

1 Rosemary M. Rivas (SBN 209147)
 2 David M. Berger (SBN 277526)
 3 Rosanne L. Mah (SBN 242628)
 4 **GIBBS LAW GROUP LLP**
 5 1111 Broadway, Suite 2100
 6 Oakland, California 94607
 7 (510) 350-9700 (tel.)
 8 (510) 350-9701 (fax)
 9 rmr@classlawgroup.com
 10 dmb@classlawgroup.com
 11 rlm@classlawgroup.com

12 *Attorneys for Plaintiff*

13 **UNITED STATES DISTRICT COURT FOR THE**
 14 **NORTHERN DISTRICT OF CALIFORNIA**

15 BAY AREA THERAPY GROUP A
 16 MARRIAGE AND FAMILY COUNSELING
 17 CORP., individually and on behalf of all others
 18 similarly situated,

19 Plaintiff,

20 v.

21 CHANGE HEALTHCARE INC., OPTUM,
 22 INC. and UNITEDHEALTH GROUP
 23 INCORPORATED,

24 Defendants.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

TABLE OF CONTENTS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- I. INTRODUCTION 1
- II. PARTIES 2
- III. JURISDICTION AND VENUE 3
- IV. FACTUAL ALLEGATIONS..... 4
 - A. Background 4
 - B. The February 2024 Data Breach Exposed Significant Vulnerabilities in Defendants’
Computer Networks, Leading to the Shutdown of Critical Healthcare Infrastructure. 6
 - C. The Data Breach and Shutdown have Created a National Crisis in the Healthcare
Industry, Severely Impacting the Financial Security of Hundreds of Thousands of
Healthcare Providers. 11
 - D. The Data Breach and Resulting Shutdown were Foreseeable Risks of Which
Defendants were on Notice and Could Have Prevented. 13
 - E. Defendants, at all Relevant Times, had a Duty to Plaintiff and Class Members. 15
 - F. Plaintiff’s Experience..... 18
- V. CLASS ACTION ALLEGATIONS 19
- VI. CAUSES OF ACTION 21
- VII. PRAYER FOR RELIEF 27
- VIII. DEMAND FOR JURY TRIAL..... 27

1 Plaintiff Bay Area Therapy Group a Marriage and Family Counseling Corp. (“Plaintiff”),
2 individually and on behalf of all others similarly situated, alleges the following:

3 **I. INTRODUCTION**

4 1. Plaintiff brings this proposed class action lawsuit against Defendants Change
5 Healthcare Inc., Optum, Inc. and UnitedHealth Group Incorporated (“Defendants”) for their failure
6 to maintain the security of their computer networks in accordance with state and federal law.
7 Defendants’ computer networks include data processing systems, portals, and platforms that have
8 become critical infrastructure for administering healthcare across the United States. Defendants’
9 computer networks process billions of healthcare transactions annually, performing more than 100
10 critical functions used by over 1,000,000 healthcare providers, including hospitals, physicians,
11 therapists, pharmacies, and laboratories, and affecting medical care for many millions of
12 Americans. Through aggressive acquisition and expansion, Defendants have broadened the reach
13 of their services to include the systems that healthcare providers use to submit claims for payment
14 to insurers and other payors, platforms that verify individuals’ insurance coverage, programs used
15 to verify prior authorizations for medical treatment and prescription drugs, and dozens of other
16 critical functions.

17 2. Given their role providing critical infrastructure in the nationwide delivery of
18 healthcare, Defendants knew they needed to implement incredibly robust cybersecurity controls
19 to prevent disruptions. Lives are literally on the line. Instead, Defendants neglected to implement
20 the robust cybersecurity controls that such critical infrastructure demands. As a result of
21 Defendants’ negligence, failures, and omissions, a well-known group of cybercriminals, called
22 ALPHV/Blackcat (“Blackcat”) that have been known for some time to target healthcare
23 organizations, was able to infiltrate Defendants’ computers networks and steal for ransom
24 confidential health data and source code, among other things (“Data Breach”).

25 3. The Data Breach exposed the vulnerabilities in Defendants’ computer networks and
26 as a result, Defendants took all of the affected computer networks offline, leaving healthcare
27 providers in dire straits. Since the Data Breach was discovered on February 21, 2024, healthcare
28 providers have been unable to provide critical services and get paid on claims for medical treatment

1 they have provided. Defendants’ negligence, failures, and omissions have catastrophically harmed
2 hard-working medical providers around the country, forcing many to the edge of bankruptcy and
3 delaying or denying vital medical treatments needed by patients around the county.

