Electronically FILED by Superior Court of California, County of Riverside on 01/10/2025 11:42 AM
Case Number CVRI2500186 0000116389269 - Jason B. Galkin, Executive Officer/Clerk of the Court By Kristen King, Clerk

KOPELOWITZ OSTROW P.A.
Kristen Lake Cardoso (CA Bar No. 338762)
cardoso@kolawyers.com
Kenneth J. Grunfeld (*pro hac vice* forthcoming)
grunfeld@kolawyers.com
One West Las Olas, Suite 500
Fort Lauderdale, FL 33301
Telephone: (954) 525-4100

Counsel for Plaintiff and the Proposed Class

SUPERIOR COURT OF THE STATE OF CALIFORNIA
FOR THE COUNTY OF RIVERSIDE

DONALD CROSSLIN, individually and on behalf of all others similarly situated,

Plaintiff,

v.

DAP HEALTH, INC.,

Defendant.

Case No. CVRI2500186

CLASS ACTION

CLASS ACTION COMPLAINT FOR DAMAGES

1. **Negligence/Negligence *Per Se***
2. **Breach of Implied Contract**
3. **Invasion of Privacy**
4. **Violation of the California Confidentiality of Medical Information Act (Cal. Civ. Code §§ 56.36 *et seq.*)**
5. **Unjust Enrichment**

DEMAND FOR JURY TRIAL

Plaintiff Donald Crosslin ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), brings this action against Defendant DAP Health, Inc. ("Defendant"), alleging as follows upon Plaintiff's personal knowledge, information and belief, and investigation of counsel.

I. INTRODUCTION

1. This action arises from Defendant's failure to properly secure and safeguard Plaintiff's and approximately 129,048 Class Members' sensitive protected health information ("PHI") and personal identifying information[1] ("PII"), which as a result, is now in criminal cyberthieves' possession.

2. In July 2024, criminal hackers accessed Defendant's email server and stole emails and files containing Plaintiff's and Class Members' most private, confidential PII and PHI, including their names, Social Security numbers, addresses, dates of birth, phone numbers, driver's license numbers, passport numbers, birth certificate numbers, vehicle license plate and VIN numbers, financial account numbers, Medicare/Medicaid numbers, health insurance plan and policy numbers, medical diagnoses, medical procedures and treatments, procedure/treatment dates and locations, treatment costs, laboratory test results and images, vital signs records, medical histories, allergies, prescription drugs taken and written, medical provider names, and other sensitive data (collectively, "Private Information"), causing widespread injuries to Plaintiff and Class Members (the "Data Breach").

3. Defendant operates a network of health centers located throughout Riverside and San Diego counties, furnishing services including "dentistry; family medicine; gender-affirming care; HIV prevention, testing, and treatment (free); infectious diseases care; LGBTQ+ care; mental health care; outpatient substance use disorder

[1] The Federal Trade Commission ("FTC") defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth. . . .." 17 C.F.R. § 248.201(b)(8).

treatment and recovery services; pediatrics; pharmacy services; primary care; radiology; urgent care; and women's health (including OB-GYN)," as well as social service programs like housing and food assistance.[2]

4. Plaintiff and Class Members are current and former patients of Defendant who, as a condition and in exchange for receiving healthcare services from Defendant, were required to and did entrust Defendant with their confidential, non-public Private Information. Defendant collected, used, and maintained Plaintiff's and Class Members' Private Information to facilitate its operations, including providing and billing for its services, and stored and transmitted this Private Information on its email accounts and servers.

5. Healthcare providers like Defendant that handle patients' Private Information (especially the particularly sensitive PII and PHI involved in this Data Breach) owe the individuals to whom that information relates a duty to adopt reasonable measures to protect it from disclosure to unauthorized third parties, and to keep it safe and confidential. This duty arises under contract, statutory and common law, federal and state law and regulation, industry standards, and representations made to Plaintiff and Class Members, and because it is foreseeable that the exposure of Private Information to unauthorized persons—especially hackers with nefarious intentions—will harm the affected individuals, including but not limited to the invasion of their private financial matters.

6. Defendant breached its duties owed to Plaintiff and Class Members by failing to safeguard the Private Information it collected from them and maintained, including by failing to implement industry standards for data security to protect the sensitive data against cyberattacks, which allowed cybercriminals to access and exfiltrate over 100,000 individuals' Private Information from Defendant's care.

[2] *See About DAP Health*, DAP Health, https://www.daphealth.org/about-us/ (last visited Jan. 8, 2025).

7. According to Defendant's website notice about the Data Breach,[3] on July 22, 2024, Defendant "detected suspicious activity in its email environment," and ultimately determined that criminal hackers accessed and acquired files and data stored thereon.

8. The Private Information compromised in the Data Breach includes the following categories of PII and PHI of Defendant's current and former patients:

> Name, Address; Phone; Date of Birth; SSN; Patient ID; Medical Records Number; Medical Treatment Location; Medicare/Medicaid Number; Health Insurance Plan/Policy Number; Cost of Medical Treatment/Insurance; Diagnosis/Treatment/Procedure; Medical History / Allergies; Prescription Drugs Taken / Written; Test Results / Images / Vital Signs; Date of Admission/ Treatment; Healthcare Provider Name; Financial Account Number; User ID & Password; License Plate / VIN Vehicle ID; Driver's License Number; Passport Number; and Birth Certificate Number.[4]

9. Upon information and belief, the mechanism of the cyberattack and the potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus, Defendant knew failing to take reasonable steps to secure the Private Information left it in a dangerous condition.

10. Despite knowing the risks, Defendant failed to adequately protect Plaintiff's and Class Members' Private Information—and failed to even encrypt or redact this highly sensitive data when storing and transmitting it on its internet-facing email server. This unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect Plaintiff's and Class Members' sensitive data.

11. Defendant breached its duties and obligations by failing in one or more of the following ways: (a) to design, implement, monitor, and maintain reasonable network and account safeguards against foreseeable threats; (b) to design, implement, and maintain reasonable data retention policies; (c) to adequately train or oversee staff and service providers regarding data security; (d) to comply with industry-standard data security

[3] *Notice of Data Privacy Event*, DAP Health, https://www.daphealth.org/hipaa-substitute-notice/ (last visited Jan. 8, 2025).
[4] *Id.*

practices; (e) to warn Plaintiff and Class Members of Defendant's inadequate data security practices; (f) to encrypt or adequately encrypt the Private Information it collected, transmitted, and stored; (g) to require access controls like multifactor authentication ("MFA") or limitations on employees with access to Private Information; (h) to use reasonable logging, monitoring, and alerting tools to recognize or detect that its email server had been compromised and accessed in a timely manner to mitigate the harm; (i) to utilize widely available software able to detect and prevent this type of attack; and (j) to otherwise secure the Private Information using reasonable and effective data security procedures free of foreseeable vulnerabilities and breaches.

12. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality and security of their Private Information. In entrusting their Private Information to Defendant, Plaintiff and Class Members reasonably expected this sophisticated business entity to keep their Private Information confidential and security maintained, to use it only for legitimate healthcare purposes, and to disclose it only as authorized. Defendant failed to do so, causing the unauthorized disclosure of Plaintiff's and Class Members' Private Information in the Data Breach.

