John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Email: jnelson@milberg.com

Attorney for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

JAY GOLDSTEIN, individually and on behalf of all others similarly situated, Plaintiff, vs. PROSPECT MEDICAL HOLDINGS, INC., Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Jay Goldstein ("Plaintiff") brings this Class Action Complaint ("Complaint") against Defendant Prospect Medical Holdings, Inc. ("Prospect" or "Defendant") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard Plaintiff's and other similarly situated patients and/or patients' sensitive information, including full names, dates of birth, and Social Security numbers ("personally identifiable information" or "PII") and medical and health insurance information, which is protected health information ("PHI", and collectively with PII, "Private Information") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

2. Defendant is a healthcare corporation composed of "hospitals and affiliated medical groups" that provide medical services to patients in "California, Connecticut, Pennsylvania, Texas and Rhode Island."[1]

3. Former and current patients of Defendant are required to entrust Defendant with sensitive, non-public Private Information, in order to obtain medical services from Defendant. Defendant retains this information for at least many years and even after the relationship has ended.

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

[1] https://www.pmh.com/ (last accessed Oct. 12, 2023).

5. On August 1, 2023, Defendant "learned of a data security incident that disrupted the operations of some of [its] IT systems."[2] In response, Defendant "engaged the expertise of a third-party forensic investigation firm to conduct a thorough investigation."[3]

6. According to Defendant's untitled letter sent to Plaintiff and Class Members (the "Notice Letter"), the compromised Private Information included individuals' names; dates of birth; Social Security numbers, diagnoses information, lab results, prescription information, treatment information, and medical record numbers.[4]

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

[2] *See* Notice Letter. A sample copy is available at https://apps.web.maine.gov/online/aeviewer/ME/40/c4f1f925-6136-45dd-99fa-6c92cab12031.shtml (last accessed Oct. 12, 2023).

[3] *Id.*

[4] *Id.*

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

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

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

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

10. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

11. Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of himself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

PARTIES

12. Plaintiff, Jay Goldstein, is a natural person and resident of Santa

Monica, California, where he intends to remain.

13. Defendant is a Delaware corporation with its principal place of business located at 3415 South Sepulveda Boulevard, 9th Floor, Los Angeles, California 90034.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.[5]

15. This Court has personal jurisdiction over Defendant because its principal place of business is in this District, regularly conducts business in California, and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

16. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

FACTUAL ALLEGATIONS

[5] According to the report submitted to the Office of the Maine Attorney General, 67 Maine residents were impacted in the Data Breach. *See* https://apps.web.maine.gov/online/aeviewer/ME/40/c4f1f925-6136-45dd-99fa-6c92cab12031.shtml (last accessed Oct. 12, 2023).

Defendant's Business

17. Defendant is a healthcare corporation composed of "hospitals and affiliated medical groups" that provide medical services to patients in "California, Connecticut, Pennsylvania, Texas and Rhode Island."[6]

18. Plaintiff and Class Members are current and former patients of Defendant.

19. As a condition of receiving medical services at Prospect, Defendant requires that its patients, including Plaintiff and Class Members, entrust it with highly sensitive personal information.

20. The information held by Defendant in its computer systems or shared with its vendors at the time of the Data Breach included the unencrypted Private Information of Plaintiff and Class Members.

21. Upon information and belief, Defendant made promises and representations to its patients, including Plaintiff and Class Members, that the Private Information collected from them as a condition of obtaining medical services at Prospect would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

22. Indeed, Defendant's Privacy Statement provides that: "we have

[6] https://www.pmh.com/ (last accessed Oct. 12, 2023).

security measures in place to protect against the loss, misuse and/or unauthorized access of personal information . . . We aim to protect and keep confidential all information that is voluntarily provided to us through this website[.]"[7]

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

24. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class Members relied on the sophistication of Defendant 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. Plaintiff and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

25. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties and to audit, monitor, and verify the integrity of its IT vendors' and affiliates' data security practices and systems. Defendant has a legal duty to keep

[7] https://www.pmh.com/globalassets/pmh/footer/pmhprivacypolicy.pdf (last accessed Oct. 12, 2023).

patient's Private Information safe and confidential.

26. Defendant had obligations created by FTC Act, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

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

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

The Data Breach

29. On August 3, 2023 Defendant's network was breached by a well known ransomware group called Rhysida.[8] The Rhysida group previously rose to prominence after exfiltrating and leaking data stolen from the Chilean Armed Forces. The group has been so active that the Department of Health and Human

[8] https://www.bleepingcomputer.com/news/security/rhysida-claims-ransomware-attack-on-prospect-medical-threatens-to-sell-data/

Services published a bulletin outlining the group's mechanism of attack and advising health care organizations to take precautions against Rhysida.[9] The HHS bulletin further warned that of the eight organizations attacked by Rhysida ransomware, the exfiltrated data was subsequently published from five of those organizations.[10]

30. Following the Data Breach, "[Rhysida] claim that they stole 1 TB of documents and a 1.3 TB SQL database containing 500,000 social security numbers, passports, driver's licenses, corporate documents, and patients' medical information."[11] The group also publicly posted "screenshots of driver's licenses, social security cards, documents, and what appears to be patients' medical information." The group demanded a payment of roughly $1.3 million in exchange for the stolen information.

