(Eddie) Jae K. Kim (SBN: 236805)
LYNCH CARPENTER, LLP
117 E Colorado Blvd, Ste 600
Pasadena, CA 91105-3712
Telephone: (213) 723-0707
Facsimile: (858) 313-1850
ekim@lcllp.com

Attorneys for Plaintiff and the Proposed Class
[Additional counsel on signature page]

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

MATTHEW ARDI, individually and on behalf of all others similarly situated,

Plaintiff,

v.

1LIFE HEALTHCARE, INC., d/b/a ONE MEDICAL,

Defendant.

Case No. 3:26-cv-06189

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Matthew Ardi ("Plaintiff") brings this Class Action Complaint on behalf of himself, and all others similarly situated, against Defendant 1Life Healthcare, Inc., d/b/a One Medical ("One Medical" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to Plaintiff, which are based on personal knowledge:

I. NATURE OF THE CASE

1. Plaintiff brings this class action against Defendant One Medical for its failure to properly secure and safeguard Plaintiff's and other similarly situated individuals' ("Class Members") personally identifying information, including demographic information (collectively "PII" or "Private Information").[1]

2. In addition, Plaintiff also brings this class action against One Medical for its failure to properly secure and safeguard Plaintiff's and Class Members' protected health information ("PHI") including patient clinical records.[2]

3. PII and PHI are collectively referred to as "Private Information."

4. One Medical is a membership-based primary care practice owned by Amazon, providing its over 800,000 members with access to services such as routine checkups, mental health support, and chronic disease management nationwide.

5. Plaintiff and Class Members are individuals who were required to indirectly and/or directly provide Defendant with their Private Information. By collecting, storing, and maintaining Plaintiff's and Class Members' Private Information, One Medical has a resulting duty to secure, maintain, protect, and safeguard the Private Information that it collects and stores against unauthorized access and disclosure through reasonable and adequate data security measures.

6. Despite One Medical's duty to safeguard the Private Information of Plaintiff and

[1] Steve Adler, *ShinyHunters Data Extortion Group Threatens to Leak 8.8 TB of Stolen One Medical Data*, The HIPAA Journal (June 22, 2026), https://www.hipaajournal.com/one-medical-data-breach/.

[2] *Id.*

Class Members, their Private Information in Defendant's possession was compromised when a hacker using the online moniker 'ShinyHunters' posted on its dark web data leak website, on or about June 13, 2025, that it stole approximately 8.8 terabytes of sensitive data from Defendant. (the "Data Breach").[3]

7. Upon information and belief, the Data Breach occurred when cybercriminals infiltrated Defendant's inadequately protected network servers and accessed highly sensitive PII that was being kept.

8. In response to the Data Breach, One Medical stated that their "review to date has identified a subset of files containing demographic and clinical records from a certain number of patients at designated One Medical Seniors [] clinics in Atlanta, Cape Cod, Charlotte, Piedmont Triad, Houston, Phoenix, Tucson, and Seattle."[4]

9. Defendant posted an announcement regarding the Data Breach on its website, but has not provided individualized notice advising patients whether, or to what extent, their data was compromised.

10. One Medical maintained the Private Information of Plaintiff and Class Members in a negligent and/or reckless manner. In particular, the Private Information was maintained on One Medical's computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

11. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' Private Information was safeguarded, failing to take

[3] *Id.*
[4] *One Medical Seniors Security Event Notification*, https://www.onemedical.com/security-event-notice/ (last visited June 22, 2026).

available steps to prevent 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.

12. As a result, Plaintiff's and Class Members' Private Information was compromised by an unauthorized third-party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe and are entitled to injunctive and other equitable relief.

13. As a direct and proximate result of Defendant's failure to implement and follow basic security procedures, Plaintiff's and Class Members' Private Information is now in the hands of cybercriminals.

14. Plaintiff and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, intrusion of their health privacy, and similar forms of criminal mischief, risks which may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

15. Plaintiff, on behalf of himself and all others similarly situated, alleges claims for negligence, breach of implied contract, unjust enrichment and violation of the California Confidentiality of Medical Information Act arising from the Data Breach. Plaintiff seeks damages and injunctive relief, including the adoption reasonably sufficient practices to safeguard the Private Information in Defendant's custody to prevent incidents like the Data Breach from reoccurring in the future, and for Defendant to provide identity theft protective services to Plaintiff and Class Members for their lifetimes.