13. Criminal hackers targeted and obtained Plaintiff's and Class Members' Private Information from Defendant because of the data's value in exploiting and stealing Plaintiff's and Class Members' identities. As a direct and proximate result of Defendant's inadequate data security and breaches of duties to handle Private Information with reasonable care, Plaintiff's and Class Members' Private Information was accessed by cybercriminals and exposed to an untold number of unauthorized individuals with malicious intentions. The present and continuing risk to Plaintiff and Class Members as victims of the Data Breach will remain for their respective lifetimes.

14. The harm resulting from a cyberattack like this Data Breach manifests in numerous ways including identity theft and financial fraud, and the exposure of an individual's Private Information due to breach ensures that he or she will be at a

substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for a lifetime. Mitigating that risk, to the extent even possible, requires individuals to devote significant time and money to closely monitor their credit, financial accounts, and email accounts, and to take several additional prophylactic measures.

15. The risk of identity theft caused by this Data Breach is impending and has materialized, as Plaintiff's and Class Members' Private Information was targeted, accessed, and misused by criminal hackers.

16. As a result of Defendant's deficient cybersecurity and the consequential Data Breach, Plaintiff and Class Members have suffered and will continue to suffer concrete injuries in fact including, *inter alia*, (a) actual and/or materialized and imminent risk of identity theft and fraud; (b) financial costs incurred due to actual identity theft; (c) lost time and productivity dealing with actual identity theft; (d) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (e) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (f) deprivation of value of their Private Information; (g) loss of privacy; (h) emotional distress including anxiety and stress in with dealing with the Data Breach; (i) loss of the benefit of the bargain with Defendant; and (j) the continued risk to their sensitive Private Information, which remains in Defendant's possession and subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect the confidential data it collects and maintains.

17. To recover for these harms, Plaintiffs, individually and on behalf of the Classes as defined herein, brings claims for negligence/negligence *per se*, breach of contract, invasion of privacy/intrusion upon seclusion, violation of the California Confidentiality of Medical Information Act, and unjust enrichment to address Defendant's inadequate safeguarding of Plaintiff's and Class Members' sensitive Private Information.

18. Plaintiff, individually and on behalf of putative Class Members, seeks compensatory, consequential, nominal, statutory, and punitive damages, attorney's fees and costs, declaratory judgment, and injunctive relief requiring Defendant to (a) disclose, expeditiously, the full nature of the Data Breach and the types of Private Information exposed; (b) implement improved data security practices to reasonably guard against future breaches of Private Information in Defendant's possession; and (c) provide, at Defendant's own expense, all impacted Data Breach victims with lifetime credit monitoring and identity theft protection services.

II. PARTIES

19. Plaintiff Donald Crosslin is a citizen and resident of Riverside County, California.

20. Defendant DAP Health, Inc. is a California nonprofit corporation with its principal place of business at 1695 N Sunrise Way, Palm Springs, CA 92262.

III. JURISDICTION AND VENUE

21. This Court has jurisdiction over this controversy pursuant to California Code of Civil Procedure § 410.10. The total amount of damages incurred by Plaintiff and the Class in the aggregate exceeds the $25,000 jurisdictional minimum of this Court. Further, the amount in controversy as to Plaintiff individually does not exceed $75,000.

22. This Court has jurisdiction over Defendant because it is located within Riverside County, California.

23. Venue is proper in this Court under California Business and Professional Code § 17203 and Code of Civil Procedure §§ 395(a) and 395.5 because Defendant is headquartered within this Court's jurisdiction and because a substantial part of the events giving rise to Plaintiff's claims occurred in this county.

IV. FACTUAL ALLEGATIONS

A. Defendant Collects and Maintains Private Information and Promises to Protect It.

24. Defendant is a healthcare provider that operates a network of 26 health centers throughout Riverside and San Diego counties, furnishing services including "dentistry; family medicine; gender-affirming care; HIV prevention, testing, and treatment (free); infectious diseases care; LGBTQ+ care; mental health care; outpatient substance use disorder treatment and recovery services; pediatrics; pharmacy services; primary care; radiology; urgent care; and women's health (including OB-GYN)," as well as social service programs like housing and food assistance.[5]

25. To facilitate Defendant's operational and financial functions, including marketing, fundraising, and providing and billing for healthcare services, Defendant collects and maintains its patients' Private Information.

26. Plaintiff and Class Members are current and former patients of Defendant who, as a condition of and in exchange for receiving services from Defendant, were required to entrust Defendant with their personal and confidential Private Information.

27. Defendant derived economic benefits from collecting Plaintiff's and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform its income-generating operations, including providing and billing for services.

28. Additionally, Defendant benefits from Plaintiff's and Class Members' Private Information by using it for marketing and fundraising purposes.

29. At all relevant times, Defendant knew it was using its email server to store and transmit Plaintiff's and Class Members' valuable, sensitive Private Information and that as a result, its email environment would be attractive targets for cybercriminals.

30. Defendant also knew that any breach of its email servers and systems and exposure of the data stored therein would result in the increased risk of identity theft and fraud for the hundreds of thousands of individuals whose Private Information was compromised, as well as intrusion into those individuals' private health and financial

[5] *See About DAP Health*, DAP Health, https://www.daphealth.org/about-us/ (last visited Jan. 8, 2025).

matters.

31. In exchange for receiving Plaintiff's and Class Members' Private Information, Defendant promised to safeguard the sensitive, confidential data and to only use it for authorized and legitimate purposes.

32. Defendant made promises and representations to its patients, including Plaintiff and Class Members, that the Private Information it collected from them would be kept safe and confidential, the information's privacy would be maintained, and Defendant would delete any sensitive information after it was no longer required to maintain it.

33. Indeed, Defendant's *Summary of Notice Privacy Practice*, published on its website and, on information and belief provided to all patients receiving services from Defendant, acknowledges and promises,

> **We are required by law to maintain the privacy and security of your protected health information.**
>
> - We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
> - We will not use or share your information other than as described here unless you tell us we can in writing. . . .
> - We must follow the duties and privacy practices described in this notice and give you a copy of it.[6]

34. Defendant's *Patient/Client's Bill of Rights*, published on its website and, on information and belief provided to all patients receiving services from Defendant, further promises and warrants to patients,

> **YOU HAVE A RIGHT TO**
>
> **Respect and Privacy**
> Be treated in a respectful manner that honors your dignity and privacy. . . .
>
> **Confidentiality**

[6] *Summary of Notice Privacy Practice*, DAP Health, https://www.daphealth.org/about-us/client-privacy/ (last visited Jan. 8, 2025).

> Have your personal health information kept confidential as protected under state and federal laws.[7]

35. Defendant's promises to adequately maintain and protect Plaintiff's and Class Members' Private Information demonstrates its understanding that such data's confidentiality and integrity is critical.

36. Healthcare patients in general value the confidentiality of their Private Information and demand security to safeguard it. For their part, Plaintiff and Class Members have taken reasonable steps to maintain their Private Information in confidence.

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

38. Plaintiff and Class Members relied on Defendant's promises and sophistication to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information.

39. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of its promises to safeguard that information, including in the manners set forth in Defendant's *Summary Notice of Privacy Practices* and *Patient/Client's Bill of Rights*.

40. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties to Plaintiff and Class Members, and knew or should have known that it was responsible for protecting their Private Information from unauthorized disclosure. Defendant failed to do so, causing this Data Breach.