31. On or about September 29, 2023, Defendant began sending Plaintiff and other Data Breach victims an untitled letter (the "Notice Letter"), informing them that:

> On August 1, 2023, Prospect Medical learned of a data security incident that disrupted the operations of some of our IT systems. We immediately took steps to secure our systems, contain the incident, and notify law enforcement. Additionally, we engaged the expertise of a third-party forensic investigation

[9] https://www.hhs.gov/sites/default/files/rhysida-ransomware-sector-alert-tlpclear.pdf

[10] *Id.*

[11] https://www.bleepingcomputer.com/news/security/rhysida-claims-ransomware-attack-on-prospect-medical-threatens-to-sell-data/

> firm to conduct a thorough investigation.
>
> Through our ongoing investigation, on September 13, 2023, we determined that an unauthorized party gained access to our IT network between the dates of July 31, 2023 and August 3, 2023. While in our IT network, the unauthorized party accessed files that contain information pertaining to Prospect Medical patients. Our investigation concluded that some of these files contained your information, such as your name, Social Security number, diagnosis information, lab results, prescription information, treatment information, medical record number, and date of birth.[12]

32. Omitted from the Notice Letter were the details of 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 remains protected.

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

34. A ransomware attack, like that experienced by Defendants is a type of cyberattack that is frequently used to target companies due to the sensitive patient data they maintain.[13] In a ransomware attack the attackers use software to encrypt

---

[12] The Notice Letter.

[13] *Ransomware warning: Now attacks are stealing data as well as encrypting it*, available at https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/

data on a compromised network, rendering it unusable and demanding payment to restore control over the network.[14]

35. Companies should treat ransomware attacks as any other data breach incident because ransomware attacks don't just hold networks hostage, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[15] As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence […] the initial assumption should be that data may have been exfiltrated."

36. An increasingly prevalent form of ransomware attack is the "encryption+exfiltration" attack in which the attacker encrypts a network and exfiltrates the data contained within.[16] In 2020, over 50% of ransomware attackers exfiltrated data from a network before encrypting it.[17] Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion

---

[14] *Ransomware: The Data Exfiltration and Double Extortion Trends*, available at https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends

[15] *The chance of data being stolen in a ransomware attack is greater than one in ten*, available at https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/

[16] *2020 Ransomware Marketplace Report, available at https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report*

[17] *Ransomware FAQs*, available at https://www.cisa.gov/stopransomware/ransomware-faqs

attempt."[18] And even where companies pay for the return of data attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[19]

37. The attacker accessed and acquired files Defendant shared with a third party containing unencrypted Private Information of Plaintiff and Class Members, including their Social Security numbers, PHI, and other sensitive information. Plaintiff's and Class Members' Private Information was accessed and stolen in the Data Breach.

38. Plaintiff believes that his Private Information and that of Class Members was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

Data Breaches Are Preventable

39. Defendant could have prevented this Data Breach by, among other things, properly encrypting Private Information being shared with its vendors or otherwise ensuring that such Private Information was protected while in transit or accessible.

40. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for

[18] *Id.*

[19] *Id.*

Plaintiff and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

41. The unencrypted Private Information of Class Members will end up for sale to identity thieves on the dark web, if it has not already, or it could simply fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

42. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[20]

43. To prevent and detect ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, patients and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting

[20] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Aug. 23, 2021).

and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[21]

44. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

[21] *Id.* at 3-4.

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].[22]

45. Given that Defendant was storing the Private Information of its current and former patients, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

Defendant Acquires, Collects, And Stores Patients' Private Information

46. Defendant has historically acquired, collected, stored, and shared the Private Information of Plaintiff and Class Members.

47. As a condition of obtaining medical services at Prospect, Defendant requires that its patients entrust it with highly sensitive personal information.

48. By obtaining, collecting, sharing, and using Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and

[22] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Nov. 11, 2021).

Class Members' Private Information from disclosure.

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

50. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiff and Class Members or by exercising due diligence in selecting its IT vendors and properly auditing those vendor's security practices.