II. PARTIES

16. Plaintiff Matthew Ardi is an adult, who at all relevant times, was a resident and citizen of the state of Illinois.

17. Plaintiff has suffered actual injury from having his Private Information exposed and/or stolen as a result of the Data Breach, including: (a) required mitigation efforts, including researching the Data Breach and needing to monitor his financial statements to ensure his

information is not used for identity theft and fraud; (b) damages to and diminution of the value of his Private Information, a form of intangible property that loses value when it falls into the hands of criminals; (c) loss of privacy; and (d) continuous imminent and impending injury raising from increased risk of financial identity theft and fraud.

18. As a result of the Data Breach, and the sensitivity of the Private Information compromised, Plaintiff will continue to be at a substantial and certainly impending risk for fraud and identity theft, and their attendant damages, for years to come.

19. Defendant 1Life Healthcare, Inc., d/b/a One Medical is a Delaware corporation with its principal place of business at One Embarcadero Center, Suite 1900, San Francisco, CA 94111.

III. JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class is a citizen of a state different than Defendant.[5]

21. This Court has personal jurisdiction over Defendant because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District and Defendant resides in this District.

22. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District and Defendant resides in this District.

IV. FACTUAL BACKGROUND

23. Defendant operates a membership-based primary care practice that offers patients

[5] *See* 28 U.S.C. § 1332(d)(10) (stating that for purposes of CAFA jurisdiction, an unincorporated association deemed to be citizen of State where it has its principal place of business and under whose laws it is organized).

access to healthcare services through both telehealth appointments and in-person office visits, including routine primary care, preventive care, and treatment or management of ongoing health conditions.

24. Plaintiff and Class Members are and/or were patients of Defendant.

25. As a condition of obtaining Defendant's services, Plaintiff and Class Members directly or indirectly entrusted One Medical with their sensitive Private Information.

26. Plaintiff and Class Members value the confidentiality of their Private Information and, accordingly, have taken reasonable steps to maintain the confidentiality of their Private Information.

27. In entrusting their Private Information to Defendant, Plaintiff and Class Members reasonably expected that Defendant would safeguard their highly sensitive information.

28. By obtaining, collecting, and storing Plaintiff's and Class Members' Private Information, One Medical assumed equitable and legal duties to safeguard Plaintiff's and Class Members' highly sensitive information, to only use this information for business purposes, and to only make authorized disclosures.

29. Despite these duties, One Medical failed to implement reasonable data security measures to protect Plaintiff's and Class Members' Private Information and ultimately allowed threat actors to breach its computer systems and exfiltrate Plaintiff's and Class Members' Private Information stored therein.

A. THE VALUE OF PRIVATE INFORMATION AND EFFECTS OF UNAUTHORIZED DISCLOSURE

30. One Medical understood that the Private Information it collects was highly sensitive and of significant value to those who would use it for wrongful purposes.

31. One Medical also knew that a breach of its computer systems, and exposure of the Private Information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose Private Information was compromised.

32. These risks are not theoretical; in recent years, numerous high-profile breaches

have occurred at business such as Equifax, Facebook, Yahoo, Marriott, Anthem, and many others.

33. Private Information has considerable value and constitutes an enticing and well-known target to hackers. Hackers can easily sell stolen data as there has been "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[6]

34. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud.[7] The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individual, businesses, and government entities in the U.S. In 2024, there were 6,670 publicly disclosed data breaches, exposing 16.8 billion records. The United States specifically saw a 12% increase in the total number of data breaches.[8]

35. Indeed, a 2022 poll of security executives predicted an increase in attacks over the next two years from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[9]

36. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 6.5 million people in 2024.[10]

---

[6] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/ (last visited June 22, 2026).
[7] *What To Know About Identity Theft*, FTC Consumer Advice (Sept. 2024), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited June 22, 2026).
[8] *2025 Global Threat Intelligence Report*, Flashpoint (Mar. 18, 2025), https://go.flashpoint.io/2025_GTIR (last visited June 22, 2026).
[9] Chuck Brooks, *Alarming Cyber Statistics For Mid-Year 2022 That You Need to Know*, Forbes (June 3, 2022), https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last visited June 22, 2026).
[10] *Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited June 22, 2026).