4 4. The American Hospital Association (“AHA”) has described the situation as a
5 “staggering loss of revenue.”¹ According to an estimate from First Health Advisory, a digital risk
6 assurance firm, the Data Breach “is costing some providers over \$100 million a day.”² Rick
7 Pollack, President and CEO of the AHA, remarked that the Data Breach is the “most serious
8 incident of its kind leveled against a U.S. healthcare organization.”

9 5. The healthcare industry has been a target of cyberattacks for years given the
10 massive amount of confidential personal health information (“PHI”) and personal identifying
11 information (“PII”) that healthcare organizations collect, store, and maintain and that can be used
12 to commit identity theft. Since as early as 2014, government agencies have warned the healthcare
13 industry about the threat of cyberattacks and has repeatedly cautioned them to ensure that their
14 systems are secure and protected. The U.S. government has also specifically warned the industry
15 that Blackhat has hit at least 70 organizations since December 2023, a majority of them healthcare
16 organizations. Therefore, the Data Breach and related shutdown were entirely foreseeable and
17 could have been avoided.

18 6. Plaintiff, individually and on behalf of all others similarly situated, alleges claims
19 for negligence, negligent interference with prospective economic advantage, violations of
20 California’s Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.*, and for unjust
21 enrichment.

22 II. PARTIES

23 7. Plaintiff Bay Area Therapy Group a Marriage and Family Counseling Corp. is a
24 citizen of California and maintains its principal place of business in Concord, California.

26 ¹ See <https://www.aha.org/lettercomment/2024-03-13-aha-urges-more-congressional-action-help-providers-affected-change-healthcare-cyberattack> (last visited March 18, 2024).

28 ² *Id.*

1 8. Defendant Change Healthcare Inc. is a publicly traded company with its principal
2 place of business in Nashville, Tennessee and is incorporated in Delaware. It became a subsidiary
3 of UnitedHealth Group Incorporated in 2022 and is operated by Optum, Inc., another UnitedHealth
4 Group subsidiary.

5 9. Defendant Optum, Inc. maintains its principal place of business in Eden Prairie,
6 Minnesota and is incorporated in Delaware.

7 10. Defendant UnitedHealth Group Incorporated is one of the largest publicly traded
8 companies by revenue and maintains its principal place of business in Minnetonka, Minnesota and
9 is incorporated in Delaware. UnitedHealth Group exercises control over the management of the
10 Change Healthcare cybersecurity systems as evidenced by UnitedHealth Group's response to the
11 Data Breach as alleged herein.

12 **III. JURISDICTION AND VENUE**

13 11. This Court has jurisdiction over this action under the Class Action Fairness
14 Act, 28 U.S.C. § 1332(d). There are at least 100 members in the proposed class, the aggregated
15 claims of the individual class members exceed the sum or value of \$5,000,000, exclusive of
16 interests and costs, and this is a class action in which one or more members of the proposed Class,
17 including Plaintiff, are citizens of a state different from Defendants. The Court has supplemental
18 jurisdiction over the alleged state law claims under 28 U.S.C. § 1367 because they form part of the
19 same case or controversy.

20 12. This Court may exercise jurisdiction over Defendants because they are registered
21 to conduct business in California; have sufficient minimum contacts in California; and
22 intentionally avail themselves of the markets within California through the promotion, sale, and
23 marketing of their services, thus rendering the exercise of jurisdiction by this Court proper and
24 necessary.

25 13. Venue is proper in this District under 28 U.S.C. § 1391 because Plaintiff resides in
26 this District and a substantial part of the events or omissions giving rise to Plaintiff's claims
27 occurred in this District.

28 //

IV. FACTUAL ALLEGATIONS

A. Background

14. Change Healthcare is a healthcare technology company that works across the U.S. health system “to make clinical, administrative and financial processes simpler and more efficient for payers, providers, and consumers.” Change Healthcare offers healthcare providers such as doctors, hospitals, therapists, pharmacies, laboratories, and clinics services and support in key areas such as provider claim processing, pharmacy claim transactions, verification of insurance, disbursement of provider payments, and authorizations and medical necessity reviews. Healthcare providers utilize Change Healthcare’s services either through a direct contractual relationship or indirectly through third-party intermediaries.