51. Upon information and belief, Defendant made promises to Plaintiff and Class Members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

52. Indeed, Defendant's Privacy Statement provides that: "we have security measures in place to protect against the loss, misuse and/or unauthorized access of personal information . . . We aim to protect and keep confidential all information that is voluntarily provided to us through this website[.]"[23]

53. Plaintiff and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Defendant Knew or Should Have Known of the Risk Because Healthcare

[23] https://www.pmh.com/globalassets/pmh/footer/pmhprivacypolicy.pdf (last accessed Oct. 12, 2023).

Entities In Possession Of Private Information Are Particularly Suspectable To Cyber Attacks

54. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting health care entities that collect and store Private Information, like Defendant, preceding the date of the breach.

55. Data thieves regularly target companies like Defendant's due to the highly sensitive information that they custody. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

56. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[24]

57. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients and/or patients, March 2019), University of Washington Medicine (974,000 patients and/or patients, December 2018), Florida Orthopedic Institute (640,000 patients and/or patients, July 2020), Wolverine

[24] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/ (last accessed Oct. 11, 2023).

Solutions Group (600,000 patients and/or patients, September 2018), Oregon Department of Human Services (645,000 patients and/or patients, March 2019), Elite Emergency Physicians (550,000 patients and/or patients, June 2020), Magellan Health (365,000 patients and/or patients, April 2020), and BJC Health System (286,876 patients and/or patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals

58. As a custodian of 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 its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

59. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[25]

60. Despite the prevalence of public announcements of data breach and

[25] FBI, Secret Service Warn of Targeted, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbisecret-service-warn-of-targeted-ransomware (last visited Sep. 13, 2022).

data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

61. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

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

63. Additionally, as companies became more dependent on computer systems to run their business,[26] *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,

[26]https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html

and technical safeguards.[27]

64. In the Notice Letter, Defendant offers to provide 12 months of credit monitoring and identity theft insurance services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff and Class Members' Private Information. Moreover, once this service expires, Plaintiff and Class Members will be forced to pay out of pocket for necessary identity monitoring services.

65. Defendant's offer of credit and identity monitoring establishes that Plaintiff's and Class Members' sensitive Private Information *was* in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems.

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

67. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once

[27] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022

Private Information is stolen—particularly Social Security numbers and PHI—fraudulent use of that information and damage to victims may continue for years.

68. As a healthcare entity in possession of sensitive Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to them by Plaintiff and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

Defendant Fails To Comply With FTC Guidelines

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

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

problems.[28]

71. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[29]

72. 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.

73. The FTC has brought enforcement actions against healthcare companies for failing to protect patient data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential patient data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C.

---

[28] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Oct. 17, 2022).

[29] *Id.*

§ 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

74. These FTC enforcement actions include actions against healthcare companies, like Defendant. *See, e.g., In the Matter of LabMd, Inc., A Corp*, 2016-2 Trade Cas. (Henry Ford) ¶ 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.").

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

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

77. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Private Information of its patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with HIPAA Guidelines

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

of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

79. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[30] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

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

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

82. 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.

83. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in

[30] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

electronic media." 45 C.F.R. § 160.103.

84. HIPAA's Security Rule requires Defendant to do the following:

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

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

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

d. Ensure compliance by its workforce.

85. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]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).

86. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to

protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

87. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[31]

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

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

90. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance

[31] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added).

documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[32] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[33]

Defendant Fails To Comply With Industry Standards

91. As noted above, experts studying cyber security routinely identify healthcare companies in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

92. Several best practices have been identified that, at a minimum, should

[32] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.

[33] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

be implemented by healthcare companies in possession of Private Information, like Defendant, including but not limited to: educating all patients; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which patients can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

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

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

cybersecurity readiness.

95. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Defendant's Breach

96. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless by conducting the following acts and/or omissions:

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

b. Failing to adequately protect Private Information;

c. Failing to ensure the confidentiality and integrity of electronic Private Information it created, received, maintained, and/or transmitted;

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic Private Information to allow access only to those persons or software programs that have been granted access rights;

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

f. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports;

g. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic Private Information;

h. Failing to train all members of their workforces effectively on the policies and procedures regarding Private Information;

i. Failing to render the electronic Private Information it maintained unusable, unreadable, or indecipherable to unauthorized individuals;

j. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

k. Failing to audit, monitor, and verify the adequacy of its vendors' data security practices

l. Failing to adhere to HIPAA guidelines and industry standards for cybersecurity as discussed above; and,

m. Otherwise breaching their duties and obligations to protect Plaintiff's and Class Members' Private Information.

97. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access Defendant's online insurance application flow, which provided unauthorized actors

with unsecured and unencrypted Private Information.

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

99. Accordingly, as outlined below, Plaintiff and Class Members now face a present, increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members lost the benefit of the bargain they made with Defendant.