37. Artificial Intelligence ("AI") is also reshaping the cybersecurity landscape. "AI-related [common vulnerabilities and exposures] have surged, with 2,130 disclosed in 2025 alone –a 34.6% year-over-year increase."[11] Further, 16% of all breaches in 2025 involved attackers using AI.[12]

38. The ramifications of One Medical's failure to keep Plaintiff's and Class Members' Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[13]

39. The exposure of highly sensitive personal information creates ongoing risk because "when highly sensitive types of data are exposed, the breach is only the beginning."[14] That risk persists as "[e]very breach feeds an underground ecosystem of exposed data. When attackers obtain highly sensitive identity credential, they rarely use them just once. Instead, they combine information from multiple breaches to construct detailed identity profiles that can be exploited many time across different fraud scheme."[15]

---

[11] Peter Girnus et al., *Fault Lines in the AI Ecosystem: TrendAI State of AI Security Report*, Trend Micro (Mar. 3, 2026), https://www.trendmicro.com/vinfo/us/security/news/threat-landscape/ fault-lines-in-the-ai-ecosystem-trendai-state-of-ai-security-report (last visited June 22, 2026).

[12] *Cost of a Data Breach Report 2025*, IBM (2025), https://www.ibm.com/downloads/documents/us-en/131cf87b20b31c91 (last accessed June 22, 2026)

[13] *Report to Congressional Requesters, Personal Information, June 2007*, U.S. Gov't Accountability Office, https://www.gao.gov/new.items/d07737.pdf, (last visited June 22, 2026).

[14] Matt Cullina, *Small Breaches, Big Consequences*, Forbes (June 10, 2026), https://www.forbes.com/councils/forbesbusinesscouncil/2026/06/10/small-breaches-big-consequences/ (last visited June 22, 2026).

[15] *Id.*

40. Even if stolen Private Information does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

41. Although spear phishing attacks "make up only 0.1% of all email-based attacks," their outstanding impact is reflected in the fact that "2 out of 3 successful email attacks are spear phishing attacks that use personalized messages, social engineering, and other tactics."[16]

42. A company does not become less likely to experience another breach simply because it has already experienced one; to the contrary, "[o]nce hackers realize an organization is vulnerable to an attack, they will repeatedly attempt to breach its network[.]" Further, "95% of organizations surveyed by IBM between March 2022 and March 2023 said they had experienced more than on data breach."[17]

43. Other research indicates that "[t]wo-thirds of companies that experience cyberattack are hit again within a year. These successive incidents can play out in multiple ways: simultaneously, a few days apart, or many months later."[18]

44. "It can take an average of 277 days - that's about nine months – for an organization to identify and contain a breach. During that extended period of time, not only might cybercriminal remain in the environment wreaking havoc, but the means by which they entered remains available

---

[16] *Market Report: 2023 Spear-Phishing Trends*, Barracuda (May 24, 2023), https://assets.barracuda.com/assets/docs/dms/2023-spear-phishing-trends.pdf (last visited June 22, 2026).

[17] Beth Stackpole, *MIT Report Details New Cybersecurity Risks*, MIT Sloan (Apr. 30, 2024), https://mitsloan.mit.edu/ideas-made-to-matter/mit-report-details-new-cybersecurity-risks (last visited June 22, 2026).

[18] Neil Clauson, *When Cyberattackers Strike Again – and Again*, Mimecast (Nov. 13, 2024), https://www.mimecast.com/blog/when-cyberattackers-strike-again----and-again/ (last visited June 22, 2026).

to others as well."[19]

45. The specific types of personal data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiff and other Class Members especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

46. Based on the value of Plaintiff's and Class Members' Private Information to cybercriminals, One Medical knew or should have known the importance of safeguarding the Private Information entrusted to it and of the foreseeable consequences if its data security systems were breached. One Medical failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

B. ONE MEDICAL BREACHED ITS DUTY TO PROTECT PLAINTIFF'S AND CLASS MEMBERS' PRIVATE INFORMATION

47. On or around June 13, 2026, One Medical was the target of a cybersecurity incident that compromised its data network.

48. The Private Information exfiltrated in the Data Breach includes, at the very least, demographic information and patient clinical records.

49. One Medical has issued a public announcement of the Data Breach on their website, but has not issued, and does not appear to have issued, any notification or disclosure to affected individuals or regulatory authorities regarding the Data Breach, including any explanation of the scope, nature, or potential consequences of the compromise.

50. Based on Defendant's announcement of the Data Breach the cyberattack was expressly designed to gain access to private and confidential data of specific individuals, including (among other things) the Private Information of Plaintiff and the Class Members and that the cybercriminals were successful in exfiltrating sensitive information from Defendant's data network.

