upon information and belief, Defendant made promises and representations to its patients, including Plaintiffs and Class Members, that their Private Information would be kept safe and confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

21. Plaintiffs' and Class Members' Private Information was provided to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

[4] *Id*.

22. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiffs and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

23. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep consumer's Private Information safe and confidential.

24. Defendant had obligations created by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

25. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform the services it provides.

26. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

The Data Breach

27. On October 24, 2024, Defendant announced that an unauthorized actor gained access to certain files and data stored within its systems.

28. The Notice of Data Security Incident posted on Defendant's website states:

> On June 20, 2024, Gándara became aware of unusual activity within its network environment. In response, Gándara immediately took steps to secure its network and launched an investigation with the assistance of independent cybersecurity experts. As a result, Gándara learned that that certain personal / protected health

> information was acquired without authorization. Gándara then engaged a third-party vendor to commence a comprehensive review of the affected data. On October 1, 2024, that review concluded and Gándara learned of the identities of individuals involved. Gándara then took steps to provide notification as quickly as possible.
>
> The affected information may have included names, addresses, dates of birth, driver's license numbers, Social Security numbers, medical treatment / diagnosis information, and health insurance information. Please note that not all data elements were affected for all individuals.
>
> As soon as the incident was discovered, Gándara took the steps referenced above. Gándara notified the Federal Bureau of Investigation and will provide whatever cooperation is necessary to hold the perpetrators accountable. Gándara also notified the U.S. Health and Human Services Office for Civil Rights and consumer reporting agencies of this incident. Gándara is also taking additional steps to prevent a similar event from occurring in the future.[5]

29. Worryingly, Defendant already admitted that that "personal / protected health information ***was acquired*** without authorization."[6]

30. And yet, Defendant waited over until October 24, 2024, before it began notifying the class—a full 126 days after the Data Breach was discovered.

31. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

32. The attacker accessed and acquired files containing unencrypted Private Information of Plaintiffs and Class Members. Plaintiffs' and Class Members' Private Information was accessed and stolen in the Data Breach.

---

[5] *See* Garda Mental Health Center, Notice of Data Security Incident (Oct. 24, 2024), https://www.gandaracenter.org/general-4 (last visited Nov. 1, 2024) (emphasis added).

[6] *Id*.

33. Plaintiffs further believe that their Private Information, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

Defendant Acquires, Collects, and Stores the Private Information of Plaintiffs and Class Members

34. Defendant derives a substantial economic benefit from providing health care services to its patients, and as a part of providing that service, Defendant retains and stores Plaintiffs' and Class Members' Private Information.

35. By obtaining, collecting, and storing the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting the Private Information from disclosure.

36. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

37. Defendant's patients, including Plaintiffs and Class Members, relied on Defendant to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

38. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiffs and Class Members.

39. Upon information and belief, Defendant made promises to Plaintiffs and Class Members to maintain and protect Plaintiffs' and Class Members' Private Information, demonstrating an understanding of the importance of securing Private Information.

40. Defendant's negligence in safeguarding the Private Information of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Defendant Knew or Should Have Known of the Risk Because Institutions in Possession of Private Information are Particularly Susceptible to Cyber Attacks.

41. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting institutions that collect and store Private Information, like Defendant, preceding the date of the Data Breach.

42. Data thieves regularly target institutions like Defendant due to the highly sensitive information in their custody. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

43. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[7]

44. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the Private Information it collected and maintained would be targeted by cybercriminals.

[7] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (https://notified.idtheftcenter.org/s/), at 6.

45. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

46. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being compromised.

47. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially tens of thousands of individuals' detailed, Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

48. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

49. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen—particularly PHI—fraudulent use of that information and damage to victims may continue for years.

Value of Personally Identifiable Information

50. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[8] The FTC describes "identifying information" as "any name or number that may be used, alone or

[8] 17 C.F.R. § 248.201 (2013).

in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[9]

51. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[10]

52. For example, Private Information can be sold at a price ranging from $40 to $200.[11] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[12]

53. Theft of PHI is also 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."[13]

54. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information (e.g., patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to

---

[9] *Id.*

[10] *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/.