COMMON INJURIES & DAMAGES

100. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their Private Information; (e) invasion of privacy; and (f) the continued risk to their Private

Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

The Data Breach Increases Victims' Risk Of Identity Theft

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

102. The unencrypted Private Information of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

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

104. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt

other hacking crimes against the individual to obtain more data to perfect a crime.

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

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

107. With "Fullz" packages, cyber-criminals can cross-reference two

[34] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of 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.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited on May 26, 2023).

sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

108. 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' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

109. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiff and the other Class Members.

110. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

111. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam

telemarketers).

Loss Of Time To Mitigate Risk Of Identity Theft And Fraud

112. 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 resource and asset of time has been lost.

113. 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 the risk of identity theft. The Notice Letter sent by Defendant to Plaintiff and Class Members encourages them to take "some additional steps you can take in response, please see the additional information provided in this letter."[35]

114. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, signing up for the credit and identity theft monitoring services offered by Defendant, and checking

[35] Notice Letter.

their financial accounts for any indication of fraudulent activity, which may take years to detect..

115. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[36]

116. Plaintiff's mitigation efforts are also 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.[37]

Diminution Value Of Private Information

117. PII and PHI are valuable property rights.[38] Their value is axiomatic,

---

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

[37] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited July 7, 2022).

[38] *See, e.g.,* Randall T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private Information, which companies obtain at little

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.

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

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

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

121. Conversely sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[43]

122. Theft of PHI is also gravely serious: "[a] thief may use your name or

---

cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

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

[40] https://datacoup.com/

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

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

[43] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Sep. 13, 2022).

health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."

123. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[44]

124. 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 by its compromise and unauthorized release. 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 loss of value.

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

[44] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last accessed July 20, 2021)

Social Security numbers,, PHI, and dates of birth.

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

127. The fraudulent activity resulting from the Data Breach may not come to light for years.

128. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

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

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

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

131. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes –*e.g.,* opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

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

133. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[45] The information disclosed in this Data Breach is

[45] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report*

impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

134. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

135. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach.

Loss Of The Benefit Of The Bargain

136. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When obtaining medical services at Defendant under certain terms, Plaintiff and other reasonable patients understood and expected that they were, in part, paying, or being paid less, for services and data security to protect the Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received medical services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

PLAINTIFF GOLDSTEIN'S EXPERIENCE

Finds, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

137. Plaintiff Jay Goldstein is a former Prosect patient that obtained medical services at Defendant in or about 2020.

138. As a condition obtaining medical services at Prospect, Plaintiff was required to provide his Private Information to Defendant, including his name, date of birth, and Social Security number.

139. At the time of the Data Breach—July 31, 2023 through August 3, 2023—Defendant retained Plaintiff's Private Information in its system.

140. Plaintiff Jay Goldstein is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his 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. Plaintiff would not have entrusted his Private Information to Defendant had he known of Defendant's lax data security policies.

141. Plaintiff Jay Goldstein received the Notice Letter, by U.S. mail, directly from Defendant, dated September 29, 2023. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties, including his name, Social Security number, diagnosis information, lab results, prescription information, treatment information, medical record number, and date of birth.

142. As a result of the Data Breach, and at the direction of Defendant's

Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, signing up for the credit and identity theft monitoring services offered by Defendant, and checking his financial accounts for any indication of fraudulent activity, which may take years to detect.. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

143. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

144. Plaintiff further suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

145. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

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

147. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

148. Plaintiff Jay Goldstein has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

149. This action is properly maintainable as a class action. Plaintiff brings this class action on behalf of himself and on behalf of all others similarly situated.

150. Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

Nationwide Class

All individuals residing in the United States whose Private Information was

compromised in the data breach announced by Defendant in September 2023 (the "Class").

California Subclass
All individuals residing in the state of California whose Private Information was compromised in the data breach announced by Defendant in September 2023 (the "California Subclass").

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

152. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. At least 190,000 individuals were notified by Defendant of the Data Breach, according to the breach report submitted to Office of the Maine Attorney General.[46] The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

153. Common questions of law and fact exist as to all members of the Class that predominate over any questions affecting solely individual members of the

[46] https://apps.web.maine.gov/online/aeviewer/ME/40/c4f1f925-6136-45dd-99fa-6c92cab12031.shtml (last accessed Oct. 12, 2023).

Class. The questions of law and fact common to the Class, which may affect individual Class members, include, but are not limited to, the following:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;

b. Whether Defendant had respective duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had respective duties not to use the Private Information of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g.. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

h. 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;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct; and

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

154. Typicality: Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

155. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Nationwide Class as a whole. Defendant's policies challenged herein apply to and affect Class

Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

156. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

157. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such

a claim, it would still be economically impractical and impose a burden on the courts.

158. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

159. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

160. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

161. Unless a Class-wide injunction is issued, Defendant may continue in its

failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

162. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Code of Civil Procedure § 382.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

163. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

164. Defendant requires its patients, including Plaintiff and Class Members, to submit non-public Private Information in the ordinary course of providing its medical services.