51. The exact number of individuals affected by the Data Breach has not been publicly

[19] *Id.; see also Cost of a Data Breach*, *supra* n.12.

disclosed.

52. The Data Breach occurred as a direct result of One Medical's failure to implement and follow basic security procedures to protect its current and former patients' Private Information that it had collected and stored.

C. ONE MEDICAL FAILED TO COMPLY WITH FTC GUIDELINES

53. One Medical is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

54. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[20]

55. Among other guidance, the FTC recommends the following cybersecurity guidelines for businesses in order to protect sensitive information in their systems: [21]

a. Identify all connections to the computers where sensitive information is stored;

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;

d. Scan computers on their network to identify and profile the operating

[20] *Start with Security – A Guide for Business*, United States Federal Trade Comm'n (Aug. 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/920a_start_with_security_en_aug2023_508_final_0.pdf (last visited June 22, 2026).

[21] *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 22, 2026).

system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;

e. Pay particular attention to the security of their web applications - the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks;

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet;

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls -settings that determine which devices and traffic get through the firewall - to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a

business's network, the transmission should be investigated to make sure it is authorized.

56. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private 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.[22]

57. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

58. One Medical failed to properly implement basic data security practices. One Medical's failure to employ reasonable and appropriate measures to protect against unauthorized access to its patients' Private Information constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

59. One Medical was at all times fully aware of its obligations to protect the Private Information of its patients given the reams of Private Information that it had access to as Plaintiff's and the Class Members' service provider. One Medical was also aware of the significant repercussions that would result from a failure to properly secure the Private Information it maintained.

D. ONE MEDICAL'S FAILURE TO PREVENT, IDENTIFY, AND TIMELY REPORT THE DATA BREACH

60. One Medical failed to take necessary precautions and failed to employ adequate measures necessary to protect its computer systems against unauthorized access and keep

[22] *Id.*

Plaintiff's and Class Members' Private Information secure.

61. The Private Information that One Medical allowed to be exposed in the Data Breach is the type of private information that One Medical knew or should have known would be the target of cyberattacks.

62. Despite its own knowledge of the inherent risks of cyberattacks, and notwithstanding the FTC's data security principles and practices,[23] One Medical failed to disclose that its systems and security practices were inadequate to reasonably safeguard individuals' Private Information.

63. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.[24] Immediate notification to individuals impacted by a data breach is critical so that those impacted can take measures to protect themselves.

64. Here, One Medical has acted inexcusable by failing to provide timely notice to the individuals whose personal information was compromised in the Data Breach, despite its knowledge of the incident and its obligations to safeguard such information.

65. Plaintiff and Class Members remain in the dark regarding what data was stolen, the particular malware used, and what steps are being taken to secure their Private Information in the future. Thus, Plaintiff and Class Members are left to speculate as to where their Private Information ended up, who has used it, and for what potentially nefarious purposes. Indeed, they are left to further speculate as to the full impact of the Data Breach and how Defendant intends to enhance its information security systems and monitoring capabilities to prevent further breaches.

E. THE DATA BREACH'S INCLUSION OF PHI IS PARTICULARLY SIGNIFICANT

66. With respect to the data breaches implicating PHI, a study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or

[23] *Protecting Personal Information: A Guide for Business*, Fed. Trade Comm'n (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited June 22, 2026).

[24] *Id.*

identity theft."[25]

67. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[26]

68. The reality is that cybercriminals seek nefarious outcomes from a data breach and "stolen health data can be used to carry out a variety of crimes."[27]

69. Health information in particular is likely to be used in detrimental ways – by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[28]

70. "These ransomware groups have established healthcare as a target vertical due to the critical nature of health data and the perceived willingness of healthcare organizations to pay ransoms to avoid disruption of patient care and regulatory consequences under frameworks such as HIPAA."[29]

71. Health information "remains one of the most valuable commodities in the cybercriminal underground due to its permanence, sensitivity and ability to support multiple forms of fraud simultaneously."[30]

---

[25] *70% Of Data Involved In Healthcare Breaches Increases Risk Of Fraud*, DistilINFO (Oct. 3, 2019), https://distilgovhealth.com/2019/10/03/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud/ (last visited June 22, 2026).

[26] *Id.*

[27] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HealthTech (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited June 22, 2026).

[28] *Id.*

[29] Stephen Hilt et al., *The Cybercriminal Underground: Mapping the Healthcare Data Economy*, TrendAI (June 4, 2026), https://www.trendaisecurity.com/en-us/resources-insights/research/the-cybercriminal-underground-mapping-the-healthcare-data-economy (last visited June 22, 2026).

