Robert C. Schubert (S.B.N. 62684)
(rschubert@sjk.law)
Amber L. Schubert (S.B.N. 278696)
(aschubert@sjk.law)
Sonum Dixit (S.B.N. 353395)
(sdixit@sjk.law)
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, California 94123
Telephone: (415) 788-4220
Facsimile: (415) 788-0161

Counsel for Plaintiff Donna Sanders and the Putative Class

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO / OAKLAND DIVISION

DONNA SANDERS, 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-7053

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

Upon personal knowledge as to her own acts, and based upon her investigation, the investigation of counsel, and information and belief as to all other matters, Plaintiff Donna Sanders, on behalf of herself and all others similarly situated, alleges as follows:

SUMMARY OF THE ACTION

1. Plaintiff brings this class action against 1Life Healthcare, Inc., d/b/a One Medical ("Defendant" or "One Medical") for its failure to adequately secure and safeguard her and at least thousands of other individuals' personally identifying information ("PII") and protected health information ("PHI") (together, "Private Information"), including demographic and clinical records.

2. One Medical is a primary care provider that Amazon purchased for $3.9 billion in 2023.[1]

3. One Medical acquired Iora Health in 2021, and "inherited Iora's patient data, its vendor relationships, and every HIPAA obligation attached to them," according to Baxter Lee, president of security firm Clearwater.[2]

4. An unauthorized party gained access to third-party file storage systems owned by One Medical between June 8, 2026, and June 11, 2026.[3]

5. Cybercriminal group ShinyHunters has claimed credit for the Data Breach, and claimed to have exfiltrated 8.8 terabytes of data.[4]

6. The Data Breach reportedly affected an undisclosed number of "Iora Health/One Medical Seniors patients in Atlanta, Cape Cod, Charlotte, Piedmont Triad, Denver, Houston, Phoenix, Tucson, and Seattle."[5]

[1] Andrea Fox, *One Medical-owned legacy systems breached in cyberattack*, HEALTHCARE IT NEWS (JUN. 24, 2026), https://www.healthcareitnews.com/news/one-medical-owned-legacy-systems-breached-cyberattack (last visited July 9, 2026).

[2] *Id.*

[3] *Id.*

[4] Steve Alder, *ShinyHunters Data Extortion Group Threatens to Leak 8.8 TB of Stolen One Medical Data*, THE HIPAA J. (JUN. 22, 2026), https://www.hipaajournal.com/one-medical-data-breach/ (last visited July 9, 2026).

[5] *Id.*

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

7. The Data Breach was directly and proximately caused by Defendant's failure to implement reasonable and industry-standard data security practices necessary to protect its systems from a foreseeable and preventable cyberattack. Through this wrongful conduct, the sensitive Private Information of thousands of individuals is now in the hands of cybercriminals, who target this sensitive data for its value to identity thieves. Plaintiff and Class Members are now at a significantly increased and impending risk of fraud, identity theft, and similar forms of criminal mischief—risks which may last 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. Moreover, Plaintiff and Class Members have lost the inherent value of their private data.

8. By aggregating information obtained from the Data Breach with other sources or other methods, criminals can assemble a full dossier of private information on an individual to facilitate a wide variety of frauds, thefts, and scams. Criminals can and do use victims' names and other personal information to open new financial accounts, incur credit charges, obtain government benefits and identifications, fabricate identities, and file fraudulent tax returns well before the person whose Private Information was stolen becomes aware of it. Any one of these instances of identity theft can have devastating consequences for the victim, causing years of often irreversible damage to their credit scores, financial stability, and personal security.

9. Despite knowing that the Data Breach occurred in June 2026, Defendant has not publicly disclosed the number of individuals affected or exact data exfiltrated beyond demographic information and clinical records. Defendant has not informed Plaintiff and Class Members how many people were impacted, how the cybercriminals accessed Defendant's systems and the root cause of the Data Breach, whether the exfiltrated information was encrypted or anonymized, why it took so long to notify victims, or what specific remedial steps Defendant has taken to safeguard Private Information within its systems and networks (or otherwise purge unnecessary information) and to prevent further cyberattacks going forward. Without these critical details, Plaintiff and Class Members cannot meaningfully mitigate the resulting effects of the Data Breach.

10. Plaintiff is a Data Breach victim and received a notification of the Data Breach from Defendant on or around June 29, 2026.

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

11. As a result of Defendant's conduct and the resulting Data Breach, Plaintiff's and Class Members' privacy has been invaded, their Private Information is now in the hands of criminals, they have either suffered or will suffer fraud or identity theft, or face an imminent and ongoing risk of identity theft and fraud. Accordingly, these individuals now must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

12. Plaintiff, on behalf of herself and all others similarly situated, herein alleges claims for negligence and breach of implied contract. Plaintiff on behalf of herself and the Class, seeks: (i) actual damages, economic damages, and nominal damages; (ii) fees and costs of litigation; (iii) injunctive relief, including the adoption of reasonably sufficient practices to safeguard Private Information in Defendant's custody, care, and control in order to prevent incidents like the Data Breach from recurring in the future and for Defendant to provide long-term identity theft protective services to Plaintiff and Class Members; and (iv) such other relief as the Court deems just and proper.

PARTIES

A. Plaintiff

13. Plaintiff Donna Sanders is a resident and citizen of Arizona.

B. Defendant

14. Defendant 1Life Healthcare, Inc. is a Delaware corporation with its principal place of business located at One Embarcadero Center, Floor 19, San Francisco, California 94111.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because at least one member of the putative Class, as defined below, is a citizen of a state other than that of Defendant, there are more than 100 putative Class Members, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs.

16. This Court has general personal jurisdiction over Defendant because it maintains its principal place of business in San Francisco, California, and regularly conducts business in California, and has sufficient minimum contacts in California, such as to not offend traditional notions of fair play and substantial justice.