165. Defendant gathered and stored the Private Information of Plaintiff and Class Members as part of its business of soliciting its services to its patients, which solicitations and services affect commerce.

166. Plaintiff and Class Members entrusted Defendant with their Private Information with the understanding that Defendant would safeguard their

information.

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

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

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

170. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative,

technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

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

172. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Private Information, a necessary part of being patients of Defendant.

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

174. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

175. Defendant also had a duty to exercise appropriate clearinghouse

practices to remove former patients' Private Information it was no longer required to retain pursuant to regulations.

176. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

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

178. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

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

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

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

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

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

f. Failing to remove former patients' Private Information it was no longer required to retain pursuant to regulations,

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

h. Failing to audit, monitor, and verify the adequacy of its vendors' security practices; and

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

179. Defendant violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

180. Plaintiff and the Class are within the class of persons that the FTC Act and HIPAA were intended to protect.

181. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against.

182. Defendant's violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

183. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

184. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

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

186. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

187. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have

known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

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

189. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

190. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

191. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

192. Defendant has admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of

the Data Breach.

193. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the Private Information of Plaintiff and the Class would not have been compromised.

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

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

third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

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

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

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

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

200. Plaintiff and Class Members are also entitled to injunctive relief

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

COUNT II
Breach Of Implied Contract
(On Behalf of Plaintiff and the Class)

201. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

202. Plaintiff and Class Members were required to provide their Private Information to Defendant as a condition of receiving medical services from Defendant.

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

204. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the

Private Information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

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

206. Defendant solicited, offered, 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.

207. In accepting the Private Information of Plaintiff and Class Members, Defendant understood and agreed that it was required to reasonably safeguard the Private Information from unauthorized access or disclosure.

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

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

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

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

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

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

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

215. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to

delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

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

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

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

COUNT III
Unjust Enrichment / Quasi Contract
(On Behalf of Plaintiff and the Class)

219. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

220. This Count is pleaded in the alternative to the breach of implied contract claim (Count II) above.

221. Plaintiff and Class Members conferred a monetary benefit upon

Defendant in the form of providing their valuable Private Information to Defendant.

222. Plaintiff and Class Members provided Defendant their Private Information on the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures from the revenue it derived therefrom. In exchange, Plaintiff and Class Members should have received adequate protection and data security for such Private Information held by Defendant.

223. Defendant benefited from receiving Plaintiff's and Class Members' labor and from receiving their Private Information through its ability to retain and use that information for its own benefit. Defendant understood and accepted this benefit.

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

225. Because all Private Information provided by Plaintiff and Class Members was similarly at risk from a foreseeable and targeted data breach, Defendant's obligation to safeguard the Private Information it collected from its patients was inherent to the relationship.

226. Defendant also understood and appreciated that Plaintiff's and Class Members' Private Information was private and confidential, and its value depended

upon Defendant maintaining the privacy and confidentiality of that information.

227. Defendant failed to provide reasonable security, safeguards, and protections to the Private Information of Plaintiff and Class Members.

228. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff' and Class Members' Private Information.

229. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead made calculated decisions to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

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

231. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

232. Defendant acquired the monetary benefit and Private Information through inequitable means in that they failed to disclose the inadequate security

practices previously alleged.

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

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

235. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury as described herein.

236. Plaintiff and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

COUNT IV
Violation of the California Unfair Competition Law,
Cal. Bus. & Prof. Code §17200 *et seq.*
(On Behalf of Plaintiff and the California Subclass)

237. Plaintiff re-alleges and incorporates by reference each and every allegation in this Complaint, as if fully set forth herein.

238. Defendant is a "person" defined by Cal. Bus. & Prof. Code § 17201.

239. Defendant violated Cal. Bus. & Prof. Code § 17200 *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

240. Defendant's "unfair" acts and practices include:

a. Defendant failed to implement and maintain reasonable security measures to protect Plaintiff's and California Subclass Members'

personal information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Defendant Data Breach. Defendant failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industry;

b. Defendant's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45), California's Customer Records Act (Cal. Civ. Code § 1798.80 *et seq.*), and California's Consumer Privacy Act (Cal. Civ. Code § 1798.150);

c. Defendant's failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendant's inadequate security, consumers could not have reasonably avoided the harms that Defendant caused; and

d. Engaging in unlawful business practices by violating Cal. Civ. Code §

1798.82.

241. Defendant has engaged in "unlawful" business practices by violating multiple laws, including the FTC Act, 15 U.S.C. § 45, and California common law.

242. Defendant's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and California Subclass Members' personal information, which was a direct and proximate cause of the Defendant Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, which was a direct and proximate cause of the Defendant Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Defendant Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and California Subclass Members' personal information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and California Subclass Members' personal information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

243. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' personal information.

244. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass Members were injured and lost money or property, which would not have occurred but for the unfair and deceptive acts, practices, and omissions alleged herein, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personal

information.

245. Defendant's violations were, and are, willful, deceptive, unfair, and unconscionable.

246. Plaintiff and California Subclass Members have lost money and property as a result of Defendant's conduct in violation of the UCL, as stated herein and above.

247. By deceptively storing, collecting, and disclosing their personal information, Defendant has taken money or property from Plaintiff and California Subclass Members.

248. Defendant acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and California Subclass Members' rights.

249. Plaintiff and California Subclass Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unlawful, and fraudulent business practices or use of their personal information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

COUNT V
Violation of the California Consumer Privacy Act,
Cal. Civ. Code §§ 1798.100 *et seq.*, § 1798.150(a)
(On Behalf of Plaintiff and the California Subclass)

250. Plaintiff re-alleges and incorporates by reference each and every allegation in this Complaint, as if fully set forth herein.

251. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically provides:

> Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:
>
> > (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.
> >
> > (B) Injunctive or declaratory relief.
> >
> > (C) Any other relief the court deems proper.

252. Defendant is a "business" under § 1798.140(b) in that it is a corporation organized for profit or financial benefit of its shareholders or other owners, with gross revenue in excess of $25 million.

253. Plaintiff and California Subclass Members are covered "consumers" under § 1798.140(g) in that they are natural persons who are California residents.

254. The personal information of Plaintiff and the California Subclass Members at issue in this lawsuit constitutes "personal information" under §

1798.150(a) and 1798.81.5, in that the personal information Defendant collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

255. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the California Subclass Members' personal information and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the California Subclass Members. Specifically,

Defendant subjected Plaintiff's and the California Subclass Members' nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

256. As a direct and proximate result of Defendant's violation of its duty, the unauthorized access and exfiltration, theft, or disclosure of Plaintiff's and California Subclass Members' personal information included exfiltration, theft, or disclosure through Defendant's servers, systems, and website, and/or the dark web, where hackers further disclosed the personal identifying information alleged herein.

257. As a direct and proximate result of Defendant's acts, Plaintiff and the California Subclass Members were injured and lost money or property, including but not limited to the loss of Plaintiff's and California Subclass Members' legally protected interest in the confidentiality and privacy of their personal information, stress, fear, and anxiety, nominal damages, and additional losses described above.

258. Section 1798.150(b) specifically provides that "[n]o [prefiling] notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages."

259. On October 16, 2023, Plaintiff provided Defendant with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). If Defendant

fails to respond, has not cured, or is unable to cure the violation within 30 days thereof, Plaintiff will amend this Complaint to seek all relief available under the CCPA including damages to be measured as the greater of actual damages or statutory damages in an amount up to seven hundred and fifty dollars ($750) per consumer per incident. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

260. Accordingly, Plaintiff and the California Subclass Members by way of this complaint seek actual pecuniary damages suffered as a result of Defendant's violations described herein.

COUNT VI
Violation of the California Customer Records Act,
Cal. Civ. Code §§ 1798.80 *et seq*.
(On Behalf of Plaintiff and the California Subclass)

261. Plaintiff re-alleges and incorporates by reference each and every allegation in this Complaint, as if fully set forth herein.

262. Cal. Civ. Code § 1798.81.5 provides that "[i]t is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

263. Section 1798.81.5(b) further states that: "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to

the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

264. Cal. Civ. Code § 1798.84(b) provides that [a]ny customer injured by a violation of this title may institute a civil action to recover damages." Section 1798.84(e) further provides that "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined."

265. Plaintiff and the California Subclass Members are "customers" within the meaning of Civ. Code § 1798.80(c) and 1798.84(b) because they are individuals who provided personal information to Defendant for the purpose of obtaining a product and/or service, via their employment with Defendant's clients, from Defendant.

266. The personal information of Plaintiff and the California Subclass Members at issue in this lawsuit constitutes "personal information" under § 1798.81.5(d)(1) in that the personal information Defendant collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government

document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

267. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Plaintiff's and California Subclass Members' personal information and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the California Subclass Members. Specifically, Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information of Plaintiff and the California Subclass Members from unauthorized access, destruction, use, modification, or disclosure. Defendant further subjected Plaintiff's and the California Subclass Members' nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant's violation of the duty to implement and maintain

reasonable security procedures and practices appropriate to the nature of the information, as described herein.

268. As a direct and proximate result of Defendant's violation of its duty, the unauthorized access, destruction, use, modification, or disclosure of the personal information of Plaintiff and the California Subclass Members included hackers' access to, removal, deletion, destruction, use, modification, disabling, disclosure and/or conversion of the personal information of Plaintiff and the California Subclass Members by the cyber attackers and/or additional unauthorized third parties to whom those cybercriminals sold and/or otherwise transmitted the information.