[30] Sarah Weston, *Healthcare Data Has Become One of Cybercrime's Most Valuable Commodities*, Intelligent CISO (June 9, 2026), https://www.intelligentciso.com/2026/06/09/healthcare-data-has-become-one-of-cybercrimes-most-valuable-commodities/ (last visited June 22, 2026).

72. Cybersecurity threat researchers warn that, "[w]hat we're seeing is not isolated cybercrime, but a mature underground economy built around healthcare." Health information has become such a valuable commodity that, "[i]nitial access brokers, ransomware affiliates, credential sellers and fraud specialists now operate as a part of an interconnected supply chain designed to monetize patient data repeatedly and at scale."[31]

73. As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals - they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to - we've even seen $60 or $70."[32]

74. The "high value of medical records on the dark web has surpassed that of social security and credit card numbers. These records can sell for up to $1,000 online . . ."[33]

75. Specialized medical records carry an even higher price. For example, "oncology medical records can be worth between $950 and $2,000 per patient, and genomic data alone can command $1,700 to $5,000. When genomic data is linked with phenotypic data…the value can exceed $6,000."[34]

76. Cybercriminals sell health information at a far higher premium than stand-alone PII. This is because health information enables thieves to go beyond traditional identity theft and obtain medical treatments, purchase prescription drugs, submit false bills to insurance companies, or even undergo surgery under a false identity. The shelf life for this information is also much longer—while individuals can update their credit card numbers, they are less likely to change their

---

[31] *Id.*

[32] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, IDX (May 14, 2015), https://www.idx.us/knowledge-center/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat (last accessed June 22, 2026).

[33] Steger, *supra* n.27.

[34] Seth Joseph, *What Is Your Health Record Worth? The Unseen Economics Behind Your Medical Data*, Forbes (Aug. 20, 2025), https://www.forbes.com/sites/sethjoseph/2025/08/20/what-is-your-health-record-worth-the-unseen-economics-behind-your-medical-data/ (last accessed June 22, 2026).

health insurance information. When medical identity theft occurs, the associated costs to victims can be exorbitant. According to a 2015 study, at least 65% of medical identity theft victims had to "pay an average of $13,500 to resolve the crime."[35]

77. As noted above, some of the information that was compromised in the Data Breach included, among other things, "demographic and clinical records."[36] Accordingly, Plaintiff and Class Members must remain especially vigilant given the highly sensitive nature of the PHI at issue in this Data Breach.

F. ONE MEDICAL FAILED TO COMPLY WITH HIPAA'S MANDATES

78. Defendant is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and 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. In addition, One Medical is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

80. HIPAA's Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information, while HIPAA's Security Standards for the Protection of Electronic Protected Health Information establishes national security standards for health information that is stored or transmitted electronically.

81. 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. Such health information includes "individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media."

---

[35] Justin Klawans, *What is medical identity theft and how can you avoid it?*, The Week (Aug. 2, 2023), https://theweek.com/feature/briefing/1025328/medical-identity-theft-how-to-avoid.

[36] *See One Medical Seniors Security Event Notification*, https://www.onemedical.com/security-event-notice/ (last visited June 22, 2026).

45 C.F.R. § 160.103.

82. HIPAA's Security Rule requires entities such as One Medical to, *inter alia*, do the following: (i) ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits; (ii) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (iii) protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and (iv) ensure compliance by its workforce.

83. HIPAA also requires entities such as One Medical 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, One Medical is required under HIPAA to "[i]implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

84. Moreover, both HIPAA and HITECH required One Medical 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.

85. Finally, HIPAA requires an entity to provide notice of a data breach to affected individuals "without unreasonable delay and in no case later than 60 days following discovery of the breach." 45 C.F.R. §§ 164.400-414.

86. One Medical was, at all times, aware of the mandates of HIPAA. Despite being aware of these mandates and its concomitant obligations, One Medical failed to comply with its obligations and protect the PHI of Plaintiff and the Class Members.

87. Defendant's failure in this regard is especially egregious given that Defendant was fully aware of the breadth and depth of PHI it obtained and stored and the foreseeable

consequences that would result from unauthorized disclosure of this information.

G. PLAINTIFF AND CLASS MEMBERS SUFFERED DAMAGES

88. The ramifications of One Medical's failure to keep Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

89. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct. Further, the value of Plaintiff's and Class Members' Private Information has been diminished by its exposure in the Data Breach.