15. According to the Change Healthcare website, its “extensive network, innovative technology, and expertise inspire a stronger, better coordinated, increasingly collaborative, and more efficient healthcare system.” It bills itself as a “trusted partner for organizations committed to improving the healthcare system through technology.”

16. Change Healthcare also represents to providers that its “advanced technology and services help . . . enhance patient engagement and access, improve outcomes, drive revenue performance, and improve operational efficiency.” Change Healthcare represents to payers that its “advanced technology solutions and services help payers achieve their priorities across the member journey.” Change Healthcare promises its partners that its “advanced technology solutions empower our partners to achieve their strategic business objectives and meet their customers’ needs.” And it assures patients that its “solutions streamline the engagement, care, and payment experience to improve the patient journey.”

17. Change Healthcare processes 15 billion healthcare transactions annually and touches one in every three U.S. patient records through its clinical connectivity solutions.

18. Previously, Change Healthcare was an independent company that was not owned by any particular healthcare provider or insurer. In 2021, UnitedHealth Group (“UHG”) proposed a deal to acquire Change Healthcare for a merger with Optum, a healthcare provider and subsidiary of UHG.

1 19. Melinda Reid Hatton, AHA Vice President and General Counsel, voiced concerns
2 about the proposed deal and wrote to the Department of Justice (“DOJ”) asking it to investigate.
3 In the letter to the DOJ, Ms. Hatton wrote, “The proposed acquisition would produce a massive
4 consolidation of competitively sensitive healthcare data and shift such data from Change
5 Healthcare, a neutral third party, to Optum.”³

6 20. The DOJ investigated and filed a complaint to stop UHG’s transaction. In its
7 complaint, the DOJ described Change Healthcare as a technology company that operates “the
8 nation’s largest electronic data interchange (EDI) clearinghouse, which transmits data between
9 healthcare providers and insurers, allowing them to exchange insurance claims, remittances, and
10 other healthcare-related transactions . . . It has access to a vast trove of competitively sensitive
11 claims data that flows through its EDI clearinghouse—over a decade’s worth of historic data as
12 well as billions of new claims each year.”⁴

13 21. Moreover, according to the DOJ, “50 percent of all medical claims in the United
14 States pass through Change’s EDI clearinghouse.⁵ Change’s self-described ‘pervasive network
15 connectivity,’ including approximately ‘900,000 physicians, 118,000 dentists, 33,000 pharmacies,
16 5,500 hospitals and 600 laboratories,’ means that even when United’s health insurer rivals choose
17 not to be a Change customer, health insurers have no choice but to have their claims data pass
18 through Change’s EDI clearinghouse. Not only does Change process vast amounts of
19 competitively sensitive claims data, but it also has secured ‘unfettered’ rights to use over 60 percent
20 of this data for its own business purposes including, for example, using claims data for healthcare
21
22
23

24 ³ See [https://www.darkdaily.com/2021/04/07/aha-expresses-opposition-to-merger-between-](https://www.darkdaily.com/2021/04/07/aha-expresses-opposition-to-merger-between-unitedhealth-groups-optuminsight-and-change-healthcare-doj-agrees-to-look-into-the-13b-deal/)
25 [unitedhealth-groups-optuminsight-and-change-healthcare-doj-agrees-to-look-into-the-13b-deal/](https://www.darkdaily.com/2021/04/07/aha-expresses-opposition-to-merger-between-unitedhealth-groups-optuminsight-and-change-healthcare-doj-agrees-to-look-into-the-13b-deal/)
26 (last visited March 18, 2024).

27 ⁴ See <https://www.justice.gov/atr/case-document/file/1476901/dl> (last visited March 18, 2024).

28 ⁵ *Id.*

1 analytics. Additionally, through its claims editing product, Change has access to the proprietary
2 plan and payment rules for all of United’s most significant health insurance competitors.”⁶

3 22. The DOJ, however, lost its challenge to UHG’s acquisition of Change Healthcare
4 after a district judge ruled in UHG’s favor and the DOJ chose not to appeal.