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

[12] *In the Dark*, VPNOVERVIEW, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

[13] *Medical I.D. Theft*, EFraudPrevention https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected.

cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, Private Information is a valuable commodity for which a "cyber black market" exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites. Unsurprisingly, the health care industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

55. Between 2005 and 2019, at least 249 million people were affected by health care data breaches.[14] Indeed, during 2019 alone, over 41 million health care records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[15] In short, these sorts of data breaches are increasingly common, especially among health care systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[16]

56. According to account monitoring company LogDog, medical data sells for $50 and up on the dark web.[17]

57. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[18]

---

[14] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/.

[15] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/.

[16] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches/.

[17] [17] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

[18] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/.

58. A study by Experian found that the average cost of medical identity theft is "about $20,000" per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for health care they did not receive to restore coverage.[19] Almost half of medical identity theft victims lose their health care coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[20]

59. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach—PHI and names—is impossible to "close" and difficult, if not impossible, to change.

60. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[21]

61. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

62. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also

---

[19] *See* Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.

[20] *Id.; see also Healthcare Data Breach: What to Know About them and What to Do After One,* EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-toknow-about-them-and-what-to-do-after-one/ (last visited Nov. 1, 2024).

[21] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), 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.[22]

Defendant Failed to Comply with FTC Guidelines.

63. The 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. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the FTCA, 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

64. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer information 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. 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 into 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.

[22] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

65. The FTC further recommends that companies not maintain Private Information 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 the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

66. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data by 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 the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

67. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

68. Defendant was at all times fully aware of its obligation to protect the Private Information of consumers under the FTCA yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

69. Defendant recognizes these duties, declaring in its "Privacy Policy" that:

a. "It is the policy of the Gándara Center to keep all information regarding a person receiving services confidential, in compliance with all applicable state and federal laws and regulations."[23]

b. "Confidential information includes the person's name, social security number, address, date of birth, and any other data, which may identify them. Confidential information also pertains to Protected Health Information (PHI) as delineated in the Health Insurance Portability and Accountability Act (HIPAA) and 42CFR Part 2[.]"[24]

c. "Access to confidential client information, as defined and described in this Policy, is restricted to authorized agency personnel with a need to know such information in order to provide, supervise, or administer services to the client."[25]

d. "Authorized personnel are restricted from sharing any confidential information with non-authorized personnel."[26]

e. "All personnel have an affirmative responsibility to report any breach of confidentiality to his/her immediate supervisor."[27]

f. "Information may be shared among authorized personnel only as necessary to facilitate effective services. This includes the Case Records Review committee, in order to conduct case record audits and utilization reviews."[28]

---

[23] *Privacy Policy*, GÁNDARA CENTER, https://www.gandaracenter.org/privacy-policy (last visited Oct. 30, 2024).

[24] *Id*.

[25] *Id*.

[26] *Id*.

[27] *Id*.

[28] *Id*.

g. "Consultants, volunteers, interns, auditors, contractors, and other outside agents shall have access to confidential information only to the extent necessary to conduct authorized functions. Such individuals shall be required to sign an agreement stating they will treat the information in a confidential manner and not disclose such information to unauthorized individuals."[29]

h. "Confidential information may only be released under the following conditions . . . [t]he service recipient (or authorized parent/guardian) has consented in writing to the release of information to a specified person or agency."[30]

i. "All personnel are required to know and strictly follow all procedures involving the protection of client confidentiality."[31]

j. "The Compliance Officer or other designated individual shall provide an orientation to this Policy and Procedures and applicable state and federal laws and regulations to all incoming employees, volunteers, and contractors."[32]

k. "Annual in-service training shall be provided to all personnel on any change in laws and regulations."[33]

Defendant Failed to Comply with HIPAA Guidelines.

70. Defendant is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and

[29] *Id*.

[30] *Id*.

[31] *Id*.

[32] *Id*.

[33] *Id*.

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.

71. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

72. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

73. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

74. HIPAA requires "comply[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

75. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

76. HIPAA's Security Rule requires defendants to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

77. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

78. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); see also 42 U.S.C. §17902.

79. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

80. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. See 45 C.F.R. § 164.530(e).

81. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. See 45 C.F.R. § 164.530(f).

82. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material. The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.

83. Defendant was at all times fully aware of its HIPAA obligations to protect the Private Information of consumers yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

Defendant Failed to Comply with Industry Standards.

84. Experts studying cybersecurity routinely identify health care institutions like Defendant as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

85. Some industry best practices that should be implemented by institutions dealing with sensitive Private Information, like Defendant, include, but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

86. Other best cybersecurity practices that are standard at large institutions that store Private Information include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

87. 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.

88. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

Defendant Breached Its Duty to Safeguard Plaintiffs' and Class Members' Private Information.

89. In addition to its obligations under federal laws, Defendant owed duties to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members.

90. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data and failed to audit, monitor, or ensure the integrity of its data security practices. 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 that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect consumers' Private Information;

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

d. Failing to adhere to industry standards for cybersecurity as discussed above; and

e. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

91. Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems, which contained unsecured and unencrypted Private Information.

92. Had Defendant remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

Common Injuries & Damages

93. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual 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 (price premium damages); (d) diminution of value of their Private Information; (e) invasion of privacy; and (f) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

The Data Breach Increases Victims' Risk of Identity Theft.

94. Plaintiffs and Class Members are at a heightened risk of identity theft for years to come.

95. The unencrypted Private Information of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted Private

Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

96. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

97. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

98. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches can be the starting point for these additional targeted attacks on the victim.

99. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Full" packages.[34]

[34] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be

100. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

101. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

Loss of Time to Mitigate Risk of Identity Theft and Fraud

102. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports

made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm.

could expose the individual to greater financial harm—yet, the resource and asset of time has been lost.

103. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and re-securing their own computer networks; and checking their financial accounts and health insurance statements for any indication of fraudulent activity, which may take years to detect.

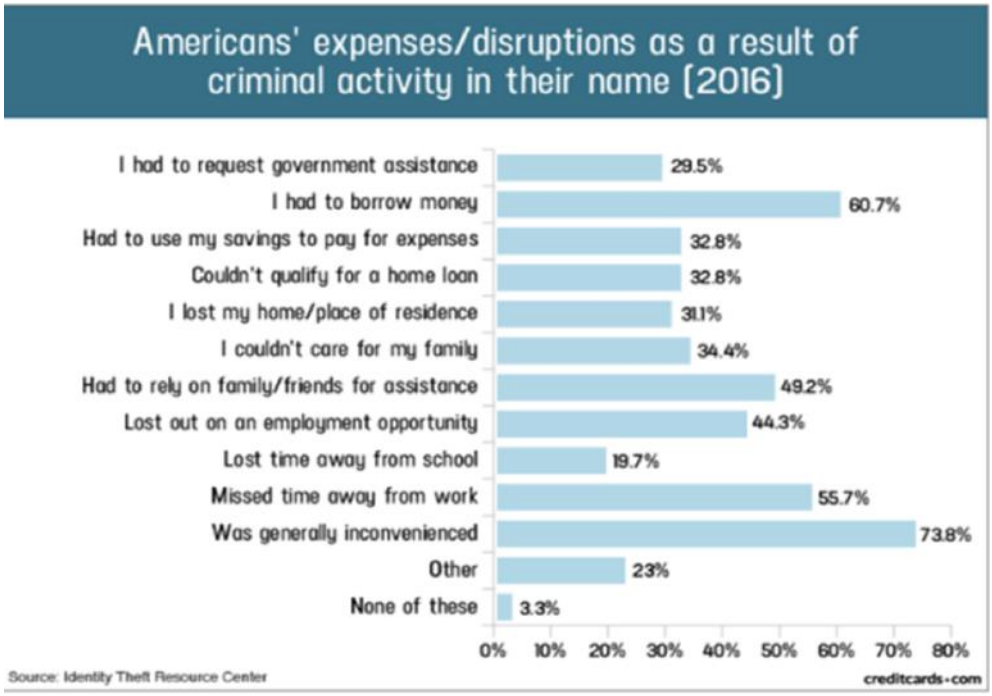
104. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[35]

105. These efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven 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.[36]

[35] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[36] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps.

106. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[37]



Diminution of Value of Private Information

107. PII and PHI are valuable property rights.[38] Their 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 a doubt that Private Information has considerable market value.

---

[37] Jason Steele, "Credit Card and ID Theft Statistics," Oct. 24, 2017, https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

[38] *See, e.g.*, Randall 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).

108. An active and robust legitimate marketplace for Private Information exists. In 2019, the data brokering industry was worth roughly $200 billion.[39]

109. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[40,41]

110. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[42]

111. Theft of PHI is also 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."

112. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

---

[39] https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

[40] https://datacoup.com/.

[41] https://digi.me/what-is-digime/.

[42] Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

113. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if their data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

114. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on its network, amounting to hundreds of thousands of individuals' detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

115. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

The Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary.

116. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes.

117. Such fraud may go undetected for years; consequently, Plaintiffs and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

118. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class

Members from the risk of identity theft that arose from the Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

Rhysida & the Dark Web.

119. Worryingly, the cybercriminals that obtained Plaintiffs' and Class Members' PII/PHI appear to be the notorious cybercriminal group "Rhysida."[43]

120. Rhysida is an especially notorious cybercriminal group. In fact, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) released a joint report warning the public about Rhysida.[44] Specifically, the joint "Cybersecurity Advisory" (CSA) stated, *inter alia*, that:

a. "Rhysida—an emerging ransomware variant—has predominately been deployed against the education, healthcare, manufacturing, information technology, and government sectors since May 2023."[45]

b. "Rhysida actors have been observed leveraging external-facing remote services to initially access and persist within a network."[46]

c. Remote services, such as virtual private networks (VPNs), allow users to connect to internal enterprise network resources from external locations. Rhysida actors have commonly been observed authenticating to internal VPN access points with

[43] *Rhysida Ransomware Group Targets Gándara Center in Major Healthcare Cyberattack*, HALCYON (July 17, 2024) https://ransomwareattacks.halcyon.ai/attacks/rhysida-ransomware-group-targets-gandara-center-in-major-healthcare-cyberattack.

[44] *#StopRansomware: Rhysida Ransomware*, FBI & CISA (Nov. 15, 2023) https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-319a.

[45] *Id*.

[46] *Id*.

compromised valid credentials, notably due to organizations lacking MFA enabled by default."[47]

d. "Rhysida actors . . . threaten[] to publish the sensitive exfiltrated data unless the ransom is paid."[48]

e. "Rhysida actors direct victims to send ransom payments in Bitcoin to cryptocurrency wallet addresses provided by the threat actors."[49]

121. Here, third party reports reveal that:

a. "The Rhysida ransomware group has claimed responsibility for a cyberattack on the Gándara Center."

b. "The attackers have listed the center on their dark web leak site, demanding a ransom of 10 Bitcoin, approximately $650,000, with a payment deadline set for July 25th, 2024."

c. "The attack has resulted in the encryption of critical data, and the group has threatened to publish the exfiltrated information unless the ransom is paid."

122. A screenshot of Rhysida's Dark Web webpage is reproduced below. Worryingly, the Dark Web webpage includes scans of sensitive letters, spreadsheets, and even a scan of a Massachusetts driver's license (these portions of the screenshot have been blurred to protect victims' privacy).[50]