17. Venue in this District is proper under 28 U.S.C. § 1391 because One Medical resides in this District and a substantial part of the conduct giving rise to Plaintiff's claims occurred in this District, including Defendant collecting or storing the Private Information of Plaintiff and the putative Class Members.

18. Divisional Assignment: This action arises in San Francisco County, in that a substantial part of the events which give rise to the claims asserted herein occurred in San Francisco County, where One Medical is headquartered and located. Pursuant to L.R. 3-2(d), all civil actions that arise in San Francisco County shall be assigned to the San Francisco or Oakland Division.

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

FACTUAL BACKGROUND

A. One Medical Collects, Stores, and Maintains Personally Identifiable Information

19. "One Medical is a primary care practice on a mission to make getting quality care more affordable, accessible, and enjoyable for all through a blend of human-centered design, technology, and an exceptional team."[6]

20. One Medical provides "preventive and everyday health visits, chronic care management, pediatric and mental health services."[7]

21. One Medical operates in 19 U.S. cities, and also works with 8,500 companies to provide One Medical health benefits to employees.[8]

22. On September 1, 2021, One Medical acquired Iora Health.[9]

23. On February 22, 2023, Amazon completed acquisition of One Medical.[10]

24. One Medical's Frequently Asked Questions has the following response to the question, "What can I do if I have questions about privacy and security?":

> We take the security and confidentiality of your personal information seriously." We follow industry best practices in software development and testing, including periodic vetting by internal and external security researchers. Your data is encrypted in transit and at rest, and our infrastructure runs on an industry-leading highly secure, HIPAA-compliant data center. value. We build trust with stakeholders by leading with ethics and through the integrity of our technology. We are dedicated to transparency, deep listening, and delivering on our commitments.[11]

25. Amazon Health Services' Notice of Privacy Practices, which applies to One Medical, states: "Privacy and security are foundational to how we design and operate our products and

[6] *About Us – Transforming primary care*, ONE MEDICAL, https://www.onemedical.com/about-us/ (last visited July 9, 2026).

[7] *One Medical Joins Amazon to Make It Easier for People to Get and Stay Healthier*, ONE MEDICAL (FEB. 22, 2023), https://www.onemedical.com/mediacenter/one-medical-joins-amazon/ (last visited July 9, 2026).

[8] ONE MEDICAL, *supra* note 6.

[9] *Id.*

[10] *Id.*

[11] *FAQ*, ONE MEDICAL, https://www.onemedical.com/faq/ (last visited July 9, 2026).

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

services. We know your health information is important to you and we take the responsibility of safeguarding and protecting it seriously."[12]

26. According to the press release that announced Amazon's acquisition of One Medical:

> The Health Insurance Portability and Accountability Act (HIPAA) governs what One Medical, Amazon, and others can do with Protected Health Information and this includes information like medication history, medical conditions, and treatment information. Amazon and One Medical have extensive experience protecting data of all kinds appropriately across a variety of businesses and nothing about this acquisition changes Amazon or One Medical's commitment to privacy or the strong protections we have for Protected Health Information.[13]

27. One Medical is aware of the sensitive nature of the Private Information it collects, and it acknowledges the importance of data privacy.

28. One Medical's public-facing statements on privacy and security make it clear that it is aware of the need to safeguard the sensitive Private Information entrusted to it by clients and consumers as part of providing its healthcare services.

29. Despite these strong proclaimed proactive policies and approaches to data security and privacy for its patients, Defendant failed to adequately secure and safeguard its systems and networks from a foreseeable and preventable cyberattack. This conduct proximately resulted in the Data Breach and significant harm to Plaintiff and the Class.

B. The Data Breach Exposed Valuable Private Information

30. An unauthorized party gained access to third-party file storage systems owned by One Medical between June 8, 2026, and June 11, 2026.[14]

31. Cybercriminal group ShinyHunters has claimed credit for the Data Breach, and claimed to have exfiltrated 8.8 terabytes of data.[15]

---

[12] *Amazon Health Services Notice of Privacy Practices*, ONE MEDICAL (FEB. 27, 2026), https://www.onemedical.com/hipaa/ (last visited July 9, 2026).

[13] ONE MEDICAL, *supra* note 7.

[14] *Id.*

[15] Steve Alder, *ShinyHunters Data Extortion Group Threatens to Leak 8.8 TB of Stolen One Medical Data*, THE HIPAA J. (JUN. 22, 2026), https://www.hipaajournal.com/one-medical-data-breach/ (last visited July 9, 2026).

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

32. The Data Breach reportedly affected an undisclosed number of "Iora Health/One Medical Seniors patients in Atlanta, Cape Cod, Charlotte, Piedmont Triad, Denver, Houston, Phoenix, Tucson, and Seattle."[16]

33. According to One Medical, demographic information and clinical records were exfiltrated.[17]

C. Defendant Had Ample Notice That It Was a Likely Cyberattack Target

34. At all relevant times, Defendant knew, or should have known, that the Private Information it was entrusted with was a target for malicious actors. Defendant knew this given the unique type and the significant volume of data on its networks, servers, and systems, comprising individuals' detailed and confidential personal information and, thus, the significant number of individuals who the exposure of the Private Information would harm.

35. As custodian of Plaintiff's and Class Members' Private Information, Defendant knew or should have known the importance of protecting its Private Information, and of the foreseeable consequences and harms to such persons if any data breach occurred.

36. According to the Consumer Financial Protection Bureau, the number of data breach and identity theft complaints it received grew from 14,319 in 2020 to 32,469 in 2022.[18] It is well known among companies that Private Information such as social security numbers and financial information is valuable and frequently targeted by criminals.