5 23. In October 2022, Optum completed its combination with Change Healthcare.
6 According to a press release UHG issued, “The combined businesses share a vision for achieving
7 a simpler, more intelligent and adaptive health system for patients, payers and care providers. The
8 combination will connect and simplify the core clinical, administrative and payment processes
9 health care providers and payers depend on to serve patients. Increasing efficiency and reducing
10 friction will benefit the entire health system, resulting in lower costs and a better experience for
11 all stakeholders.”⁷

12 **B. The February 2024 Data Breach Exposed Significant Vulnerabilities in Defendants’**
13 **Computer Networks, Leading to the Shutdown of Critical Healthcare Infrastructure.**

14 24. On February 21, 2024, Defendants discovered the Data Breach and that their
15 computer networks were not secure and could not protect PHI and PII as required by state and
16 federal law. UHG set up a website regarding the Data Breach at www.unitedhealthgroup.com to
17 announce the Data Breach and stated that it disconnected the Change Healthcare systems.⁸ UHG
18 made a similar statement in a filing with the U.S. Securities and Exchange Commission.⁹ UHG
19 also stated, “The Company has retained leading security experts, is working with law
20 enforcement and notified customers, clients and certain government agencies . . . At this time,
21

22 ⁶ *Id.*

23
24 ⁷ See <https://www.optum.com/en/about-us/news/page.hub.optum-and-change-healthcare-complete-combination.html> (last visited March 18, 2024).

25
26 ⁸ See <https://www.unitedhealthgroup.com/newsroom/2024/2024-03-07-uhg-update-change-healthcare-cyberattack.html> (last visited March 18, 2024).

27
28 ⁹ See <https://www.sec.gov/Archives/edgar/data/731766/000073176624000045/unh-20240221.htm> (last visited March 18, 2024)

1 the Company believes the network interruption is specific to Change Healthcare systems, and all
2 other systems across the Company are operational.”¹⁰

3 25. UHG initially claimed that a nation-state actor was responsible for the Data Breach.
4 Blackcat, however, claimed responsibility for the Data Breach and stated on its dark web site that
5 it had stolen the confidential health and personal identifying information relating to millions of
6 Americans.

7 26. Specifically, Blackcat said it gained access to 6TB of data, including medical
8 records, and payment and claims information containing personally identifiable information like
9 names, contact information such as phone numbers and email addresses, and Social Security
10 Numbers.

11 27. Blackcat also claimed to have stolen Change Healthcare’s source code and the
12 confidential and sensitive information of CVS Caremark, Metlife, Health Net, Federal Medicare,
13 and Tricare.

14 28. Below is the statement that Blackcat issued regarding the cyberattack, indicating
15 that the group has reviewed a substantial amount of confidential medical and personal identifying
16 information:

17 Change Healthcare - Optum - UnitedHealth

18 2/28/2024, 4:19:59 PM

19 UnitedHealth has announced that the attack is “strictly related” to Change
20 Healthcare only and it was initially attributed to a nation state actor.

21 Two lies in one sentence.

22 Only after threatning [sic] them to announce it was us, they started telling a different
23 story.

24 It is true that the attack is centered at Change Healthcare production and corporate
25 networks, but why is the damage extremely high? Change Healthcare production
26 servers process extremely sensitive data to all of UnitedHealth clients that rely on
27 Change Healthcare technology solutions. Meaning thousands of healthcare
28 providers, insurance providers, pharmacies, etc . . .

¹⁰ *Id.*

1 Also, being inside a production network one can imagine the amount of critical and
2 sensitive data that can be found.

3 We were able to exfiltrate to be exact more than 6 TB of highly selective data. The
4 data relates to all Change Health clients that have sensitive data being processed by
5 the company.

6 The list of affected Change Health partners that we have sensitive data for is
7 actually huge with names such as:

- 8 - Medicare
- 9 - Tricare
- 10 - CVS-CareMark
- 11 - Loomis
- 12 - Davis Vision
- 13 - Health Net
- 14 - MetLife
- 15 - Teachers Health Trust
- 16 - Tens of insurance companies and others

17 Anyone with some decent critical thinking will understand what damage can be
18 done with such intimate data on the affected clients of UnitedHealth/UnitedHealth
19 solutions as well, beyond simple scamming/spamming.

20 After 8 days and Change Health have [sic] still not restored its operations and chose
21 to play a very risky game hence our announcement today.