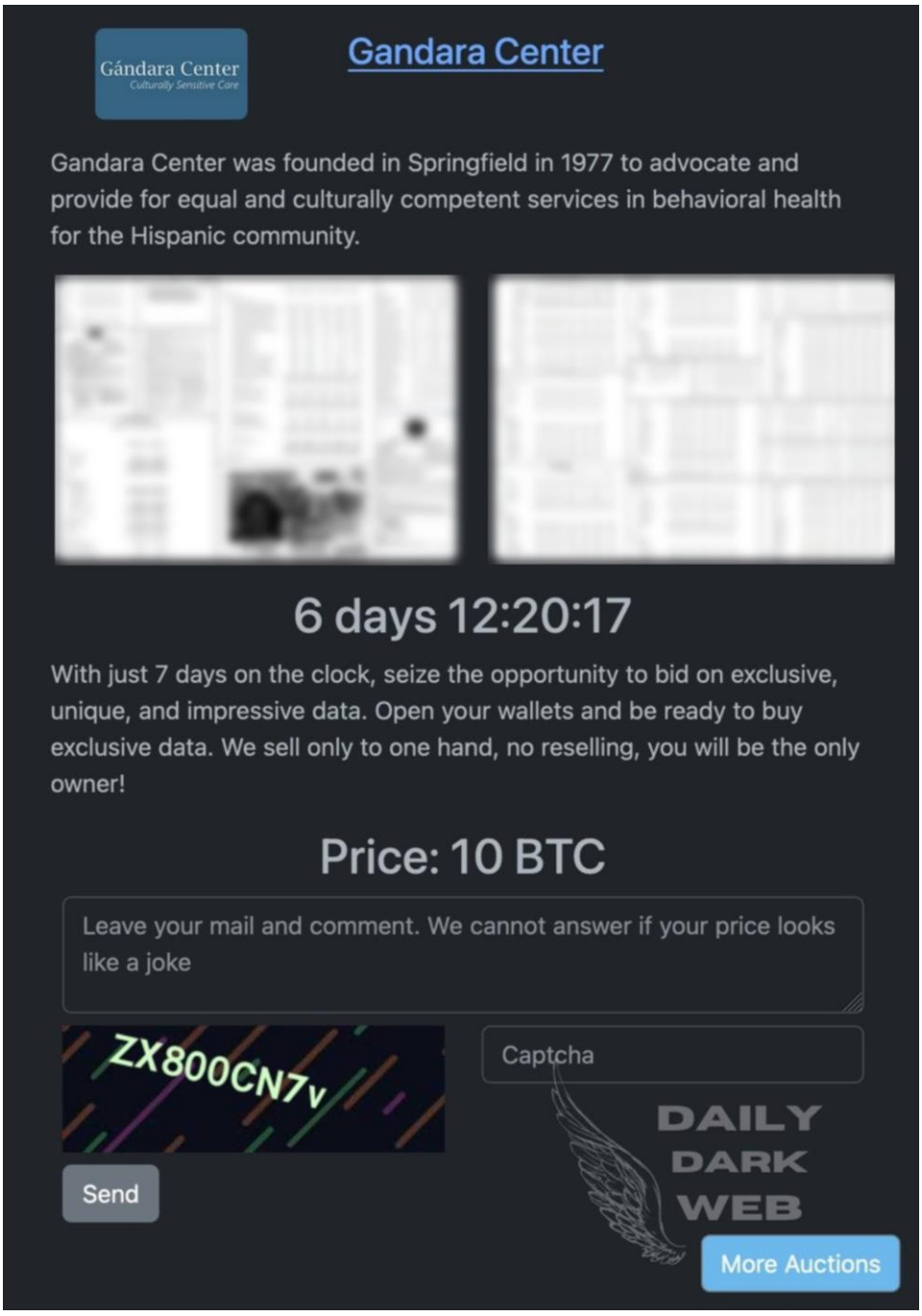
---

[47] *Id*.

[48] *Id*.

[49] *Id*.

[50] Dark Web Intelligence (@DailyDarkWeb), X (3:33 AM · Jul 18, 2024) https://x.com/DailyDarkWeb/status/1813854612547670478.



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

124. Still, despite this public evidence of broad misuse, Defendant misleadingly claims that "Gándara is not aware of any evidence of the misuse of any information potentially involved in this incident."[51]

Plaintiff Eugene Mitchell's Experience

125. Plaintiff provided his Private Information to Defendant in connection with his employment from about 2017 through March 2024.

126. At the time of the Data Breach, Defendant retained Plaintiff's Private Information in its system.

127. Plaintiff received a Notice Letter dated October 24, 2024, from Defendant informing him that his Private Information was included in the Data Breach.[52]

128. Plaintiff's Private Information was compromised in the Data Breach and stolen by cybercriminals who illegally accessed Defendant's network for the specific purpose of targeting the Private Information.