90. PII remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, credit card information can be sold at a price ranging from $10 to $240, and bank details have a price range of $30 to $4,255.[37] "Fullz" packages, which includes "extra information about the legitimate credit card owner in case" the scammer's "bona fides are challenged when they attempt to use the credit card" are also offered on the dark web.[38]

91. Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their Private Information as a result of the Data Breach. A recent study found that "[v]ictims of identity theft (24%) were twice as likely as nonvictims (11%) to learn that an entity with their personal information experienced a data breach in the past year."[39]

92. Further, Plaintiff and Class Members have incurred and will incur out of pocket

---

[37] Ben Luthi, *Here's What Your Data Sells for on the Dark Web, Experian* (June 30, 2025), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited June 22, 2026).

[38] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web, Armor* (Apr. 3, 2018), https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited June 22, 2026).

[39] Erika Harrell, *Just the Stats: Data Breach Notifications and Identity Theft, 2021*, Bureau of Justice Statistics (Jan. 2024), https://bjs.ojp.gov/data-breach-notifications-and-identity-theft-2021 (last visited June 22, 2026).

costs for protective measures, such as identity theft protection, credit monitoring, credit report fees, credit freeze fees, and similar costs related to the Data Breach.

93. Besides the monetary damage sustained in the event of identity theft, consumers may have to spend hours trying to resolve identity theft issues. For example, the FTC estimates that it takes consumers an average of 200 hours of work over approximately six months to recover from identity theft.[40]

94. Plaintiff and Class Members are also at a continued risk because their information remains in One Medical's systems, which the Data Breach showed are susceptible to compromise and attack and are subject to further attack so long as One Medical fails to take necessary and appropriate security and training measures to protect the Private Information in its possession.

95. Plaintiff and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their Private Information to strangers.

96. As a result of One Medical's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer injuries, including out of pocket expenses; loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the Data Breach; theft of their valuable Private Information; the imminent and certainly impeding injury flowing from fraud and identity theft posed by their Private Information being disclosed to unauthorized recipients and cybercriminals; damages to and diminution in value of their Private Information; and continued risk to Plaintiff's and the Class Members' Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as One Medical fails to undertake appropriate and adequate measures to protect the Private Information entrusted to it.

97. Furthermore, Defendant has not offered identity theft monitoring and/or identity

[40] Kathryn Parkman, *How to Report identity Theft*, ConsumerAffairs (Feb. 17, 2022), https://www.consumeraffairs.com/finance/how-to-report-identity-theft.html (last visited June 22, 2026).

theft protection for its patients. This lack of resolution is inadequate when the victims will likely face many years of identity theft.

98. The absence of and/or limited duration of these services is wholly inadequate as they fail to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and they entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

V. CLASS ALLEGATIONS

99. Plaintiff brings this class action on behalf of himself and all other individuals who are similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure.

100. Plaintiff seeks to represent a class of persons to be defined as follows:

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

101. Excluded from the Class are One Medical, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

102. This proposed class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the class definition in an amended pleading or when he moves for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

103. **Numerosity:** Plaintiff is informed and believes, and thereon alleges, that there are at minimum, tens of thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendant's records, including but not limited to the files implicated in the Data Breach.

104. **Commonality:** This action involved questions of law and fact common to the Class. Such common questions include but are not limited to:

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

b. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' Private Information, and breached its duties thereby;

c. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct; and

d. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

105. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiff and members of the Class were all patients of Defendant, and each had their Private Information exposed and/or accessed by an unauthorized third-party.

106. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the members of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and has no interests antagonistic to the members of the Class. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class Members are substantially identical as explained above.

107. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

108. **Predominance:** Common questions of law and fact predominate over any

questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages are common to Plaintiff and each member of the Class. If Defendant breached its duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

109. **Injunctive Relief:** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. R. Civ. P. 23(b)(2).

110. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria, and Class Members may be readily identified through Defendant's books and records.

VI. CLAIMS FOR RELIEF

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

111. Plaintiff re-alleges the above allegations as if fully set forth herein.

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

113. Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in securing, safeguarding, storing, and protecting the PII and PHI it collected from them as a condition of obtaining services from One Medical from being compromised, lost, stolen, accessed and misused by unauthorized parties. This duty includes, among other things, designing, maintaining, overseeing, and testing Defendant's security systems to ensure that PII and PHI in One Medical's possession was adequately secured and protected.

114. 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 their Private Information

were wrongfully disclosed.