22 So for everyone, both those affected and fellow associates. [sic] to understand what
23 is at stake our exfiltrated data includes millions of:

- 24 - active US military/navy personnel PII
- 25 - medical records
- 26 - dental records
- 27 - payments information
- 28 - Claims information
- 29 - Patients PII including Phone numbers/addresses/SSN/emails/etc ...
- 30 - 3000+ source code files for Change Health solutions (for source-code
31 review gents out there)
- 32 - Insurance records
- 33 - many many more

1 UnitedHealth you are walking on a very thin line be careful you just might fall over.

2 PS: For all those cyber intelligence so called expert . . . we did not use ConnectWise
3 exploit as our initial access so you should base your reports you tell people on actual
4 facts not kiddi [sic] speculations.

5 29. Screenshots of some of the data were reportedly shared as proof of the Data Breach.
6 On February 28, 2024, UHG confirmed that the Data Breach was perpetrated by Blackcat.

7 30. Blackcat has a reputation for engaging in “double extortion tactics,” that is,
8 exfiltrating confidential and sensitive data before using ransomware to encrypt the files.

9 31. On March 7, 2024, two weeks after the Data Breach, UHG said in a statement: “We
10 are working aggressively on the restoration of our systems and services.”¹¹ UHG also stated, “All
11 of us at UnitedHealth Group feel a deep sense of responsibility for recovery and are working
12 tirelessly to ensure that providers can care for their patients and run their practices, and that patients
13 can get their medications. We’re determined to make this right as fast as possible.”¹²

14 32. Shortly after Defendants publicly announced the Data Breach, the AHA issued a
15 security advisory notifying members and the public that “**Change Healthcare has not provided**
16 **a specific timeframe for which recovery of the impacted applications is expected**” (emphasis
17 in original).¹³ The AHA also recognized that hospitals and health systems “may be experiencing
18 challenges with obtaining care authorizations for their patients, as well as delays in payment.”¹⁴ It
19 stated that it was in communication with the Department of Health and Human Services, including
20 the Centers for Medicare & Medicaid Services, about “options to support patients’ timely access
21
22

23 ¹¹ See [https://www.unitedhealthgroup.com/newsroom/2024/2024-03-07-uhg-update-change-](https://www.unitedhealthgroup.com/newsroom/2024/2024-03-07-uhg-update-change-healthcare-cyberattack.html)
24 [healthcare-cyberattack.html](https://www.unitedhealthgroup.com/newsroom/2024/2024-03-07-uhg-update-change-healthcare-cyberattack.html) (last visited March 18, 2024).

25 ¹² *Id.*

26 ¹³ See [https://www.aha.org/2024-02-24-update-unitedhealth-groups-change-healthcares-](https://www.aha.org/2024-02-24-update-unitedhealth-groups-change-healthcares-continued-cyberattack-impacting-health-care-providers)
27 [continued-cyberattack-impacting-health-care-providers](https://www.aha.org/2024-02-24-update-unitedhealth-groups-change-healthcares-continued-cyberattack-impacting-health-care-providers) (last visited March 18, 2024).

28 ¹⁴ *Id.*

1 to care and provide temporary financial support to providers. We also are having these discussions
2 with Optum. We will provide more information as it becomes available.”¹⁵

3 33. In a letter to Health and Human Services, the AHA stated that while the full scope
4 was “unknown,” the AHA expected impacts to be far-reaching given Change Healthcare’s national
5 presence.¹⁶ The AHA also explained how the incident has affected healthcare providers in terms
6 of being unable to collect revenue. “[W]ithout this critical revenue source, hospitals and health
7 systems may be unable to pay salaries for clinicians and other members of the care team, acquire
8 necessary medicines and supplies, and pay for mission critical contract work in areas such as
9 physical security, dietary and environmental services,” the AHA stated.¹⁷ “In addition, replacing
10 previously electronic processes with manual processes will add considerable administrative costs
11 on providers, as well as divert team members from other tasks. It is particularly concerning that
12 while Change Healthcare’s systems remain disconnected, it and its parent entities benefit
13 financially, including by accruing interest on potentially billions of dollars that belong to health
14 care providers.”¹⁸

15 34. Antitrust experts have opined that the Data Breach shows why placing “one
16 conglomerate at the center of multiple health care functions is inherently risky.”¹⁹

17 //

22 ¹⁵ *Id.*

23 ¹⁶ *See* [https://www.aha.org/lettercomment/2024-02-26-aha-letter-hhs-implications-change-](https://www.aha.org/lettercomment/2024-02-26-aha-letter-hhs-implications-change-healthcare-cyberattack)
24 [healthcare-cyberattack](https://www.aha.org/lettercomment/2024-02-26-aha-letter-hhs-implications-change-healthcare-cyberattack) (last visited March 18, 2024).