129. Plaintiff takes reasonable measures to protect his Private Information. He has never knowingly transmitted unencrypted Private Information over the internet or other unsecured source.

130. Plaintiff stores any documents containing his Private Information in a safe and secure location and diligently chooses unique usernames and passwords for his online accounts.

131. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. He

[51] *Notice of Data Security Incident*, GÁNDARA CENTER, https://www.gandaracenter.org/general-4 (last visited Oct. 30, 2024).

[52] Ex. A.

monitors accounts and credit scores and has sustained emotional distress. This is time that was lost and unproductive and took away from other activities and work duties.

132. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that he entrusted to Defendant for the purpose of obtaining services from Defendant, which was compromised in and as a result of the Data Breach.

133. Plaintiff suffered lost time, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

134. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Private Information, especially his name, Social Security number, and PHI, being placed in the hands of criminals.

135. Defendant obtained and continues to maintain Plaintiff's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff's Private Information was compromised and disclosed as a result of the Data Breach.

136. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Wanda Delrio's Experience

137. Plaintiff used Defendant's healthcare services, requiring her to provide her Private Information to Defendant.

138. At the time of the Data Breach, Defendant retained Plaintiff's Private Information in its system.

139. Plaintiff received a Notice Letter dated October 24, 2024, from Defendant informing her that her Private Information was included in the Data Breach.

140. Plaintiff's Private Information was compromised in the Data Breach and stolen by cybercriminals who illegally accessed Defendant's network for the specific purpose of targeting the Private Information.

141. Plaintiff takes reasonable measures to protect her Private Information. She has never knowingly transmitted unencrypted Private Information over the internet or other unsecured source.

142. Plaintiff stores any documents containing her Private Information in a safe and secure location and diligently chooses unique usernames and passwords for her online accounts.

143. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. She monitors accounts and credit scores and has sustained emotional distress. This is time that was lost and unproductive and took away from other activities and work duties.

144. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that he entrusted to Defendant for the purpose of obtaining services from Defendant, which was compromised in and as a result of the Data Breach.

145. Plaintiff suffered lost time, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

146. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information, especially her name, Social Security number, and PHI, being placed in the hands of criminals.

147. Defendant obtained and continues to maintain Plaintiff's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff's Private Information was compromised and disclosed as a result of the Data Breach.

148. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Raffaele Santaniello's Experience

149. Plaintiff Raffaele Santaniello is a former patient of Defendant and thus provided his Private Information to Defendant.

150. At the time of the Data Breach, Defendant retained Plaintiff's Private Information in its system.

151. Plaintiff received a Notice Letter dated October 24, 2024, from Defendant informing him that his Private Information was included in the Data Breach.

152. Plaintiff's Private Information was compromised in the Data Breach and stolen by cybercriminals who illegally accessed Defendant's network for the specific purpose of targeting the Private Information.

153. Plaintiff reasonably understood that a portion of the funds paid to Defendant would be used to pay for adequate cybersecurity and protection of Private Information.

154. Plaintiff takes reasonable measures to protect his Private Information. He has never knowingly transmitted unencrypted Private Information over the internet or other unsecured source.

155. Plaintiff stores any documents containing his Private Information in a safe and secure location and diligently chooses unique usernames and passwords for his online accounts.

156. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. He monitors accounts and credit scores and has sustained emotional distress. This is time that was lost and unproductive and took away from other activities and work duties.

157. In fact, Plaintiff ***already suffered*** from identity theft and fraud in the aftermath of the Data Breach, including:

a. a fraudulent charge on his PayPal Mastercard on December 4, 2024, totaling $63.38 for "STEAMGAMES;"

b. a fraudulent charge on his PayPal account on December 4, 2024, totaling $149.00 for "TOPSTEPTRADE;" and

c. a fraudulent charge on his PayPal account on December 4, 2024, totaling $121.99 for "SP AVOXZ."

158. Additionally, in the months after the Data Breach, Plaintiff's credit score decreased by approximately 100 points. This is a substantial injury because Plaintiff intends to purchase a house within the next year or two.