37. The Federal Trade Commission has warned consumers that identity thieves use Private Information to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[19]

38. In April 2020, ZDNet reported that "ransomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to

[16] *Id.*
[17] *Id.*
[18] *See Compromised: Why experts say data breaches are on the rise,* NBC 6 SOUTH FLORIDA, https://www.nbcmiami.com/responds/compromised-why-experts-say-data-breaches-are-on-the-rise/3473306/ (last visited June 5, 2025).
[19] *See* What to Know About Identity Theft, FEDERAL TRADE COMMISSION (Sept. 2024), https://consumer.ftc.gov/articles/what-know-about-identity-theft (last visited June 5, 2025).

maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[20]

39. Criminals can commit all types of fraud, including: obtaining a driver's license or official identification card in the victim's name but the thief's picture, using the victim's name and SSN to obtain government benefits, to obtain lending or lines of credit, filing a fraudulent tax return using the victim's information. Identity thieves may obtain a job using the victim's social security number, rent a house, or give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[21]

40. Defendant was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[22]

41. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[23]

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

[20] Catalin Cimpanu, *Ransomware mentioned in 1,000+ SEC filings over the past year*, ZDNET (April 30, 2020), https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last visited Sept. 1, 2025).

[21] *See* Warning Signs of Identity Theft, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited June 5, 2025).

[22] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited Sept. 7, 2020).

[23] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited June 23, 2026).

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

42. When compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[24] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[25]

43. Healthcare related data breaches have continued to rapidly increase, with several prominent examples in recent years, including Change Healthcare (192.7 million individuals, February 2024), and Episource (5.4 million people, January 2025), as well as several downstream victims of the MOVEit file-transfer breach, including Maximum, Welltok, and Delta Dental of California, each of which involved several million patients' information.

44. According to the FBI's annual internet crime report, healthcare and public health were the single most-targeted sector for cyberthreats in 2025.[26]

45. "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[27]

46. In the healthcare industry, the number one threat vector from a cyber security standpoint is phishing. Cybersecurity firm Proofpoint reports that "phishing is the initial point of

---

[24] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited June 23, 2026).

[25] *Id.*

[26] AMERICAN HOSPITAL ASSOCIATION, *FBI: Health care was top target for ransomware, other cyberthreats in 2025*, (April 10, 2026), available at https://www.aha.org/news/headline/2026-04-10-fbi-health-care-was-top-target-ransomware-other-cyberthreats-2025 (last visited June 23, 2026)

[27] INSIDE DIGITAL HEALTH, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited June 23, 2026).

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

compromise in most significant [healthcare] security incidents, according to a recent report from the Healthcare Information and Management Systems Society (HIMSS). And yet, 18% of healthcare organizations fail to conduct phishing tests, a finding HIMSS describes as 'incredible.'"[28]

47. The report from Proofpoint was published March 27, 2019, and summarized findings of recent healthcare industry cyber threat surveys and recounted good, common sense steps that the targeted healthcare companies should follow to prevent email-related cyberattacks.

48. One of the best protections against email related threats is security awareness training and testing on a regular basis. This should be a key part of a company's on-going training of its employees. "[S]ince phishing is still a significant, initial point of compromise, additional work needs to be done to further lower the click rate," the HIMSS report states. "This can be done through more frequent security awareness training, phishing simulation, and better monitoring of metrics pertaining to phishing (including whether there are any particular repeat offenders)."[29]

49. ProtonMail Technologies publishes a guide for IT Security to small businesses (i.e., companies without the heightened standard of care applicable in the healthcare industry). In its 2019 guide, ProtonMail dedicates a full chapter of its Book guide to the danger of phishing and ways to prevent a small business from falling prey to it. It reports:

> Phishing and fraud are becoming ever more extensive problems. A recent threat survey from the cybersecurity firm Proofpoint stated that between 2017 and 2018, email-based attacks on businesses increased 476 percent. The FBI reported that these types of attacks cost companies around the world $12 billion annually.
>
> Similar to your overall IT security, your email security relies on training your employees to implement security best practices and to recognize possible phishing attempts. This must be deeply ingrained into every staff member so that every time they check their emails, they are alert to the possibility of malicious action.[30]

---

[28] Aaron Jensen, *Healthcare Phishing Statistics: 2019 HIMSS Survey Results*, PROOFPOINT (Mar. 27, 2019), https://www.proofpoint.com/us/security-awareness/post/healthcare-phishing-statistics-2019-himss-survey-results (last visited June 23, 2026).

[29] *Id.*

[30] *The ProtonMail Guide to IT Security for Small Businesses*, PROTONMAIL (2019), *available at* https://protonmail.com/it-security-complete-guide-for-businesses (last visited Sept. 7, 2020).

50. The guidance that ProtonMail provides non-healthcare industry small businesses is likely still not adequate for a company like One Medical, with the heightened healthcare standard of care based on HIPAA, CMIA, and the increased danger from the sensitivity and wealth of Private Information it retains, but ProtonMail's guidance is informative for showing how inadequately One Medical protected the Private Information of the Plaintiff and Class Members. ProofPoint lists numerous tools under the heading, "How to Prevent Phishing":

a. **Training:** "Training your employees on how to recognize phishing emails and what to do when they encounter one is the first and most important step in maintaining email security. *This training should be continuous as well.* . . ."

b. **Limit Public Information:** "Attackers cannot target your employees if they don't know their email addresses. Don't publish non-essential contact details on your website or any public directories . . . .

c. **Carefully check emails:** "First off, your employees should be skeptical anytime they receive an email from an unknown sender. Second, most phishing emails are riddled with typos, odd syntax, or stilted language. Finally, check the 'From' address to see if it is odd . . . . If an email looks suspicious, employees should report it."

d. **Beware of links and attachments:** "Do not click on links or download attachments without verifying the source first and establishing the legitimacy of the link or attachment. . . ."