25 ¹⁷ *Id.*

26 ¹⁸ *Id.*

27 ¹⁹ *See* [https://www.statnews.com/2024/02/27/change-healthcare-cyber-attack-reveals-](https://www.statnews.com/2024/02/27/change-healthcare-cyber-attack-reveals-consolidation-risks/)
28 [consolidation-risks/](https://www.statnews.com/2024/02/27/change-healthcare-cyber-attack-reveals-consolidation-risks/) (last visited March 18, 2024).

1 **C. The Data Breach and Shutdown have Created a National Crisis in the Healthcare**
2 **Industry, Severely Impacting the Financial Security of Hundreds of Thousands of**
3 **Healthcare Providers.**

4 35. The Data Breach and resulting shutdown have had reverberations across the U.S.
5 healthcare industry that continue today, and the fallout is placing healthcare providers in a
6 precarious situation.

7 36. Since the discovery of the vulnerabilities in Defendants' computer networks on
8 February 21, 2024, many healthcare providers have been unable to submit claims to insurers for
9 payment, and many have not received payments for claims submitted before February 21, 2024.
10 One physician, Dr. Purvi Parikh, told CNBC that her practice has not been paid by insurers for her
11 patients' visits, which creates problems for paying operational expenses like medical supplies and
12 payroll.²⁰ Dr. Parikh said there were no immediate workarounds and that it could take weeks to
13 change to a new platform.²¹

14 37. Licensed clinical social worker Jenna Wolfson reported that she has been unable to
15 receive any payments due to the Data Breach and that many of her colleagues are facing the same
16 problems.²² According to Wolfson, "There are people right now that might not see payment on the
17 work that they're doing today for months, and they still have an entire practice to keep above
18 water."²³

19 38. Dr. Margaret Parsons, a dermatologist at a 20-person practice in Sacramento,
20 California, told KFF Health News that she and her colleagues have not been able to electronically
21 submit claims for payment since February 21, 2024 and that the payment process for California's
22
23

24 ²⁰ *Id.*

25 ²¹ *Id.*

26 ²² *See* [https://healthitsecurity.com/features/understanding-the-impact-of-the-change-healthcare-](https://healthitsecurity.com/features/understanding-the-impact-of-the-change-healthcare-cyberattack-on-providers)
27 [cyberattack-on-providers](https://healthitsecurity.com/features/understanding-the-impact-of-the-change-healthcare-cyberattack-on-providers) (last visited March 18, 2024).

28 ²³ *Id.*

1 Medicare Program does not accept paper claims which usually take 3-6 months to process.²⁴ “We
2 will be in trouble in very short order, and are very stressed,” said Dr. Parsons.²⁵

3 39. Dr. Stephen Sisselman, an independent primary care physician in New York, said,
4 “How can you pay staff, supplies, malpractice insurance – all this – without revenue? It’s
5 impossible.”²⁶

6 40. If the shutdown lasts a month, Jackson Health Systems, in Miami-Dade Florida,
7 will be short on as much as \$30 million in payments, according to its chief revenue officer.²⁷

8 41. According to the president of Florida Hospital Association, Mary Mayhew, her
9 members built “sophisticated systems that are reliant on Change Healthcare,”²⁸ and that changing
10 processes could take about 90 days during which they will have no cash flow. “It’s not like flipping
11 a switch,” said Mayhew.²⁹

12 42. On March 13, 2024, the AHA wrote to Senators Ron Wyden and Mike Crapo about
13 the Data Breach. According to the AHA’s letter, the downed systems “are hampering providers’
14 ability to verify patients’ health insurance coverage, process claims and receive payment from
15 many payers, exchange clinical records with other providers, provide cost estimates and bill
16 patients, and in some instances, access the clinical guidelines used in clinical decision support tools
17 and as part of the prior authorization process.”³⁰

18
19 _____
20 ²⁴ See <https://www.npr.org/sections/health-shots/2024/03/09/1237038928/health-industry-ransomware-cyberattack-change-healthcare-optum-uhc-united> (last visited March 18, 2024).