[7] *Patient/Client's Bill of Rights*, DAP Health (April 24, 2015), available at https://www.daphealth.org/clients-bill-of-rights/ (last visited Jan. 8, 2025).

B. Defendant Failed to Adequately Safeguard Plaintiff's and Class Members' Private Information, causing the Data Breach.

41. On or about December 26, 2024, Defendant began sending Plaintiff and other Data Breach victims letters titled *Notice of Data Breach* ("Notice Letters").

42. Plaintiff's Notice Letter informs as follows:

> **What Happened?**
>
> On July 22, 2024, DAP Health detected suspicious activity in its email environment. Upon discovery of this event, DAP Health promptly engaged a specialized third-party cybersecurity firm and IT personnel to assist with securing the environment, as well as, to conduct a comprehensive forensic investigation to determine the nature and scope of the event. As a result of the investigation, DAP Health learned that an unauthorized actor accessed and/or acquired certain files and data stored within its email environment. . . .
>
> **What Information Was Involved?**
>
> As part of its normal business operations, DAP Health collected certain information from its employees, patients, and clients. To that end, and as a result of DAP Health's investigation, DAP Health determined that the information related to you that may have been acquired without authorization as a result of the event consists of your: Name, Phone, Date of Birth, Patient ID, Medical Records Number, Medical Treatment Location, Diagnosis/Treatment/Procedure, Test Results / Images / Vital Signs, Date of Admission/ Treatment, Healthcare Provider Name.

43. Omitted from the Notice Letters are crucial details like the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information is protected.

44. Thus, Defendant's purported disclosure amounts to no real disclosure at all, as it fails to inform Plaintiff and Class Members of the Data Breach's critical facts with any degree of specificity. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach was and is severely diminished.

45. Upon information and belief, the hackers behind the Data Breach first

breached Defendant's email server using common and rudimentary initial access techniques that Defendant knew or should have known were necessary to protect against.

46. Defendant could have prevented this Data Breach by properly securing and encrypting the files and email servers containing Plaintiff's and Class Members' Private Information, using controls like limitations on personnel with access to sensitive data and requiring MFA for account access, training its employees on standard cybersecurity practices like anti-phishing techniques, and implementing reasonable logging and alerting methods to detect unauthorized access promptly.

47. For example, if Defendant had implemented industry standard logging, monitoring, and alerting systems—basic technical safeguards that any PHI and/or PII-collecting company is expected to employ—then cybercriminals would not have been able to perpetrate prolonged malicious activity in Defendant's email systems without alarm bells going off, including the reconnaissance necessary to identify where Defendant stored Private Information, installation of malware or other methods of establishing persistence and creating a path to exfiltrate data, staging data in preparation for exfiltration, and then exfiltrating that data outside of Defendant's email environment without being caught or stopped until the damage was done.

48. Defendant would have recognized the malicious activities detailed in the preceding paragraph if it bothered to implement basic monitoring and detection systems, which then would have stopped the Data Breach or greatly reduced its impact.

49. Defendant did not use reasonable security procedures and practices appropriate to the sensitive and confidential nature of Plaintiff's and Class Members' Private Information it collected and maintained, such as encrypting files containing Private Information or deleting Private Information from email servers when it is no longer needed, which caused that Private Information's unauthorized access and exfiltration in the Data Breach.

50. To mitigate cyber threats from ransomware groups like the cybercriminals

behind this Data Breach, the Joint Cybersecurity and Infrastructure Security Agency ("CISA") recommends rudimentary actions that businesses like Defendant should take immediately: (a) installing updates for operating systems, software, and firmware as soon as they are released; (b) requiring phishing-resistant MFA (i.e., non-SMS text based) for as many services as possible; and (c) training users to recognize and report phishing attempts.[8]

51. Upon information and belief, Defendant failed to install updates for operating systems, software, and firmware as soon as they were released. Had Defendant installed such updates at its first opportunity as was standard and advised, the Data Breach would not have occurred, or would have at least been mitigated.

52. Further, upon information and belief, Defendant failed to require phishing-resistant MFA where possible or adequately train its employees to recognize and report phishing attempts. Had Defendant required phishing-resistant MFA, and/or trained its employees on reasonable and basic cybersecurity topics like common phishing techniques or indicators of a potentially malicious event, cybercriminals would not have been able to carry out the Data Breach through phishing.

53. As a result of Defendant's failures, Plaintiff's and Class Members' Private Information was stolen in the Data Breach when cybercriminals accessed and acquired files in Defendant's email systems containing that sensitive data in unencrypted form.

54. Defendant's tortious conduct and breach of contractual obligations, as detailed herein, are evidenced by its failure to recognize the Data Breach until cybercriminals had already accessed Plaintiff's and Class Members' Private Information and taken it from Defendant's email environment, meaning Defendant had no effective means in place to detect and prevent attempted cyberattacks.

C. Defendant Knew or Should Have Known of the Risk of a Cyber Attack Because Healthcare Providers in Possession of Private Information are Particularly

[8] *#StopRansomware Guide*, CISA (Oct. 2023), available at https://www.cisa.gov/sites/default/files/2023-10/StopRansomware-Guide-508C-v3_1.pdf (last visited Oct. 24, 2024).

Suspectable.

55. Defendant's negligence, including its gross negligence, in failing to safeguard Plaintiff's and Class Members' Private Information is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

56. Private Information of the kind accessed in the Data Breach is of great value to cybercriminals as it can be used for a variety of unlawful and nefarious purposes, including ransomware, fraudulent misuse, and sale on the internet black market known as the dark web.

57. Private Information can also be used to distinguish, identify, or trace an individual's identity, such as his or her name, Social Security number, and financial records. This may be accomplished alone, or in combination with other personal or identifying information connected or linked to an individual such as his or her birthdate, birthplace, and mother's maiden name.

58. Data thieves regularly target entities that store Private Information like Defendant due to the highly sensitive information they maintain. Defendant knew and understood that Plaintiff's and Class Members' Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize it through unauthorized access.

59. According to the Identity Theft Resource Center's report covering the year 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data events that involved sensitive information (Ex: Social Security numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)."[9]

60. The increase in such attacks, and attendant risk of future attacks, was widely

[9] *See* Identity Theft Res. Ctr., *2021 Annual Data Breach Report Sets New Record for Number of Compromises*, ITRC (Jan. 24, 2022), https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises.

known to the public and to anyone in Defendant's industry, including Defendant itself. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[10]

61. Defendant's data security obligations were particularly important given the substantial increase, preceding the date of the subject Data Breach, in cyberattacks and/or data breaches targeting entities like Defendant that collect and store PHI.

62. In 2023, an all-time high for data compromises occurred, with 3,205 compromises affecting 353,027,892 total victims. Of the 3,205 recorded data compromises, 809 of them, or 25.2% were in the medical or healthcare industry. The estimated number of organizations impacted by data compromises has increased by +2,600 percentage points since 2018, and the estimated number of victims has increased by +1400 percentage points. The 2023 compromises represent a 78 percentage point increase over the previous year and a 72 percentage point hike from the previous all-time high number of compromises (1,860) set in 2021.

63. Additionally, as companies became more dependent on computer systems to run their business,[11] e.g., working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[12]

64. Entities with custody of PHI, like Defendants, reported the largest number of data breaches among all measured sectors in 2022, with the highest rate of exposure per breach.[13] Indeed, when compromised, healthcare related data is among the most sensitive

---

[10] IBM, *Cost of a data breach 2022: A million-dollar race to detect and respond*, https://www.ibm.com/reports/data-breach (last accessed Oct. 10, 2024).