e. **Do not automatically download remote content:** "Remote content in emails, like photos, can run scripts on your computer that you are not expecting, and advanced hackers can hide malicious code in them. You should configure your email service provider to not automatically download remote content. This will allow you to verify an email is legitimate before you run any unknown scripts contained in it."

f. **Hover over hyperlinks:** "Never click on hyperlinked text without hovering your cursor over the link first to check the destination URL, which should appear in the lower corner of your window. Sometimes the hacker might disguise a malicious link as a short URL." [Proofpoint notes that there are tools online available for retrieving original URLs from shortened ones.]

g. **If in doubt, investigate:** "Often phishing emails will try to create a false sense of urgency by saying something requires your immediate action. However, if your employees are not sure if an email is genuine, they should not be afraid to take extra time to verify the email. This might include asking a colleague, your IT security lead, looking up the website of the service the email is purportedly from, or, if they have a phone number, calling the institution, colleague, or client that sent the email."

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

h. **Take preventative measures:** "Using an end-to-end encrypted email service gives your business's emails an added layer of protection in the case of a data breach. A spam filter will remove the numerous random emails that you might receive, making it more difficult for a phishing attack to get through. Finally, other tools, like Domain-based Message Authentication, Reporting, and Conformance (DMARC) help you be sure that the email came from the person it claims to come from, making it easier to identify potential phishing attacks."[31]

51. Private Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[32] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and PHI on multiple underground Internet websites, commonly referred to as the dark web.

D. Defendant Breached Its Duties to Plaintiff and Class Members, and Failed to Comply with Regulatory Requirements and Industry Practices.

52. Because Defendant was entrusted with Private Information at all times herein relevant, Defendant owed to Plaintiff and the Class a duty to exercise commercially reasonable methods and care in handling, using, maintaining, storing, and safeguarding the Private Information in its care, control, and custody, including by implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that occurred, and to promptly detect and thwart attempts at unauthorized access to their networks and systems. Defendant also owed a duty to safeguard Private Information because it was on notice that it was handling highly valuable data and knew there was a significant risk it would be targeted by cybercriminals. Furthermore, Defendant knew of the extensive, foreseeable harm that would ensue for the victims of a data breach, and therefore also owed a duty to reasonably safeguard that information.

53. HIPAA requires covered entities such as One Medical to protect against reasonably anticipated threats to the security of PHI. Covered entities must implement safeguards to ensure the

[31] *Id.*

[32] FEDERAL TRADE COMMISSION, *Warning Signs of Identity Theft, available at:* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited June 23, 2026).

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[33]

54. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

55. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the breach to each affected individual "without unreasonable delay and *in no case later than 60 days following discovery of the breach*."[34]

56. Based on information and belief, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations. One Medical's security failures include, but are not limited to, the following:

a. Failing to ensure the confidentiality and integrity of electronic protected health information that Defendant creates, receives, maintains, and transmits in violation of 45 C.F.R. §164.306(a)(1);

b. Failing to 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 in violation of 45 C.F.R. §164.312(a)(1);

c. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. §164.308(a)(1);

[33] HIPAA JOURNAL, *What is Considered Protected Health Information Under HIPAA?, available at:* https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/ (last visited June 23, 2026).

[34] *Breach Notification Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVICES, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added) (last visited June 23, 2026).

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

d. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. §164.308(a)(6)(ii);

e. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. §164.306(a)(2);

f. Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. §164.306(a)(3);

g. Failing to ensure compliance with HIPAA security standard rules by its workforce in violation of 45 C.F.R. §164.306(a)(4);

h. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. §164.502, *et seq.*;

i. Failing to effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §164.308(a)(5); and

j. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. §164.530(c).

57. Security standards commonly accepted among businesses like Defendant that store PII include, without limitation:

i. Maintaining a secure firewall configuration;

ii. Monitoring for suspicious or irregular traffic to servers or networks;

iii. Monitoring for suspicious credentials used to access servers or networks;

iv. Monitoring for suspicious or irregular activity by known users;

v. Monitoring for suspicious or unknown users;

vi. Monitoring for suspicious or irregular server requests;

vii. Monitoring for server requests for PII;

viii. Monitoring for server requests from VPNs; and

ix. Monitoring for server requests for Tor exit nodes.

58. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[35] and protection of PII which includes basic security standards applicable to all types of businesses.[36]

59. The FTC recommends that businesses:

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

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

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

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

v. 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 hacker attacks.

[35] Start with Security: A Guide for Business, FTC (June 2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[36] Protecting Personal Information: A Guide for Business, FTC (Oct. 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

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

vii. 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.

viii. 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.

ix. 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.

60. As described further below, Defendant owed a duty to safeguard Private Information under the Federal Trade Commission Act, 15 U.S.C. § 45 (the "FTC Act") to ensure that all information it received, maintained, and stored was secure. This statute was enacted to protect Plaintiff and the Class Members from the type of conduct in which Defendant engaged, and the resulting harms Defendant proximately caused Plaintiff and the Class Members.

61. Under the FTC Act, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

62. 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 Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

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

63. Defendant breached its duty to exercise reasonable care in protecting Plaintiff's and Class Members' Private Information by failing to implement and maintain adequate data security measures to safeguard Plaintiff's and Class Members' sensitive personal information, failing to encrypt or anonymize Private Information within its systems and networks, failing to monitor its systems and networks to promptly identify and thwart suspicious activity, allowing unmonitored and unrestricted access to unsecured Private Information, and allowing (or failing to prevent) unauthorized access to, and exfiltration of, Plaintiff's and Class Members' confidential and private information. Additionally, Defendant breached its duty by utilizing outdated and ineffectual data security measures which deviated from standard industry best practices at the time of the Data Breach. Through these actions, Defendant also violated its duties under the FTC Act.