159. And in the aftermath of the Data Breach, Plaintiff has suffered from a spike in spam and scam emails, text messages and phone calls.

160. Plaintiff does not recall ever learning that his information was compromised in a data breach incident—other than the breach at issue here.

161. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that he entrusted to Defendant for the purpose of obtaining services from Defendant, which was compromised in and as a result of the Data Breach.

162. Plaintiff suffered lost time, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

163. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Private Information, especially his name, Social Security number, and PHI, being placed in the hands of criminals.

164. Defendant obtained and continues to maintain Plaintiff's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff's Private Information was compromised and disclosed as a result of the Data Breach.

165. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

CLASS ALLEGATIONS

166. Pursuant to Rule 23 of the Massachusetts Rules of Civil Procedure, Plaintiffs bring this action on behalf of themselves and on behalf of all members of the proposed class defined as:

All individuals residing in the United States whose Private Information was compromised in the Data Breach ("Class").

167. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

168. Plaintiffs reserve the right to amend the definition of the proposed Class or to add a subclass before the Court determines whether certification is appropriate.

169. The proposed Class meets the criteria for certification under Massachusetts Rule of Civil Procedure 23.

170. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiffs believes the proposed Class includes at least tens of thousands of individuals who have been damaged by Defendant's conduct as alleged herein. The precise number of Class Members is unknown to Plaintiffs but may be ascertained from Defendant's records.

171. 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:

d. Whether Defendant engaged in the conduct alleged herein;

e. Whether Defendant's conduct violated the FTCA;

f. When Defendant learned of the Data Breach;

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

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

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

j. Whether Defendant owed duties to Class Members to safeguard their PII;

k. Whether Defendant breached their duties to Class Members to safeguard their PII;

l. Whether hackers obtained Class Members' PII via the Data Breach;

m. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

n. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

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

p. What damages Plaintiffs and Class Members suffered as a result of Defendant's misconduct;

q. Whether Defendant's conduct was negligent;

r. Whether Defendant breached contracts it had with its patients, including Plaintiffs and Class Members;

s. Whether Defendant were unjustly enriched;

t. Whether Plaintiffs and Class Members are entitled to damages;

u. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

v. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

172. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendant. Plaintiffs is advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

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

174. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members. For example, all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated 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.

175. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. 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, conducting 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.

176. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach.

CLAIMS FOR RELIEF

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

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

178. Defendant's patients, including Plaintiffs and Class Members, provided their non-public Private Information to Defendant as a condition of obtaining services.

179. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information were wrongfully disclosed.

180. By assuming the responsibility to collect and store this data, Defendant had duties of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

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

182. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and Class Members of the Data Breach.

183. Defendant had and continues to have duties to adequately disclose that the Private Information of Plaintiffs and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice is necessary to allow Plaintiffs and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

184. Defendant breached its duties, and thus was 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 its networks and systems;

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

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

e. Failing to remove Plaintiffs' and Class Members' Private Information it was no longer required to retain pursuant to regulations; and

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so they could take appropriate steps to mitigate the potential for identity theft and other damages.

185. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and Class Members.

186. Defendant has admitted that the Private Information of Plaintiffs and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

187. But for Defendant's wrongful and negligent breaches of duties owed to Plaintiffs and Class Members, the Private Information of Plaintiffs and Class Members would not have been compromised.

188. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and Class Members and the harm, or risk of imminent harm, suffered by Plaintiffs and Class Members. The Private Information of Plaintiffs and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

189. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) an increase in spam calls, texts, and/or emails; and (vi) the continued and certainly

increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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.

190. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

191. Additionally, as a direct and proximate result of Defendant's negligence , Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

192. Plaintiffs and Class Members are therefore entitled to damages, including restitution and unjust enrichment, declaratory and injunctive relief, and attorneys' fees, costs, and expenses.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

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

194. Plaintiffs and Class Members were required to deliver their Private Information to Defendant as part of the process of obtaining health care services provided by Defendant. Plaintiffs and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for health care services.