[11] Bd. Governors of the Fed. Res. Sys., *FEDS Notes* (May 12, 2022), https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html.

[12] Suleyman Ozarslan, *Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022* (Mar. 24, 2022), https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022.

[13] *See* Identity Theft Res. Ctr., *2022 Annual Data Breach Report*, https://www.idtheftcenter.org/publication/2022-data-breach-report.

and personally consequential. A report focusing on healthcare breaches found the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that victims were often forced to pay out of pocket costs for healthcare they did not receive in order to restore coverage. Almost 50% of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the patients were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impact the economy as a whole.[14]

65. Thus, the healthcare industry and business operating within it have become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[15]

66. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

67. As indicated by Jim Trainor, second in command at the FBI's cyber security division,

> "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[16] A complete identity theft kit with health insurance credentials may be worth up to $1,000 on the black market,

[14] *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..

[15] *9 Reasons why Healthcare is the Biggest Target for Cyberattacks*, SWIVELSECURE, https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited Oct. 10, 2024).

[16] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, IDExperts (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

whereas stolen payment card information sells for about $1.[17]

68. Defendant knew or should have known of the inherent risks in collecting and storing Private Information and the critical importance of providing adequate security for it.

69. As a healthcare provider and business in possession of patients' Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class Members and of the foreseeable consequences if Defendant's network systems were breached. Such consequences include the significant costs imposed on Plaintiff and Class Members due to a breach. Nevertheless, Defendant failed to implement or follow reasonable cybersecurity measures to protect against the Data Breach.

70. 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 Plaintiff and Class Members from being compromised.

71. Defendant was, or should have been, fully aware of the unique type and the significant volume of data stored in its network systems, amounting to at least hundreds of thousands of individuals' detailed Private Information, and, thus, the hundreds of thousands of individuals who would be harmed by the exposure of that unencrypted data.

72. Given the nature of the Data Breach, it was foreseeable that Plaintiff's and Class Members' Private Information compromised therein would be targeted by hackers and cybercriminals for use in variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiff's and Class Members' Private Information can easily obtain their tax returns or open fraudulent credit card accounts in Plaintiff's and Class Members' names.

73. Plaintiff and Class Members were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and

[17] PriceWaterhouseCoopers, *Managing cyber risks in an interconnected world* (Sept. 30, 2014), https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

leaves Plaintiff and Class Members especially vulnerable to identity theft, medical and financial fraud, and the like.

D. Defendant is Required, But Failed, to Comply with FTC Rules and Guidance.

74. The FTC has promulgated numerous guides that 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.

75. In 2016 the FTC updated its publication, *Protecting Personal Information: A Guide for Business*,[18] which established cyber-security guidelines for businesses like Defendant. These guidelines note that businesses should protect the Private Information that they keep; properly dispose of Private Information that is no longer needed; encrypt Private Information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

76. The FTC's guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[19]

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

78. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect third parties' confidential data, treating the failure to

[18] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (2016),https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed May 8, 2024).

[19] *Id.*

employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45 *et seq*. Orders resulting from these actions further clarify the measures business like Defendant must undertake to meet their data security obligations.

79. Such FTC enforcement actions include those against businesses that fail to adequately protect patient data, like Defendant here. *See, e.g.*, *In the Matter of LabMD, Inc*., 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

80. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Defendant of failing to use reasonable measures to protect Private Information they collect and maintain from consumers. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

81. The FTC has also recognized that personal data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[20]

82. Defendant failed to properly implement basic data security practices, in violation of its duties under the FTC Act.

83. Defendant's failure to comply with industry standards or employ reasonable and appropriate measures to protect against unauthorized access to and disclosure of Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

[20] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf.

E. Defendant is Required, But Failed, to Comply with HIPAA.

84. Defendant is a covered business under HIPAA (45 C.F.R. § 160.102) and required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160, Part 164, Subparts A and E; and Security Rule, 45 C.F.R. Part 160, Part 164, Subparts A and C.

85. Defendant is further subject to the Health Information Technology Act ("HITECH")'s rules for safeguarding electronic forms of medical information. See 42 U.S.C. § 17921; 45 C.F.R. § 160.103.

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

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

88. HIPAA's Security Rule required and requires that Defendant 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 their workforce.

89. HIPAA also required and 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]mplement 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).

90. HIPAA and HITECH also require procedures to prevent, detect, contain, and correct data security violations and disclosures of PHI that are reasonably anticipated but not permitted by privacy rules. See 45 C.F.R. § 164.306(a)(1), (a)(3).

91. 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." The list of resources includes a link to guidelines set by the National Institute of Standards and Technology, which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI."

92. HIPAA's Breach Notification Rule further requires that within 60 days of discovering a breach of unsecured patient PHI, as is this Data Breach, Defendant must notify each individual affected regarding the nature of the breach, the PHI compromised, steps the individual should take to protect against potential resulting harm, and what Defendant is doing to protect against future breaches. 45 C.F.R. § 164.404(b).

93. As alleged herein, Defendant violated HIPAA and HITECH. It (a) failed to maintain adequate security practices, systems, and protocols to prevent data loss, (b) failed

to mitigate the risks of a data breach, (c) failed to ensure the confidentiality and protection of PHI, (d) failed to use appropriate safeguards to prevent the unauthorized disclosure of Plaintiff's and Class Members' Private Information, and (e) failed to provide the required Data Breach notice within 60 days of discovering the incident.

F. Defendant Failed to Comply with Industry Standards.

94. A number of published industry and national best practices are widely used as a go-to resource when developing an institution's cybersecurity standards.

95. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[21]

96. The National Institute of Standards and Technology ("NIST") also recommends certain practices to safeguard systems, such as the following:

a. Control who logs on to your network and uses your computers and other devices.
b. Use security software to protect data.
c. Encrypt sensitive data, at rest and in transit.
d. Conduct regular backups of data.
e. Update security software regularly, automating those updates if possible.
f. Have formal policies for safely disposing of electronic files and old devices.

[21] *See* Rapid7, "CIS Top 18 Critical Security Controls Solutions," available at https://www.rapid7.com/solutions/compliance/critical-controls/ (last acc. Feb. 9, 2024).

g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

97. Further still, CISA makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[22]

98. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiff's and Class Members' Private Information, resulting in the Data Breach.

[22] CISA, *Shields Up: Guidance for Organizations*, https://www.cisa.gov/shields-guidance-organizations (last accessed July 8, 2024).

G. Defendant Owed Plaintiff and Class Members a Common Law Duty to Safeguard their Private Information.

99. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff 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's duty owed to Plaintiff and Class Members obligated it to provide reasonable data security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected Plaintiff's and Class Members' Private Information.

100. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information.

101. Defendant owed a duty to Plaintiff and Class Members to implement processes that would detect a compromise of Private Information in a timely manner.

102. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

103. Defendant owed a duty to Plaintiff and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

104. Defendant owed these duties of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

105. Defendant tortiously failed to take the precautions required to safeguard and protect Plaintiff's and Class Members' Private Information from unauthorized disclosure. Defendant's actions and omissions represent a flagrant disregard of Plaintiff's and Class Members' rights.