64. Defendant failed to prevent the Data Breach. Had Defendant properly maintained and adequately protected its systems, servers, and networks, the Data Breach would not have occurred.

65. Additionally, the law imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of Private Information to Plaintiff and Class Members so that it can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuses of their private information. Defendant further breached its duties by failing to provide any notice of the Data Breach to Plaintiff and Class Members. In so doing, Defendant actually and proximately caused and exacerbated the harm from the Data Breach and the injuries-in-fact of Plaintiff and Class Members.

66. HHS's Office for Civil Rights notes:

> While all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations, as they store large quantities of highly Private and valuable data.[37]

[37] HIPAA JOURNAL, *Cybersecurity Best Practices for Healthcare Organizations*, https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/ (last visited June 23, 2026).

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

67. HHS highlights several basic cybersecurity safeguards that can be implemented to improve cyber resilience that require a relatively small financial investment, yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of Private Information; (b) educating and training healthcare employees on how to protect Private Information; and (c) correcting the configuration of software and network devices.

68. Private cybersecurity firms have also identified the healthcare sector as being particularly vulnerable to cyber-attacks, both because of value of the Private Information which healthcare entities maintain and because the healthcare industry has been slow to adapt and respond to cybersecurity threats. They too have promulgated similar best practices for bolstering cybersecurity and protecting against the unauthorized disclosure of Private Information.

69. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, One Medical chose to ignore them. These best practices were known, or should have been known by One Medical, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure of Private Information.

E. The Experiences of Plaintiff

70. Plaintiff received notice that her data was exfiltrated in the Data Breach on or around June 29, 2026.[38]

71. Plaintiff trusted that Defendant would use reasonable measures to protect her data according to state and federal law.

72. As a proximate result of the Data Breach, Plaintiff will spend time for the foreseeable future and beyond dealing with its consequences and self-monitoring her accounts and credit reports to monitor potentially suspicious and fraudulent activity. This time will be lost forever and cannot be recaptured.

73. Plaintiff has and is experiencing fear, stress, and frustration because her sensitive information was stolen in the Data Breach, and not knowing by whom or for what purpose. This goes beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that the law contemplates and addresses.

[38] *See* Exhibit A.

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

74. Plaintiff suffered actual injuries in the form of damages to and diminution in the value of her Private Information —a form of intangible property was entrusted to Defendant, which was compromised in and as a proximate result of the Data Breach.

75. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from her Private Information being obtained by unauthorized third parties and possibly cybercriminals.

76. Plaintiff has a continuing interest in ensuring that her Private Information, which remains within Defendant's possession and control, is protected and safeguarded against future data breaches or cybersecurity risks.

77. Defendant deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's harmful effects by failing to promptly notify her about it. One Medical waited almost a month to notify Plaintiff.

F. Plaintiff and the Class Suffered Actual and Impending Injuries Resulting From the Data Breach

78. As a proximate result of Defendant's completely unreasonable security practices, identity thieves now possess the sensitive Private Information of Plaintiff and the Class. That information is extraordinarily valuable on the black market and incurs direct costs to Plaintiff and the Class. On the dark web—an underground Internet black market—criminals openly buy and sell stolen Private Information to create "identity kits" worth up to $2,000 each that can be used to create fake IDs, gain access to bank accounts, social media accounts, and credit cards, file false insurance claims or tax returns, or rack up other kinds of expenses.[39] And, "[t]he damage to affected [persons] may never be undone."[40]

79. Unlike the simple credit-card breaches at retail merchants, these damages cannot be avoided by canceling and reissuing plastic cards or closing an account. Identity theft is far more

[39] Nick Culbertson, *Increased Cyberattacks on Healthcare Institutions Shows the Need for Greater Cybersecurity* (Jun. 7, 2021), FORBES, https://www.forbes.com/sites/forbestechcouncil/2021/06/07/increased-cyberattacks-on-healthcare-institutions-shows-the-need-for-greater-cybersecurity/?sh=ca928c05650d.

[40] *Id.*

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

pernicious than credit card fraud. Criminals' ability to open entirely new accounts—not simply prey on existing ones—poses far more dangerous problems. Identity thieves can retain the stolen information for years until the controversy has receded because victims may become less vigilant in monitoring their accounts as time passes. Then, at any moment, the thief can take control of a victim's identity, resulting in thousands of dollars in losses and lost productivity. The U.S. Department of Justice has reported that in 2021, identity theft victims spent on average about four hours to resolve problems stemming therefrom and that the average financial loss experienced by an identity theft victim was $1,160 per person.[41] Additionally, about 80% of identity theft victims reported some form of emotional distress resulting from the incident.[42]

80. As a consequence of the Data Breach, Class Members' credit profiles can be destroyed before they even realize what happened, and they may be unable to legitimately borrow money, obtain credit, or open bank accounts. Class Members can be deprived of legitimate tax refunds or, worse yet, may face state or federal tax investigations due to fraud committed by an identity thief. And even the simple preventive step of adding oneself to a credit-fraud watch list to guard against these consequences substantially impairs Class Members' ability to obtain additional credit. In fact, many experts advise victims to place a freeze on all credit accounts, making it impossible to rent a car, get student loans, buy or rent big-ticket items, or complete a major new car or home purchase.

81. While credit card information and associated PII can sell for as little as $1-$2 on the black market, PHI can sell for as much as $363 according to the Infosec Institute.[43]

82. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be

[41] Erika Harrell and Alexandra Thompson, Victims of Identity Theft, 2021, U.S. DEPARTMENT OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, BUREAU OF JUSTICE STATISTICS (Oct. 2023), *available at* https://bjs.ojp.gov/document/vit21.pdf.

[42] *Id.*

[43] CENTER FOR INTERNET SECURITY, *Data Breaches: In the Healthcare Sector*, https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last visited June 23, 2026).