115. Defendant owed a duty of care to Plaintiff and Class Members to provide reasonable security, consistent with industry standards, to ensure that its systems and networks adequately protected their Private Information.

116. Defendant had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust One Medical with their Private Information as a condition of obtaining services was predicated on the understanding that One Medical would take adequate security precautions to protect their PII and PHI.

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

118. Plaintiff and members of the Class entrusted Defendant with their PII and PHI with the understanding that One Medical would safeguard their information.

119. Defendant's conduct also created a foreseeable risk of harm to Plaintiff and Class Members by failing to: (1) secure its systems and exercise adequate oversight of its data security protocols; (2) ensure compliance with industry standard data security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent the Data Breach.

120. Defendant knew, or should have known of, the risks inherent in collecting and storing PII and PHI, the vulnerabilities of its systems, and the importance of adequate security. Defendant should have been aware of numerous, well-publicized data breaches in the months and years preceding the Data Breach.

121. Defendant breached its common law duty to act with reasonable care in collecting and storing the Private Information of its patients, which exists independently from any contractual obligations between the parties. Specifically, Defendant breached its common law, statutory, and other duties to Plaintiff and Class Members in numerous ways, including by:

a. failing to adopt reasonable data security measures, practices, and protocols;

b. failing to implement data security systems, practices, and protocols sufficient to protect Plaintiff's and Class Members' PII and PHI;

c. storing former patients' PII and PHI longer than reasonably necessary;

d. failing to comply with industry-standard data security measures; and

e. failing to timely disclose critical information regarding the nature of the Data Breach.

122. Defendant's failure to implement and maintain adequate data security measures to protect Plaintiff's and Class Members' Private Information created conditions conducive to a foreseeable, intentional criminal act in the form of the Data Breach. Plaintiff and Class Members did not contribute to the Data Breach or the subsequent misuse of their Private Information.

123. 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 their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

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

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

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

127. 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 Class Members.

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

129. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have and will suffer damages including, but not limited to: (i) the loss of value of their Private Information and loss of opportunity to determine for themselves how their PII and PHI is used; (ii) the publication and/or theft of their PII and PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII and PHI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as One Medical fails to undertake appropriate and adequate measures to protect it; and (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised for the rest of their lives.

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

131. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy;

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

132. 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.

133. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the FTC 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.

134. Defendant's violation of federal statutes, including the FTC Act and HIPAA, constitutes negligence *per se*.

135. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, 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 fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

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

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

137. Plaintiff re-alleges the above allegations as if fully set forth herein.

138. In connection with obtaining services from Defendant, Plaintiff and Class Members entered into implied contracts with One Medical.

139. Plaintiff and Class Members were required to deliver their Private Information to Defendant as part of the process of obtaining services from Defendant.

140. Defendant solicited, offered, and invited Class Members to provide their Private Information in order to obtain services at Defendant's. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

141. Defendant accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services to Plaintiff and Class Members.

142. When Plaintiff and Class Members provided their PII and PHI to One Medical, either directly or indirectly, as a pre-condition for obtaining services, they entered into implied contracts with One Medical.

143. Pursuant to these implied contracts, in exchange for the consideration and PII and PHI provided by Plaintiff and Class Members, Defendant agreed to, among other things, and Plaintiff and Class Members understood that One Medical would: (1) provide products and/or services to Plaintiff and Class Members; (2) implement reasonable measures to protect the security and confidentiality of Plaintiff's and Class Members' PII and PHI; and (3) protect Plaintiff's and Class Members' PII and PHI in compliance with federal and state laws and regulations and industry standards.

144. 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.

145. Implicit in the agreement between Plaintiff and Class Members and Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for

business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide 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, and (f) retain the Private Information only under conditions that kept such information secure and confidential.

146. The protection of PII and PHI was a material term of the implied contracts between Plaintiff and Class Members, on the one hand, and Defendant, on the other hand. Indeed, as set forth herein, Defendant recognized its duty to provide adequate data security and ensure the privacy of its patients' PII and PHI with its practice of providing a privacy policy on its website.

147. Plaintiff and Class Members performed their obligations under the implied contract when they provided Defendant with their PII and PHI.

148. Defendant breached its obligations under its implied contracts with Plaintiff and Class Members in failing to implement and maintain reasonable security measures to protect and secure their PII and PHI, and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class Members' PII and PHI in a manner that complies with applicable laws, regulations, and industry standards.

149. 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.

150. 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.

151. 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.