H. Plaintiff and Class Members Suffered Common Injuries and Damages due to Defendant's Deficient Data Security and the Resulting Data Breach.

106. Defendant's failure to implement or maintain adequate data security measures for Plaintiff's and Class Members' Private Information directly and proximately caused injuries to Plaintiff and Class Members by the resulting disclosure of their Private Information to cybercriminals in the Data Breach.

107. Defendant's conduct, which caused the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways. Plaintiff and Class Members must immediately devote time, energy, and money to (a) closely monitor their medical statements, bills, records, and credit and financial accounts; (b) change login and password information on any sensitive account even more frequently than they already do; (c) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and (d) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

108. The unencrypted Private Information of Plaintiff and Class Members compromised in the Data Breach will end up published or for sale on the dark web because that is the *modus operandi* of hackers.

109. In addition, unencrypted and detailed Private Information may fall into the hands of companies that will use it for targeted marketing without the approval of Plaintiff and Class Members.

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

111. Plaintiff and Class Members are also at a continued risk because their Private Information remains in Defendant's systems, which have already been shown to be susceptible to compromise and are subject to further attack so long as Defendant fails to

undertake the necessary and appropriate security and training measures to protect its customers' Private Information.

112. As a result of Defendant's ineffective and inadequate data security practices, the consequential Data Breach, and the foreseeable outcome of Plaintiff's and Class Members' Private Information ending up in criminals' possession, Plaintiff and Class Members have suffered and will continue to suffer the following injuries and damages, without limitation: (a) invasion of privacy; (b) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) deprivation of value of their Private Information; (g) loss of the benefit of their bargain with Defendants; (h) emotional distress including anxiety and stress in dealing with the Data Breach's aftermath; (i) an increase in spam and scam robocalls, emails, and texts; and (j) the continued risk to their sensitive Private Information, which remains in Defendant's possession and subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect it.

Present and Ongoing Risk of Identity Theft

113. Plaintiff and Class Members are at a heightened risk of identity theft for years to come because of the Data Breach.

114. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201.

115. 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 data by selling it on the internet black market to other criminals, who then utilize it to commit a variety of identity theft related crimes discussed below. Thus, unauthorized actors can, and will, now easily access and misuse Plaintiff's and Class Members' Private Information due to the Data Breach.

116. The dark web is an unindexed layer of the internet that requires special software or authentication to access. Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion. This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

117. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, PII like the Private Information at issue here. The digital character of information stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.

118. In addition, unencrypted and detailed Private Information may fall into the hands of companies that will use it for targeted marketing without the approval of Plaintiff and Class Members.

119. Social Security numbers in particular are among the worst kinds of personal information to have stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and

> don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[23]

120. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

121. Even then, new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[24]

122. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for credit lines.[25]

123. Further, 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

---

[23] Social Security Administration, *Identity Theft and Your Social Security Number*, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

[24] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Aug. 23, 2024).

[25] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), available at https://www.ssa.gov/pubs/EN-05-10064.pdf.

it is for the thief to take on the victim's identity, or to track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

124. 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 are often the starting point for these additional targeted attacks on the victims.

125. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[26]

126. With "Fullz" packages, 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 to assemble complete dossiers on individuals.

127. 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 Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and

[26] 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 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 (last visited Feb. 26, 2024).

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 can still easily create a Fullz package and sell it at a higher price to unscrupulous operators (such as illegal and scam telemarketers) and other nefarious actors over and over. That is exactly what is happening to Plaintiff and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that their stolen Private Information is being misused, and that such misuse is traceable to the Data Breach.

128. Bad actors can also use the Private Information stolen in this Data Breach to access a victim's financial accounts. Identity thieves can impersonate victims by using call spoofing services to falsify information transmitted to a call recipient's caller ID, disguising the identity thief's phone number as the victim's. If the bad actor knows what bank or credit card company the victim uses, it can use spoofing to call the victim's financial institution while masquerading as the victim's phone number to the financial institution's caller ID, using other Private Information about the victim (like the victim's Social Security number) to falsely verify the victim's identity if prompted. Posing as the victim during such calls, identity thieves can obtain information like the victim's account number from the financial institution, or change the victim's online banking or credit card account login information.

129. Even if an identity thief does not know what bank or credit card company the victim uses, the Private Information stolen in the Data Breach can be used to obtain that information. For example, with the Private Information taken in this Data Breach—name, date of birth, address, contact information, and Social Security number—a fraudster can obtain the victim's free consumer disclosure report from a credit reporting agency. These consumer disclosure reports list information about the consumer's financial accounts, including bank addresses, routing numbers, and partial bank account numbers.

130. Similarly, identity thieves can use a victim's name, date of birth, address, contact information, and Social Security number—all Private Information stolen in this Data Breach—to obtain a free copy of the victim's credit report, which contains

information like the victim's credit card accounts (with partial card numbers) and banking institutions, as well as additional information about the victim like account balances and previous addresses.

131. Thus, even if a victim's bank account or credit card information was not compromised in this Data Breach, it is entirely possible for bad actors to use the Private Information obtained about Plaintiff and Class Members to perpetrate bank or credit card fraud against them.

132. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice,

> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.[27]

133. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[28]

134. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

135. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their Private Information. Victims of new

[27] Erika Harrell, *Bureau of Just. Stat.*, U.S. DEP'T OF JUST., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed Jan. 23, 2024).
[28] *See* https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.

account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

136. Further complicating the issues faced by victims of identity theft, data thieves may wait years before using stolen Private Information. To protect themselves, Plaintiff and Class Members will need to remain vigilant for years or even decades to come.

Loss of Time to Mitigate the Risk of Identify Theft and Fraud

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

138. In the likely event that Plaintiff and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches 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.

139. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must monitor their financial accounts for many years to mitigate that harm.

140. Plaintiff and Class Members have spent time, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover.

141. These efforts are consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a

data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 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.[29]

142. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, due to Defendant's conduct and the resulting Data Breach.

Diminished Value of Private Information

143. Private Information is a valuable property right. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

144. For example, drug and medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase Private Information on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

145. Private Information can sell for hundreds of dollars per record on the dark web.[30]

146. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion. In fact, 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. Consumers

[29] *See* FTC, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited Feb. 26, 2024).
[30] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[31]

147. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and likely release onto the dark web, where holds significant value for threat actors. Thus, Plaintiff and Class Members have been deprived of the opportunity to use or profit from their own Private Information as they choose.

148. However, this transfer of value occurred without any consideration paid to Plaintiff 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 diminution of value.

Reasonable and Necessary Future Costs of Credit and Identify Theft Monitoring

149. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered and will continue to suffer for years due to the Data Breach.

150. Given the type of Private Information involved in this Data Breach, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen Private Information will be disseminated on the black market/dark web for sale and purchase by bad actors intending to utilize it for identity theft crimes—*e.g.*, opening bank and other accounts in the victims' names to make purchases or to launder money, filing false tax returns, taking out loans or lines of credit, or filing false unemployment claims.

151. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's

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

employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

152. The Private Information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer breach, where victims can easily cancel or close accounts. The Private Information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers and medical histories).

153. Consequently, Plaintiff and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future, if not forever.

154. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

Lost Benefit of the Bargain

155. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain.