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

83. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[44]

84. Similarly, the FBI Cyber Division, in an April 8, 2014 Private Industry Notification, advised:

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.

85. The ramifications of One Medical's failure to keep its patients' 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. Fraudulent activity might not show up for six to 12 months or even longer.

86. Further, criminals often trade stolen Private Information on the "cyber black-market" for years following a breach. Cybercriminals can post stolen Private Information on the internet, thereby making such information publicly available.

87. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened. [45] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of

[44] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER HEALTH NEWS (Feb. 7, 2014) https://khn.org/news/rise-of-indentity-theft/ (last visited June 23, 2026).

[45] *See Medical ID Theft Checklist*, IDENTITYFORCE (Jan. 11, 2023), https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last visited June 23, 2026).

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[46]

88. Breaches are particularly serious in healthcare industries. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[47] Indeed, when compromised, healthcare related data is among the most private and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[48] Almost 50% of the surveyed victims lost their healthcare coverage as a result of the incident, while nearly 30% said their insurance premiums went up after the event. Forty percent of the victims were never able to resolve their identity theft at all. Seventy-four percent said that the effort to resolve the crime and restore their identity was significant or very significant. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[49]

89. As a healthcare provider, One Medical knew, or should have known, the importance of safeguarding its patients' Private Information entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed

[46] EXPERIAN, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages*"), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited June 23, 2026).

[47] IDENTITY THEFT RESOURCE CENTER, *2018 End-of-Year Data Breach Report, available at*: https://notified.idtheftcenter.org/s/resource (last visited June 23, 2026).

[48] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited June 23, 2026); *see also National Survey on Medical Identity Theft*, Feb. 22, 2010, cited at p. 2.

[49] *Id.*

on One Medical patients as a result of a breach. One Medical failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

CLASS ACTION ALLEGATIONS

90. Pursuant to Fed. R. Civ. P. 23(a), (b)(1), (b)(2), and (b)(3), and where applicable, 23(c)(4), Plaintiff seeks certification of the following Nationwide Class:

> **Nationwide Class:** All persons in the United States who were impacted by the One Medical Data Breach, including all persons who received notice that their Private Information was compromised as a result of the Data Breach (and each person a "Class Member").

91. Excluded from the Class are governmental entities, Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, affiliates, legal representatives, employees, co-conspirators, successors, subsidiaries, and assigns. Also excluded from the Class are any judges, justices, or judicial officers presiding over this matter and the members of their immediate families and judicial staff.

92. This action is brought and may be properly maintained as a class action pursuant to Fed. R. Civ. P. 23(a), (b)(1), (b)(2), and 23(b)(3), and satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of these rules.

93. *Numerosity Under Rule 23(a)(1)*. The Class is so numerous that the individual joinder of all members is impracticable, and the disposition of the claims of all members of the Class in a single action will provide substantial benefits to the parties and the Court. Upon information and belief, Plaintiff estimates that the Class is comprised of at least thousands of Class Members. The Class is sufficiently numerous to warrant certification.

94. *Commonality Under Rule 23(a)(2)*. Common legal and factual questions exist that predominate over any questions affecting only individual members of the Class. These common questions, which do not vary among members of the Class and which may be determined without reference to any Class Member's individual circumstances, include, but are not limited to:

a. Whether Defendant knew or should have known that its computer systems and networks were vulnerable to unauthorized third-party access or a cyberattack;

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

b. Whether Defendant failed to utilize and maintain adequate and reasonable security and preventive measures to ensure that its computer systems and networks were protected;

c. Whether Defendant failed to take available steps to prevent and stop the Data Breach from occurring;

d. Whether Defendant failed to comply with its own policies and applicable laws, regulations and industry standards relating to data security;

e. Whether Defendant owed a legal duty to Plaintiff and Class Members to protect their Private Information;

f. Whether Defendant breached any duty to protect the Private Information of Plaintiff and Class Members by failing to exercise due care in protecting their sensitive and private information;

g. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the Private Information of Plaintiff and Class Members.

h. Whether Defendant provided timely, accurate, and sufficient notice of the Data Breach to Plaintiff and the Class Members;

i. Whether Plaintiff and Class Members have been damaged by the wrongs alleged and are entitled to actual, statutory, or other forms of damages and other monetary relief; and

j. Whether Plaintiff and Class Members are entitled to injunctive or equitable relief, including restitution.

95. *Typicality Under Rule 23(a)(3)*. Plaintiff's claims are typical of the claims of the Class. Plaintiff had her Private Information compromised in the Data Breach. Defendant's uniformly unlawful course of conduct injured Plaintiff and Class Members.

96. *Adequacy of Representation Under Rule 23(a)(4)*. Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the Class. Plaintiff has retained counsel competent and experienced in complex litigation and consumer protection class action matters such as this action, and Plaintiff and her counsel intend to vigorously

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

prosecute this action for the Class's benefit and have the resources to do so. Plaintiff and her counsel have no interests adverse to those of the other members of the Class.

97. *Predominance and Superiority*. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy because individual litigation of each Class Member's claim is impracticable. The damages, harm, and losses suffered by the individual members of the Class will likely be small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's wrongful conduct. Even if each Class Member could afford individual litigation, the Court system could not. It would be unduly burdensome if tens of thousands of individual cases or more proceeded. Individual litigation also presents the potential for inconsistent or contradictory judgments, the prospect of a race to the courthouse, and the risk of an inequitable allocation of recovery among those individuals with equally meritorious claims. Individual litigation would increase the expense and delay to all parties and the Courts because it requires individual resolution of common legal and factual questions. By contrast, the class action device presents far fewer management difficulties and provides the benefit of a single adjudication, economies of scale, and comprehensive supervision by a single court.