269. As a direct and proximate result of Defendant's acts or omissions, Plaintiff and the California Subclass Members were injured and lost money or property including, but not limited to, the loss of Plaintiff's and the California Subclass Members' legally protected interest in the confidentiality and privacy of their personal information, nominal damages, and additional losses described above. Plaintiff seeks compensatory damages as well as injunctive relief pursuant to Cal. Civ. Code § 1798.84(b).

270. Moreover, the California Customer Records Act further provides: "A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or

licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82.

271. Any person or business that is required to issue a security breach notification under the CRA must meet the following requirements under §1798.82(d):

a. The name and contact information of the reporting person or business subject to this section;

b. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

c. If the information is possible to determine at the time the notice is provided, then any of the following:

i. the date of the breach,

ii. the estimated date of the breach, or

iii. the date range within which the breach occurred. The notification shall also include the date of the notice;

d. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

e. A general description of the breach incident, if that information is

possible to determine at the time the notice is provided;

f. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number;

g. If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information.

272. Defendant failed to provide the legally compliant notice under § 1798.82(d) to Plaintiff and members of the California Subclass. On information and belief, to date, Defendant has not sent written notice of the data breach to all impacted individuals. As a result, Defendant has violated § 1798.82 by not providing legally compliant and timely notice to all California Subclass Members. Because not all members of the class have been notified of the breach, members could have taken action to protect their personal information, but were unable to do so because they were not timely notified of the breach.

273. On information and belief, many California Subclass Members affected

by the breach have not received any notice at all from Defendant in violation of Section 1798.82(d).

274. As a result of the violations of Cal. Civ. Code § 1798.82, Plaintiff and California Subclass Members suffered incrementally increased damages separate and distinct from those simply caused by the breaches themselves.

275. As a direct consequence of the actions as identified above, Plaintiff and California Subclass Members incurred additional losses and suffered further harm to their privacy, including but not limited to economic loss, the loss of control over the use of their identity, increased stress, fear, and anxiety, harm to their constitutional right to privacy, lost time dedicated to the investigation of the breach and effort to cure any resulting harm, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal, financial, and payroll information disclosed, that they would not have otherwise incurred, and are entitled to recover compensatory damages according to proof pursuant to § 1798.84(b).

COUNT VII
Violation of the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56, *et seq.*
(On Behalf of Plaintiff and the California Subclass)

276. Plaintiff re-alleges and incorporates by reference each and every allegation in this Complaint, as if fully set forth herein.

277. In Section 56.10(a) of the California Civil Code provides that "[a]

provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization[.]"

278. Defendant is a "contractor" within the meaning of Civil Code § 56.05(d) within the meaning of Civil Code § 56.06 and/or a "business organized for the purpose of maintaining medical information" and/or a "business that offers software or hardware to consumers . . . that is designed to maintain medical information" within the meaning of Civil Code § 56.06(a) and (b), and maintained and continues to maintain "medical information," within the meaning of Civil Code § 56.05(j), for "patients" of Defendant, within the meaning of Civil Code § 56.05(k).

279. Plaintiff and California subclass members are "patients" within the meaning of Civil Code § 56.05(k) and are "endanger[ed]" within the meaning of Civil Code § 56.05(e) because Plaintiff and California subclass members fear that disclosure of their medical information could subject them to harassment or abuse.

280. Plaintiff and California subclass members, as patients, had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), created, maintained, preserved, and stored on Defendant's computer network at the time of the unauthorized disclosure.

281. Defendant, through inadequate security, allowed unauthorized third-party access to Plaintiff's and California subclass members' medical information,

without the prior written authorization of Plaintiff and California subclass members, as required by Civil Code § 56.10 of the CMIA.

282. In violation of Civil Code § 56.10(a), Defendant disclosed Plaintiff's and California subclass members' medical information without first obtaining an authorization. Plaintiff's and California subclass members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.10(a).

283. In violation of Civil Code § 56.10(e), Defendant further disclosed Plaintiff's and California subclass members' medical information to persons or entities not engaged in providing direct health care services to Plaintiff or California subclass members, or to their providers of health care or health care service plans or their insurers or self-insured employers.

284. Defendant violated Civil Code § 56.101 of the CMIA through its willful and knowing failure to maintain and preserve the confidentiality of the medical information of Plaintiff and the California subclass members. Defendant's conduct with respect to the disclosure of confidential PII and PHI was willful and knowing because Defendant designed and implemented the computer network and security practices that gave rise to the unlawful disclosure.