156. When agreeing to provide their Private Information (which was a condition precedent to obtain healthcare services from Defendant), and pay Defendant, directly or indirectly, for those services, Plaintiff and Class Members as patients and consumers understood and expected that they were, in part, paying a premium for services and data security to protect the Private Information they were required to provide.

157. In fact, Defendant did not provide the expected and bargained-for data security. Accordingly, Plaintiff and Class Members received products and services that were of a lesser value than what they reasonably expected to receive under the bargains struck with Defendant.

V. PLAINTIFF'S EXPERIENCES AND INJURIES

158. Plaintiff is a former patient of Defendant. As a condition of receiving healthcare services from Defendant, Plaintiff was required to supply Defendant with his Private Information, including his name, phone number, date of birth, medical history, medical diagnosis and treatment information, health insurance information, Social Security number, provider name, prescription history, test results and images, and other sensitive information.

159. Plaintiff greatly values his privacy and is very careful about sharing his sensitive Private Information. Plaintiff diligently protects his Private Information and stores any documents containing Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

160. Plaintiff would not have provided his Private Information to Defendant had he known it would be kept using inadequate data security and vulnerable to a cyberattack.

161. At the time of the Data Breach—in or around July 22, 2024—Defendant retained Plaintiff's Private Information in its network systems with inadequate data security, causing Plaintiff's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

162. On or about December 16, 2024, Plaintiff received Defendant's Notice Letter informing that his Private Information was accessed and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, hackers acquired files containing Plaintiff's sensitive Private Information, including his name, date of birth, phone number, patient ID, medical records number, diagnosis, medical treatments and procedures, dates and locations of treatment, test results and images, vital signs, and medical provider name.

163. Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff now monitors his financial and credit statements multiple times a

week and has spent hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

164. Plaintiff further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to 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.

165. The risk of identity theft is impending and has materialized, as Plaintiff's and Class Members' Private Information was targeted, accessed, and misused by the cybercriminals behind this Data Breach.

166. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress about his Private Information now being in the hands of cybercriminals, which has been compounded by the fact that Defendant still has not fully informed him of key details about the Data Breach's occurrence or the information stolen.

167. Moreover, since the Data Breach Plaintiff has experienced suspicious spam calls and texts using his compromised Private Information, and believes this to be an attempt to secure additional information from or about him.

VI. CLASS ACTION ALLEGATIONS

168. Plaintiff brings this action individually and on behalf of and all other similarly situated California residents pursuant to Code of Civil Procedure § 382.

169. Plaintiff seeks to represent the following Class:

> All California citizens whose Private Information may have been compromised in the Data Breach, including all California citizens who received a Notice Letter.

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

171. Plaintiff hereby reserves the right to amend or modify the Class definition under California Rules of Court, Rule 3.765, before the Court determines whether certification is appropriate.

172. Numerosity. The Class members are so numerous that joinder of all of them is impracticable. While the precise number of Class members at issue has not been determined, Plaintiff believes the Data Breach affects over 100,000 individuals.

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

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

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

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

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

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

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

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

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

i. Whether Defendant's conduct was negligent;

j. Whether Defendant's conduct was in violation of the FTC Act and/or HIPAA

such that Defendant was negligent *per se*;

k. Whether Defendant's acts breached an implied contract formed with Plaintiff and the Class Members;

l. Whether Defendant violated the California Confidentiality of Medical Records Act;

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

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

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

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

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

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

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

178. Class certification is also appropriate because Defendant has acted or refused to act on grounds that apply generally to the Class as a whole, so that class certification, final injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

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

VII. CAUSES OF ACTION

COUNT I: NEGLIGENCE/NEGLIGENCE *PER SE*

(On behalf of Plaintiff and the Class)

180. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 179 above as if fully set forth herein.

181. Defendant required Plaintiff and Class Members to submit sensitive, confidential Private Information to Defendant as a condition of receiving healthcare services from Defendant.

182. Plaintiff and Class Members provided their Private Information to Defendant, including their names, Social Security numbers, dates of birth, health insurance information, medical diagnosis and treatment information, and other sensitive data.

183. Defendant had full knowledge of the sensitivity of the Private Information to which it was entrusted, and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information was wrongfully disclosed to unauthorized persons.

184. Defendant owed a duty to Plaintiff and each Class Member to exercise reasonable care in holding, safeguarding, and protecting the Private Information it collected from them.

185. Plaintiff and Class Members were the foreseeable victims of any inadequate data safety and security practices by Defendant.

186. Plaintiff and the Class Members had no ability to protect their Private Information in Defendant's possession.

187. By collecting, transmitting, and storing Plaintiff's and Class Members' Private Information Defendant owed Plaintiff and Class Members a duty of care to use reasonable means to secure and safeguard their Private Information, to prevent the information's unauthorized disclosure, and to safeguard it from theft or exfiltration to cybercriminals. Defendant's duty included the responsibility to implement processes by which it could detect and identify malicious activity or unauthorized access on its networks or servers.

188. Defendant owed a duty of care to Plaintiff and the Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that controls for its email servers and systems, and the personnel responsible for them, adequately protected Plaintiff's and Class Members' Private Information. This duty included the responsibility to train Defendant's employees to recognize and prevent attempts to gain initial unauthorized access through common techniques like phishing.

189. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between it and its customers, which is recognized by laws and regulations including but not limited to the FTC Act and HIPAA, as well as the common law. Defendant was able to ensure its network servers and systems were sufficiently protected against the foreseeable harm a data breach would cause Plaintiff and Class Members, yet it failed to do so.

190. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the FTC Act, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

191. Pursuant to the FTC Act, 15 U.S.C. § 45 *et seq*., Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

192. Pursuant to HIPAA, 42 U.S.C. § 1302d *et seq*., Defendant had the further duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' PHI from unauthorized disclosure.

193. Pursuant to HIPAA, Defendant had a duty to implement reasonable data security measures for the PHI in its care, including by, e.g., rendering the electronic PHI in a form unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." *See* 45 C.F.R. § 164.304.

194. Additionally, pursuant to HIPAA, Defendant had a duty to provide notice of the Data Breach within 60 days of discovering it. *See* 42 C.F.R. § 2.16(b); 45 C.F.R. § 164.404(b).

195. Defendant breached its duties to Plaintiffs and Class Members under the FTC Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices and procedures to safeguard Plaintiff's and Class Members' Private Information, by failing to ensure the Private Information in its systems was encrypted and timely deleted when no longer needed, and by failing to provide notice to Plaintiffs and Class Members of the Data Breach until over 60 days after discovering it.

196. The injuries to Plaintiff and Class Members resulting from the Data Breach were directly and indirectly caused by Defendant's violations of the FTC Act and HIPAA.

197. Plaintiff and Class Members are within the class of persons the FTC Act and HIPAA are intended to protect.

198. The type of harm that resulted from the Data Breach was the type of harm the FTC Act and HIPAA are intended to guard against.

199. Defendant's failures to comply with the FTC Act and HIPAA constitute negligence *per se*.

200. Defendant's duty to use reasonable care in protecting Plaintiff's and Class Members' confidential Private Information in its possession arose not only because of the statutes and regulations described above, but also because Defendant is bound by industry standards to reasonably protect such Private Information.

201. Defendant breached its duties of care, and was grossly negligent, by acts of omission or commission, including by failing to use reasonable measures or even minimally reasonable measures to protect the Plaintiff's and Class Members' Private Information from unauthorized disclosure in this Data Breach.