98. As a result of the foregoing, class treatment under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3), and (c)(4) is appropriate.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

99. Plaintiff incorporates the above allegations as if fully set forth herein.

100. Because Defendant was entrusted with such Private Information at all times herein relevant, it owed to Plaintiff and the Class a duty to exercise commercially reasonable methods and care in handling, using, maintaining, storing, and safeguarding the Private Information in its care, control, and custody, including by implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that occurred, and to promptly detect and thwart attempts at unauthorized access to their networks and systems. This duty arose independently from any contract.

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

101. Defendant knew, or should have known, of the risks inherent in collecting and storing massive amounts of Private Information, including the importance of adequate data security and the high frequency of ransomware attacks and well-publicized data breaches. Defendant owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendant's failure to adequately safeguard its Private Information in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that sensitive information. Indeed, on its website, One Medical commits to data privacy, including safeguarding Private Information.

102. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and the Class's Private Information failing to limit access to this information to unauthorized third parties and by not properly supervising both the way the Private Information was stored, used, and exchanged, and those in One Medical's employ responsible for such tasks.

103. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their Private Information. Defendant also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and circumstances of the Data Breach. This duty is required and necessary for Plaintiff and the Class to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

104. Defendant also had a common law duty to prevent foreseeable harm to others. Defendant had full knowledge of the sensitivity and high value of the Private Information that it stored and the types of foreseeable harm and injury-in-fact that Plaintiff and Class Members could and would suffer if that Private Information were wrongfully disclosed, leaked, accessed, or exfiltrated. Defendant's conduct created a foreseeable and unreasonable risk of harm to Plaintiff and Class Members, who were the foreseeable victims of Defendant's inadequate data security practices.

105. Defendant violated its duty to implement and maintain reasonable security procedures and practices, including through its failure to adequately restrict access to its systems that held millions of individuals' Private Information or encrypt or anonymize such data.

Defendant's duty included, among other things, designing, maintaining, and testing their information security controls to ensure that Private Information in its possession was adequately secured by, for example, encrypting or anonymizing sensitive personal information, installing intrusion detection and deterrent systems and monitoring mechanisms, and using access controls to limit access to sensitive data.

106. Defendant's duty of care also arose pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") and HIPAA, under which Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

107. The FTC Act and HIPAA were enacted to protect Plaintiff and the Class Members from the type of wrongful conduct in which Defendant engaged.

108. Defendant's violation of the FTC Act and HIPAA constitutes negligence per se for purposes of establishing the duty and breach elements of Plaintiff's negligence claim. Those statutes were designed to protect a group to which Plaintiff belongs and to prevent the types of harm that resulted from the Data Breach.

109. Defendant breached its duty to exercise reasonable care in protecting Plaintiff's and Class Members' Private Information by failing to implement and maintain adequate data security measures to safeguard Plaintiff's and Class Members' sensitive personal information, failing to encrypt or anonymize Private Information within its systems and networks, failing to monitor its systems and networks to promptly identify and thwart suspicious activity, failing to delete and purge Private Information no longer necessary for its provision of services to its clients and customers, allowing unmonitored and unrestricted access to unsecured Private Information, and allowing (or failing to prevent) unauthorized access to, and exfiltration of, Plaintiff's and Class Members' confidential and private information. Additionally, Defendant breached its duty by utilizing outdated and ineffectual data security measures which deviated from standard industry best practices at the time of the Data Breach. Through these actions, Defendant also violated its duties under the FTC Act and HIPAA.

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

110. The law imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of Private Information to Plaintiff and Class Members so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuses of their Private Information. Defendant further breached their duties by failing to provide any notice of the Data Breach to Plaintiff and Class Members. In so doing, Defendant actually and proximately caused and exacerbated the harm from the Data Breach and the injuries-in-fact of Plaintiff and Class Members. Timely disclosure was necessary so that Plaintiff and Class Members could, among other things: (i) purchase identity theft protection, monitoring, and recovery services; (ii) flag asset, credit, and tax accounts for fraud; (iii) purchase or otherwise obtain credit reports; (iv) place or renew fraud alerts on a quarterly basis; (v) closely monitor loan data and public records; and (vi) take other meaningful steps to protect themselves and attempt to avoid or recover from identity theft and other harms.

111. Plaintiff and Class Members had no ability to protect their Private Information once it was in Defendant's possession and control. Defendant was in an exclusive position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

112. But for Defendant's breach of duty to adequately protect Class Members' Private Information, Class Members' Private Information would not have been stolen. As a result of Defendant's negligence, Plaintiff and Class Members suffered and will continue to suffer the various types of damages alleged herein. There is a temporal and close causal connection between Defendant's failure to implement adequate data security measures, the Data Breach, and the harms suffered by Plaintiff and Class Members.

113. As a direct and traceable result of Defendant's negligence, Plaintiff and the Class have suffered or will suffer an increased and impending risk of fraud, identity theft, damages, embarrassment, humiliation, frustration, emotional distress, and lost time and out-of-pocket costs to mitigate and remediate the effects of the Data Breach. These harms to Plaintiff and the Class include, without limitation: (i) loss of the opportunity to control how their personal information is used; (ii) diminution in the value and use of their personal information entrusted to Defendant; (iii) the compromise and theft of their personal information; (iv) out-of-pocket costs associated with the

prevention, detection, and recovery from identity theft and unauthorized use of financial accounts; (v) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including increased costs to use credit, credit scores, credit reports, and assets; (vi) unauthorized use of compromised personal information to open new financial and other accounts; (vii) continued risk to their personal information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the personal information in its possession; and (viii) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their personal information being stolen in the Data Breach.

114. Defendant's negligence was gross, willful, wanton, and warrants the imposition of punitive damages given the clear foreseeability of a hacking incident, the extreme sensitivity of the private information under Defendant's care, and its failure to take adequate remedial steps, including prompt notification of the victims, following the Data Breach.