285. In violation of Civil Code § 56.101(a), Defendant created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiff's and class

members' medical information in a manner that failed to preserve and breached the confidentiality of the information contained therein. Plaintiff's and California subclass member' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(a). 380. In violation of Civil Code § 56.101(a), Defendant negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiff's and California subclass members' medical information. Plaintiff's and California subclass members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(a).

286. Plaintiff's and California subclass members' medical information that was the subject of the unauthorized disclosure included "electronic medical records" or "electronic health records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

287. In violation of Civil Code § 56.101(b)(1)(A), Defendant's electronic health record system or electronic medical record system failed to protect and preserve the integrity of electronic medical information. Plaintiff's and California subclass members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(b)(1)(A).

288. Defendant violated Civil Code § 56.36 of the CMIA through its failure

to maintain and preserve the confidentiality of the medical information of Plaintiff and the California subclass members.

289. As a result of Defendant's above-described conduct, Plaintiff and California subclass members have suffered damages from the unauthorized disclosure and release of their individual identifiable "medical information" made unlawful by Civil Code §§ 56.10, 56.101, 56.36. 385.

290. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the unauthorized disclosure, and violation of the CMIA, Plaintiff and California subclass members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia, (i) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud-risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII and PHI, (iv) statutory damages under the California CMIA, (v) deprivation of the value of their PII and PHI, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

291. Plaintiff, individually and for each member of the California Subclass,

seeks nominal damages of one thousand dollars ($1,000) for each violation under Civil Code § 56.36(b)(1), and actual damages suffered, if any, pursuant to Civil Code § 56.36(b)(2), injunctive relief, as well as punitive damages of up to $3,000 per Plaintiff and each California subclass member, and attorneys' fees, litigation expenses and court costs, pursuant to Civil Code § 56.35.

COUNT VIII
Common Law Invasion of Privacy – Intrusion Upon Seclusion
(On Behalf of Plaintiff and the Class)

292. Plaintiff re-alleges and incorporates by reference each and every allegation in this Complaint, as if fully set forth herein.

293. To assert claims for intrusion upon seclusion, one must plead (1) that the defendant intentionally intruded into a matter as to which plaintiff had a reasonable expectation of privacy; and (2) that the intrusion was highly offensive to a reasonable person.

294. Defendant intentionally intruded upon the solitude, seclusion and private affairs of Plaintiff and Class Members by intentionally configuring their systems in such a way that left them vulnerable to malware/ransomware attack, thus permitting unauthorized access to their systems, which compromised Plaintiff's and Class Members' personal information. Only Defendant had control over its systems.

295. Defendant's conduct is especially egregious and offensive as they failed to have adequate security measures in place to prevent, track, or detect in a

timely fashion unauthorized access to Plaintiff's and Class Members' personal information.

296. At all times, Defendant was aware that Plaintiff's and Class Members' personal information in their possession contained highly sensitive and confidential personal information.

297. Plaintiff and Class Members have a reasonable expectation of privacy in their personal information, which also contains highly sensitive medical information.

298. Defendant intentionally configured their systems in such a way that stored Plaintiff's and Class Members' personal information to be left vulnerable to cyber attack without regard for Plaintiff's and Class Members' privacy interests.

299. The disclosure of the sensitive and confidential personal information of thousands of consumers, was highly offensive to Plaintiff and class members because it violated expectations of privacy that have been established by general social norms, including by granting access to information and data that is private and would not otherwise be disclosed.

300. Defendant's conduct would be highly offensive to a reasonable person in that it violated statutory and regulatory protections designed to protect highly sensitive information, in addition to social norms. Defendant's conduct would be especially egregious to a reasonable person as Defendant publicly disclosed

Plaintiff's and Class Members' sensitive and confidential personal information without their consent, to an "unauthorized person," i.e., hackers.

301. As a result of Defendant's actions, Plaintiff and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

302. Plaintiff and Class Members have been damaged as a direct and proximate result of Defendant's intrusion upon seclusion and are entitled to just compensation.

303. Plaintiff and class members are entitled to appropriate relief, including compensatory damages for the harm to their privacy, loss of valuable rights and protections, and heightened stress, fear, anxiety, and risk of future invasions of privacy.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

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

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private

Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

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

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

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

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

iii. Requiring Defendant to delete, destroy, and purge the Private Information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the

retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

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

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

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

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

viii. Requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. Requiring Defendant to conduct regular database scanning and securing checks;

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

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

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

xiv. Requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

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

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

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

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

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

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

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

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

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

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

JURY TRIAL DEMANDED

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

Dated: October 16, 2023

Respectfully submitted,

s/ John J. Nelson

John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Fax: (858) 209-6941
Email: jnelson@milberg.com

Attorney for Plaintiff and the Proposed Class

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: Prospect Medical Holdings Failed to Protect Private Data from Hackers, Class Action Says

---