202. 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 Plaintiff's and Class Members' Private Information;
b. Maintaining and/or transmitting Plaintiff's and Class Members' Private Information in unencrypted and identifiable form;
c. Failing to implement data security measures, like adequate MFA for as many systems as possible, to safeguard against known techniques for initial unauthorized access to email servers and systems;
d. Failing to adequately train employees on proper cybersecurity protocols;
e. Failing to adequately monitor the security of its email servers and systems;
f. Failure to periodically ensure its email system had plans in place to maintain reasonable data security safeguards;

g. Allowing unauthorized access to Plaintiff's and Class Members' Private Information; and

h. Failing to timely or adequately notify Plaintiff and Class Members about the Data Breach so they could take appropriate steps to mitigate the potential for identity theft and other damages.

203. But for Defendant's wrongful and negligent breaches of its duties owed to Plaintiff and Class Members, their Private Information would not have been compromised because the malicious activity would have been identified and stopped before cybercriminals had a chance to inventory Defendant's digital assets, stage them, and then exfiltrate them.

204. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' Private Information would injure Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in Defendant's industry.

205. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' Private Information would cause them one or more types of injuries.

206. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injuries, including but not limited to (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) actual identity theft, or the imminent and substantial risk of identity theft or fraud; (d) out-of-pocket and lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (e) loss of benefit of the bargain; (f) anxiety and emotional harm due to their Private Information's disclosure to cybercriminals; and (g) the continued and certainly increased risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect it.

207. Plaintiff and Class Members are entitled to damages, including compensatory, consequential, punitive, and nominal damages, in an amount to be proven at trial.

208. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) provide adequate and lifetime credit monitoring to Plaintiff and all Class Members.

COUNT II: BREACH OF IMPLIED CONTRACT

(On behalf of Plaintiff and the Class)

209. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 179 above as if fully set forth herein.

210. Defendant required Plaintiff and Class Members to provide and entrust their Private Information to Defendant as a condition of and in exchange for receiving healthcare services from Defendant.

211. When Plaintiff and Class Members provided their Private Information to Defendant, they entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such Private Information and to timely and accurately notify Plaintiff and Class Members if and when their Private Information was breached and compromised.

212. Specifically, Plaintiff and Class Members entered into valid and enforceable implied contracts with Defendant when they agreed to provide their Private Information and/or payment to Defendant.

213. The valid and enforceable implied contracts that Plaintiff and Class Members entered into with Defendant included Defendant's promises to protect Private Information it collected from Plaintiff and Class Members, or created on its own, from unauthorized disclosures. Plaintiff and Class Members provided this Private Information in reliance on Defendant's promises, including those in Defendant's Privacy Policy.

214. Under the implied contracts, Defendant promised and was obligated to (a) provide healthcare services to Plaintiff and Class Members; and (b) protect Plaintiff's and Class Members' Private Information provided to obtain such services and/or created in connection therewith. In exchange, Plaintiff and Class Members agreed to provide Defendant with payment and their Private Information.

215. Defendant promised and warranted to Plaintiff and Class Members, including through its public-facing privacy documents identified *supra*, to maintain the privacy and confidentiality of the Private Information it collected from Plaintiff and Class Members and to keep such information safeguarded against unauthorized access and disclosure.

216. Defendant's adequate protection of Plaintiff's and Class Members' Private Information was a material aspect of these implied contracts with Defendant.

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

218. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with industry standards and relevant laws and regulations, including the FTC Act and HIPAA, as well as industry standards.

219. Plaintiff and Class Members who contracted with Defendant for healthcare services including reasonable data protection and provided their Private Information to Defendant reasonably believed and expected that Defendant would adequately employ adequate data security to protect that Private Information.

220. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their Private Information to Defendant and agreed Defendant would receive payment for, amongst other things, the protection of their Private Information.

221. Plaintiff and Class Members performed their obligations under the contracts when they provided their Private Information and/or payment to Defendant.

222. Defendant materially breached its contractual obligations to protect the Private Information it required Plaintiff and Class Members to provide when that Private Information was unauthorizedly disclosed in the Data Breach due to Defendant's inadequate data security measures and procedures.

223. Defendant materially breached its contractual obligations to deal in good faith with Plaintiff and Class Members when it failed to take adequate precautions to prevent the Data Breach and failed to promptly notify Plaintiff and Class Members of the Data Breach.

224. Defendant materially breached the terms of its implied contracts, including but not limited to by failing to comply with industry standards or the standards of conduct embodied in statutes or regulations like Section 5 of the FTC Act and HIPAA, by failing to otherwise protect Plaintiff's and Class Members' Private Information, as set forth *supra*.

225. The Data Breach was a reasonably foreseeable consequence of Defendant's breaches of these implied contracts with Plaintiff and Class Members.

226. As a result of Defendant's failures to fulfill the data security protections promised in these contracts, Plaintiff and Class Members did not receive the full benefit of their bargains with Defendant, and instead received services of a diminished value compared to that described in the implied contracts. Plaintiff and Class Members were therefore damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and that which they received.

227. Had Defendant disclosed that its data security procedures were inadequate or that it did not adhere to industry standards for cybersecurity, neither Plaintiffs, Class Members, nor any reasonable person would have contracted with Defendant.

228. Plaintiff and Class Members would not have provided and entrusted their Private Information to Defendant in the absence of the implied contracts between them and Defendant.

229. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their Private Information and by failing to provide timely or adequate notice that their Private Information was compromised in and due to the Data Breach.

230. As a direct and proximate result of Defendant's breach of its implied contracts with Plaintiff and Class Members and the attendant Data Breach, Plaintiff and Class Members have suffered injuries and damages as set forth herein and have been irreparably harmed, as well as suffering and the loss of the benefit of the bargain they struck with Defendant.

231. Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT III: INVASION OF PRIVACY/INSTRUSION UPON SECLUSION

(On behalf of Plaintiff and the Class)

232. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 179 above as if fully set forth herein.

233. Plaintiff and Class Members had a legitimate expectation of privacy to their Private Information and were entitled to Defendant's protection of this Private Information in its possession against disclosure to unauthorized third parties.

234. Defendant owed a duty to its patients, including Plaintiff and Class Members, to keep their Private Information confidential and secure.

235. Defendant failed to protect Plaintiff's and Class Members' Private Information and instead exposed it to unauthorized persons, a criminal ransomware group, which upon information and belief, has or imminently will make the Private Information publicly available and disseminated it to thousands of people over the dark web, where cybercriminals go to find their next identity theft and extortion victims.

236. Defendant allowed unauthorized third parties access to and examination of the Private Information of Plaintiff and Class Members, by way of Defendant's failure to

protect the Private Information through reasonable data security measures.

237. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiff and Class Members is highly offensive to a reasonable person and represents an intrusion upon Plaintiff's and Class Members' seclusion as well as a public disclosure of private facts.

238. The intrusion was into a place or thing, which was private and is entitled to be private—sensitive and confidential information including private medical histories, images, diagnoses, and prescriptions, as well as PII like Social Security numbers and birth certificates.

239. Plaintiff and Class Members disclosed their Private Information to Defendant as a condition of and in exchange for receiving healthcare services, but privately with an intention that the Private Information would be kept confidential and protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization, given Defendant's promises to that effect.

240. Subsequent to the intrusion, Defendant permitted Plaintiff's and Class Members' data to be published online to countless cybercriminals whose mission is to misuse such information, including through identity theft and extortion.