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

196. Defendant accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services to Plaintiffs and Class Members.

197. Plaintiffs and Class Members entrusted their Private Information to Defendant. In so doing, Plaintiffs and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

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

199. Implicit in the agreement between Plaintiffs and Class Members and Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses, and (f) retain the Private Information only under conditions that kept such information secure and confidential.

200. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

201. On information and belief, at all relevant times, Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

202. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiffs' and Class Members' Private Information would remain protected.

203. Plaintiffs and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

204. Plaintiffs 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.

205. Plaintiffs 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.

206. Massachusetts law provides that every contract includes good faith and fair dealing between the parties involved.

207. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

208. Defendant breached the implied contracts it made with Plaintiffs and the Class by failing to safeguard and protect their Private Information, by failing to delete the information of

Plaintiffs and the Class once the relationship ended, and by failing to provide accurate notice to them that Private Information was compromised as a result of the Data Breach

209. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Private Information, failing to timely and accurately disclose the Data Breach to Plaintiffs and Class Members and continued acceptance of Private Information and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

210. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiffs and Class Members sustained damages, including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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.

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

212. Plaintiffs 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.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

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

214. This count is brought in the alternative to Plaintiffs' breach of implied contract claim (Count II).

215. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including from payments made by and/or on behalf of its patients, including Plaintiffs and Class Members, in exchange for health care services, for which Defendant collected and maintained Plaintiffs' and Class Members' Private Information.

216. As such, a portion of the value and monies derived from Plaintiffs and 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.

217. Plaintiffs and Class Members conferred a monetary benefit on Defendant, in providing it with their valuable Private Information.

218. Defendant knew that Plaintiffs and Class Members conferred a benefit upon it and accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendant profited from Plaintiffs' and Class Members' retained data and used Plaintiffs' and Class Members' Private Information for business purposes.

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

220. Under the principles of equity and good conscience, Defendant should not be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon it.

221. Plaintiffs and Class Members have no adequate remedy at law.

222. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) an increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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.

223. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by

establishing a constructive trust from which Plaintiffs and Class Members may seek restitution or compensation.

COUNT IV
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Class)

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

225. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

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

227. Defendant breached its respective duties to Plaintiffs and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Private Information.

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

229. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and members of the Class.

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

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

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

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

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

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

COUNT V
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

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

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

238. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of Defendant's relationship with them—especially to secure their Private Information.

239. Because of the highly sensitive nature of the Private Information, Plaintiffs and Class Members would not have entrusted Defendant, or anyone in Defendant's position, to retain their Private Information had they known the reality of Defendant's inadequate data security practices.

240. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiffs' and Class Members' Private Information.

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

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

PRAYER FOR RELIEF

WHEREFORE**,** Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class, pursuant to Federal Rule of Civil Procedure 23;

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

C. For injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the Private Information of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures; requiring Defendant to segment data by, among other things, creating firewalls and access

controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and securing checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats,

both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvi. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of actual damages, compensatory damages, and nominal damages, in an amount to be determined, and for punitive damages, as allowable by law;

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

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

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

DEMAND FOR JURY TRIAL

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

Date: January 22, 2025

Respectfully submitted,

/s/ Christina Xenides

Christina Xenides (BBO #677603)
SIRI & GLIMSTAD LLP
1005 Congress Avenue, Suite 925-C36
Austin, TX 78701
Telephone: (512) 265-5622
Email: cxenides@sirillp.com

Jeff Ostrow*
Kenneth Grunfeld*
KOPELOWITZ OSTROW P.A.
1 W. Las Olas Blvd., Ste. 500
Fort Lauderdale, FL 33301
Telephone: (954) 525-4100
Email: ostrow@kolawyers.com

Samuel J. Strauss*
Raina C. Borrelli*
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
Telephone: (872) 263-1100
Fax: (872) 263-1109
Email: sam@straussborrelli.com
Email: raina@straussborrelli.com

Leigh S. Montgomery*
Texas Bar No. 24052214
EKSM, LLP
1105 Milford Street
Houston, Texas 77006
Telephone: (888) 350-3931
Fax: (888) 276-3455
Email: lmontgomery@eksm.com

**Pro hac vice forthcoming*

Counsel for Plaintiffs and the Putative Class