115. Plaintiff and Class Members are entitled to all forms of monetary compensation set forth herein, including monetary payments to provide adequate long-term identity protection services. Plaintiff and Class Members are also entitled to the injunctive relief sought herein.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

116. Plaintiff incorporates the above allegations as if fully set forth herein.

117. Defendant entered into contracts with Plaintiff and Class Members to provide healthcare services.

118. These contracts are virtually identical to each other and were made expressly for the benefit of Plaintiff and the Class, as Defendant agreed to safeguard and protect their confidential Private Information and to timely and accurately notify Plaintiff and Class Members if their information had been breached and compromised.

119. Defendant acquired, stored, and maintained the Private Information of Plaintiff and the Class.

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

120. Plaintiff and Class Members were required to provide, or authorize the transfer of, their Private Information in order for Defendant to provide its services.

121. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of its regular business practices. Plaintiff and Class Members accepted Defendant's offer and provided their Private Information to Defendant.

122. When Plaintiff and Class Members provided their Private Information to Defendant, they entered into implied contracts with Defendant and intended and understood that Private Information would be adequately safeguarded as part of that service.

123. Defendant's implied promise of confidentiality to Plaintiff and Class Members includes consideration beyond those pre-existing general duties owed under the FTC Act and HIPAA, or other state or federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards, FTC guidelines on data security, and HIPAA regulations.

124. Defendant's implied promises include but are not limited to: (a) taking steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (b) restricting access to qualified and trained agents; (c) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (d) applying or requiring proper encryption; (e) multifactor authentication for access; (f) protecting Plaintiff's and Class Members' Private Information in compliance with federal and state laws and regulations and industry standards; and (g) other steps to protect against foreseeable data breaches.

125. Defendant's implied promises to safeguard Plaintiff's and Class Members' Private Information are evidenced by representations on Defendant's website. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant on the other, is further demonstrated by their conduct and course of dealing.

126. Plaintiff and the Class Members would not have entrusted their Private Information to Defendant in the absence of such an implied contract. Had Defendant disclosed to Plaintiff and the Class that it did not have adequate computer systems and security practices to secure sensitive

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

data, Plaintiff and the other Class Members would not have provided their Private Information to Defendant.

127. Defendant recognized that Plaintiff's and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

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

129. Defendant breached the implied contracts it made with its clients by failing to take reasonable measures to safeguard their Private Information as described herein, as well as by failing to provide accurate, adequate, and timely notice to them that their Private Information was compromised as a result of the Data Breach.

130. As a direct and proximate result of Defendant's wrongful conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages from: (i) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm, (iii) the loss of the confidentiality of the stolen Private Information, (iv) the illegal sale of the compromised data on the dark web, (v) lost work time, and (vi) other economic and non-economic harms.

131. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to strengthen its data security systems, submit to future audits of those systems, and provide adequate long-term credit monitoring and identity theft protection services to all persons affected by the Data Breach.

THIRD CAUSE OF ACTION
Injunctive/Declaratory Relief
(On Behalf of Plaintiff and the Nationwide Class)

132. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and state statutes described herein.

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

133. Defendant owes a duty of care to Plaintiff and Class Members, which required Defendant to adequately monitor and safeguard Plaintiff's and Class Members' Private Information.

134. Defendants and its officers, directors, affiliates, legal representatives, employees, co-conspirators, successors, subsidiaries, and assigns still possess the Private Information belonging to Plaintiff and Class Members.

135. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' Private Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their Private Information. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff and the Class continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

136. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to adequately secure the Private Information of Plaintiff and the Class within its care, custody, and control under the common law, and Section 5 of FTC Act;

b. Defendant breached its duty to Plaintiff and the Class by allowing the Data Breach to occur;

c. Defendant's existing data monitoring measures do not comply with its obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect the Private Information of Plaintiff and the Class within Defendant's custody, care, and control; and

d. Defendant's ongoing breaches of said duties continue to cause harm to Plaintiff and the Class.

137. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach or cybersecurity incident. This risk is real, immediate, and substantial. If another data breach or cybersecurity incident occurs,

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

Plaintiff and the Class will not have an adequate remedy at law because monetary relief alone will not compensate Plaintiff and the Class for the serious risks of future harm.

138. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Plaintiff and the Class will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendant's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

139. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach or cybersecurity incident, thus preventing future injury to Plaintiff and the Class and other persons whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class set forth herein, respectfully requests the following relief:

A. Certifying this action as a class action under Fed. R. Civ. P. 23 and appointing Plaintiff and her counsel to represent the Class;

B. Entering judgment for Plaintiff and the Class;

C. Granting permanent and appropriate injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein and directing Defendant to adequately safeguard the Private Information of Plaintiff and the Class by implementing improved security controls;

D. Awarding compensatory, consequential, and general damages, including nominal damages as appropriate, as allowed by law in an amount to be determined at trial;

E. Award Plaintiff and Class Members statutory or punitive damages and penalties as allowed by law in an amount to be determined at trial;

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

F. Ordering disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of Defendant's unlawful acts, omissions, and practices;

G. Awarding to Plaintiff and Class Members the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

H. Awarding pre- and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper; and

I. Granting such further and other relief as may be just and proper.

DEMAND FOR JURY TRIAL

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

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

Dated: July 10, 2026

SCHUBERT JONCKHEER & KOLBE LLP

/s/ Amber L. Schubert
Amber L. Schubert

Robert C. Schubert (S.B.N. 62684)
Amber L. Schubert (S.B.N. 278696)
Sonum Dixit (S.B.N. 353395)
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, California 94123
Telephone: (415) 788-4220
Facsimile: (415) 788-0161
E-mail: rschubert@sjk.law
aschubert@sjk.law
sdixit@sjk.law

Counsel for Plaintiff Donna Sanders and the Putative Class

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220