152. 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.

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

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

155. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their Private 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 Private Information was compromised as a result of the Data Breach.

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

157. Defendant's breach of its obligations of its implied contracts with Plaintiff and Class Members directly resulted in the Data Breach and the injuries that Plaintiff and Class Members have suffered from the Data Breach.

158. Plaintiff and Class Members suffered by virtue of Defendant's breach of their implied contracts because: (i) they paid for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft - risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII and PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII and PHI has been breached; (v) they were deprived of the value of their PII and PHI, for which there is a well-established national and international market; (vi) they have lost time and incurred expenses, and

will incur future costs to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) they have overpaid for the services they received without adequate data security.

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

160. 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
(On Behalf of Plaintiff and the Class)

161. Plaintiff re-alleges the above allegations as if fully set forth herein.

162. This count is plead in the alternative to the breach of implied contract count above.

163. By its wrongful acts and omissions described herein, Defendant has obtained a benefit by unduly taking advantage of Plaintiff and Class Members.

164. Plaintiff and Class Members conferred a benefit on Defendant, whereby they provided their Private Information to Defendant to obtain services.

165. Defendant prior to and at the time Plaintiff and Class Members entrusted it with their PII and PHI, caused Plaintiff and Class Members to reasonably believe that it would keep that Private Information secure.

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

167. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and accepted and retained that benefit by accepting and retaining the Private Information entrusted to

it. Defendant profited from Plaintiff's retained data and used Plaintiff's and Class Members' Private Information for business purposes.

168. Defendant failed to disclose facts pertaining to its substandard information systems, or defects and vulnerabilities therein before Plaintiff and Class Members made their decisions to provide Defendant with their Private Information.

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

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

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

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

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

174. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which Plaintiff and Class Members may seek restitution or compensation.

COUNT IV
VIOLATION OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT ("CMIA")
Cal. Civ. Code §§ 56, et seq.
(On Behalf of Plaintiff and the Class)

175. Plaintiff re-alleges all preceding allegations above as if fully set forth herein.

176. Under California's Confidentiality of Medical Information Act ("CMIA"), "persons receiving health care services have a right to expect that the confidentiality of individual identifiable medical information derived by health service providers be reasonably preserved . . . [and it] is the intention of the Legislature in enacting this act, to provide for the confidentiality of individually identifiable medical information, while permitting certain reasonable and limited uses of that information. Cal. Civ. Code Div. 1, Pt. 2.6.

177. Furthermore, "[e]very provider of health care, health care service plan, pharmaceutical company, or contractor who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein." Cal. Civ. Code § 56.101(a).

178. And "[a]ny provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided[.]" Cal. Civ. Code § 56.101(a).

179. Thus, "an individual may bring an action against a person or entity who has negligently released confidential information or records concerning him or her[.]" Cal. Civ. Code § 56.36(b).

180. Here, Defendant is subject to the CMIA because Defendant is a contractor for a provider of health care. And Defendant created, maintained, preserved, stored, abandoned, destroyed, and/or disposed of medical information regarding Plaintiff and the Class.

181. But Defendant was negligent because it failed to take reasonable precautions to ensure its data systems were protected. As a result of Defendant's negligence, an unauthorized third party viewed and obtained the medical information of Plaintiff and the Class.

182. As such, Defendant is therefore liable for damages in an amount to be determined at trial, but not less than the statutorily provided nominal damages of $1,000 for each class member.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

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

B. For equitable relief enjoining One Medical from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII and PHI, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For equitable relief compelling One Medical to utilize appropriate methods and policies with respect to patient data collection, storage, and safety, and to disclose with specificity the types of PII and PHI compromised as a result of the Data Breach;

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

E. Ordering One Medical to pay for not less than ten years of credit monitoring services for Plaintiff and Class Members;

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

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

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

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

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

JURY TRIAL DEMANDED

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

Dated: June 22, 2026

Respectfully submitted,

LYNCH CARPENTER, LLP

/s/ (Eddie) Jae K. Kim
(Eddie) Jae K. Kim (SBN: 236805)
117 E. Colorado Blvd, Suite 600
Pasadena, CA 91105-3712
Telephone: (213) 723-0707
Facsimile: (858) 313-1850
ekim@lcllp.com

-and-

Gerald D. Wells, III (SBN: 257496)
1760 Market Street, Suite 600
Philadelphia, PA 19103
T: 267-609-6910
jerry@lcllp.com

Attorneys for Plaintiff and the Proposed Class