241. The Data Breach constitutes an intentional or reckless interference by Defendant with Plaintiff's and Class Members' interests in solitude or seclusion, as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

242. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur, because it had actual knowledge that its information security practices were inadequate and insufficient to protect Plaintiff's and Class Members' Private Information from unauthorized disclosure.

243. Defendant acted with reckless disregard for Plaintiff's and Class Members'

privacy when it allowed improper access to its systems containing Plaintiff's and Class Members' Private Information without protecting said data from the unauthorized disclosure, or even encrypting such information.

244. Defendant was aware of the potential of a data breach and failed to adequately safeguard its network systems or implement appropriate policies to prevent the unauthorized release of Plaintiff's and Class Members' Private Information to cybercriminals.

245. Because Defendant acted with this knowing state of mind, it had notice and knew that its inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

246. As a direct and proximate result of Defendant's acts and omissions set forth above, Plaintiff's and Class Members' Private Information was disclosed to third parties without authorization, causing Plaintiff and Class Members to suffer injuries and damages including, without limitation, (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) out-of-pocket and lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (d) loss of benefit of the bargain; and (e) the continued and certainly increased risk to their Private Information, which remains in Defendant's possession in unencrypted form and subject to further unauthorized disclosures, so long as Defendant fails to undertake appropriate and adequate measures to protect it.

247. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the Private Information maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class Members.

COUNT IV:

Violations of California's Confidentiality of Medical Information Act

Cal. Civ. Code § 56 *Et Seq.* ("CMIA")

(On Behalf of Plaintiff and the Class)

248. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 179 above, as if fully set forth herein.

249. Defendant is a "Provider of Health Care" as defined in Cal. Civ. Code § 56.06.

250. Plaintiff and Class Members are "patients" as defined by Cal. Civ. Code § 56.05(k).

251. Plaintiff's and Class Members' Private Information that was the subject of the Data Breach included "Medical Information" as defined by Cal. Civ. Code § 56.05(j).

252. Defendant had a duty under §§ 56.06 and 56.101 of the CMIA to maintain, store, and dispose of Plaintiff's and Class Members' PHI/Medical Information in a manner that preserved their confidentiality.

253. Sections 56.06 and 56.101 of the CMIA prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction, or disposal of confidential medical information. Defendant violated these statutory obligations.

254. In violation of the CMIA, Defendant disclosed PHI/Medical Information of Plaintiff and Class Members without first obtaining authorization.

255. In violation of the CMIA, Defendant created, maintained, preserved, stored, abandoned, destroyed, or disposed of PHI/Medical Information of Plaintiff and Class Members in a manner that did not preserve the confidentiality of that PHI/Medical Information.

256. In violation of the CMIA, Defendant negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of PHI/Medical Information of Plaintiff and Class Members.

257. In violation of the CMIA, Defendant's electronic health record systems or electronic medical record systems did not protect and preserve the integrity of Plaintiff's and Class Members' PHI/Medical Information.

258. In violation of the CMIA, Defendant negligently released confidential information and records of Plaintiff and Class Members.

259. In violation of the CMIA, Defendant negligently disclosed PHI/Medical Information of Plaintiff and Class Members.

260. In violation of the CMIA, Defendant knowingly and willfully obtained, disclosed, and/or used PHI/Medical Information of Plaintiff and Class Members.

261. Because Defendant maintained Plaintiff's and Class Members' PHI/Medical Information in California, on California-based servers, where Defendants ultimately disclosed such information to third parties, the CMIA equally applies to the entire affected class to the extent it includes both California and non-California citizens. *See, e.g.*, *Doe v. Meta Platforms, Inc.*, 690 F.Supp.3d 1064, 1079 (N.D. Cal. 2023) (holding that another statute, CIPA, could apply to non-residents of California, because the conduct at issue occurred in California).

262. As a direct and proximate result of Defendant's violation of the CMIA, Plaintiffs and Class Members now face an increased risk of future harm.

263. As a direct and proximate result of Defendants' violations of the CMIA, Plaintiffs and Class Members have been injured and are entitled to compensatory damages, punitive damages, and nominal damages of $1,000 for each of Defendants' violations of the CMIA, as well as attorneys' fees and costs pursuant to Cal. Civ. Code § 56.36.

COUNT V: UNJUST ENRICHMENT

(On behalf of Plaintiff and the Class)

264. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 179 above as if fully set forth herein.

265. This claim is pleaded in the alternative to the claim for breach contract.

266. Plaintiff and Class Members conferred a direct benefit on Defendant by way of providing payment and their confidential and sensitive Private Information to Defendant as part of Defendant's business.

267. Defendant required Plaintiff's and Class Members' Private Information to conduct its business and generate revenue, which it could not do without collecting and maintaining Plaintiff's and Class Members' Private Information.

268. The monies Plaintiff and Class Members paid to Defendant included a premium for Defendant's cybersecurity obligations and were supposed to be used by Defendant, in part, to pay for the administrative and other costs of providing reasonable data security and protection for Plaintiff's and Class Members' Private Information.

269. Defendant benefitted from collecting and using Plaintiff's and Class Members' Private Information, using it to generate revenue, market its services, and fundraise.

270. Defendant enriched itself by hoarding the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheap, ineffective security measures and diverting those funds to its own personal use. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

271. Defendant failed to provide reasonable security, safeguards, and protections to the Private Information of Plaintiff and Class Members, and as a result, Defendant was overpaid.

272. Under principles of equity and good conscience, Defendant should not be permitted to retain the money Plaintiff and Class Members paid it because Defendant failed to provide adequate safeguards and security measures to protect Plaintiff's and Class Members' Private Information, which Plaintiff and Class Members paid for but did not receive.

273. Defendant wrongfully accepted and retained these benefits—payment and Plaintiff's and Class Members' Private Information—and was enriched to the detriment of Plaintiff and Class Members.

274. Defendant's enrichment at Plaintiff's and Class Members' expense is unjust.

275. As a result of Defendant's wrongful conduct and resulting unjust enrichment, Plaintiff and Class Members are entitled to restitution and disgorgement of profits, benefits, and other compensation obtained by Defendant, plus reasonable attorneys' fees and costs.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff Donald Crosslin, individually and on behalf of all others similarly situated, prays for judgment as follows:

A. An Order certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

B. Awarding Plaintiff and the Class damages that include applicable compensatory, actual, statutory, nominal, exemplary, and punitive damages, as allowed by law;

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

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

E. Awarding injunctive relief in the form of additional technical and administrative cybersecurity controls as is necessary to protect the interests of Plaintiff and the Class;

F. Enjoining Defendant from further deceptive practices and making untrue statements about its data security;

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

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

I. Awarding such further relief to which Plaintiff and the Class are entitled.

IX. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues to triable.

Dated: January 10, 2025

Respectfully submitted,

By: */s/ Kristen Lake Cardoso*
Kristen Lake Cardoso

KOPELOWITZ OSTROW P.A.
Kristen Lake Cardoso (CA Bar No. 338762)
cardoso@kolawyers.com
Kenneth J. Grunfeld (PHV forthcoming)
grunfeld@kolawyers.com
One West Las Olas, Suite 500
Fort Lauderdale, FL 33301
Telephone: (954) 525-4100

Attorneys for Plaintiff and the Putative Class