21 ²⁵ *Id.*

22 ²⁶ *Id.*

23 ²⁷ *Id.*

24 ²⁸ *Id.*

25 ²⁹ *Id.*

26 ³⁰ See <https://www.aha.org/lettercomment/2024-03-13-aha-urges-more-congressional-action-help-providers-affected-change-healthcare-cyberattack> (last visited March 18, 2024).

1 43. Moreover, the AHA reported in its March 13th letter that in response to a recent
2 AHA survey of hospitals with nearly 1,000 responses, “74% reported direct patient care impact,
3 including delays in authorizations for medically necessary care.”³¹ Further, the AHA reported that:

4 [H]ospitals, health systems and other providers are experiencing extraordinary
5 reductions in cash flow, threatening their ability to make payroll and to acquire
6 the medical supplies needed to provide care. In the same survey, 94% of hospitals
7 reported that the Change Healthcare cyberattack was impacting them financially,
8 with more than half reporting the impact as “significant or serious.” Indeed, a third
9 of the survey respondents indicated that the attack has disrupted more than half of
10 their revenue. The urgency of this matter grows by the day.³²

11 44. To make matters worse, on March 18, 2024, ratings agency Fitch said that
12 certain healthcare providers that use its services may see a hit to their credit profile as a
13 result of the Data Breach’s impact on cash flows.³³

14 **D. The Data Breach and Resulting Shutdown were Foreseeable Risks of Which Defendants
15 were on Notice and Could Have Prevented.**

16 45. Cybercriminals target the healthcare industry the most due to the treasure trove of
17 confidential health and personal information maintained and stored by healthcare organizations.
18 In 2023, the FBI reported 249 ransomware attacks in the healthcare industry.³⁴ Cyberattacks have
19 doubled from 2016 to 2021 and have resulted in the exposure of personal health information for
20 approximately 42 million patients.³⁵

21 46. The FBI warned healthcare stakeholders as early as 2014 that they are the target of
22 hackers, stating “[t]he FBI has observed malicious actors targeting healthcare related systems,
23
24

25 ³¹ *Id.*

26 ³² See <https://www.aha.org/lettercomment/2024-03-13-aha-urges-more-congressional-action-help-providers-affected-change-healthcare-cyberattack> (last visited March 18, 2024).

27 ³³ See <https://www.reuters.com/business/healthcare-pharmaceuticals/fitch-says-unitedhealth-unit-hack-could-hit-smaller-pharmacies-care-providers-2024-03-18/> (last visited March 18, 2024).

28 ³⁴ See <https://www.npr.org/sections/health-shots/2024/03/09/1237038928/health-industry-ransomware-cyberattack-change-healthcare-optum-uhc-united> (last visited March 18, 2024).

³⁵ See <https://www.ncbi.nlm.nih.gov/pmc/articles> (last visited March 18, 2024).

1 perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally
2 Identifiable Information (PII).”³⁶

3 47. In 2017, the Department of Health and Human Services released a ransomware fact
4 sheet making it clear to entities covered by the Health Insurance Portability and Accountability
5 Act (“HIPAA”) that “[w]hen electronic protected health information (ePHI) is encrypted as the
6 result of a ransomware attack, a breach has occurred because the ePHI encrypted by the
7 ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the
8 information), and thus is a “disclosure” not permitted under the HIPAA Privacy Rule.”³⁷

9 48. Under the HIPAA Privacy Rules, a breach is defined as, “[t]he acquisition, access,
10 use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which
11 compromises the security or privacy of the PHI.”³⁸ Accordingly, a ransomware attack such as the
12 one that occurred on February 21, 2024 is considered a breach under the HIPAA Rules because
13 there was an access of PHI not permitted under the HIPAA Privacy Rule.

14 49. A ransomware attack is also considered a “Security Incident” under HIPAA.
15 Under the HIPAA Rules, a “Security Incident” is defined as “the attempted or successful
16 unauthorized access, use, disclosure, modification, or destruction of information or interference
17 with system operations in an information system.” 45 CFR § 164.304. According to the
18 Department of Health and Human Services, “[t]he presence of ransomware (or any malware) on a
19 covered entity’s or business associate’s computer systems is a security incident under the HIPAA
20 Security Rule.”³⁹

21
22 _____
23 ³⁶ See [https://publicintelligence.net/fbi-targeting-healthcare20\(PII\)](https://publicintelligence.net/fbi-targeting-healthcare20(PII)) (last visited March 18, 2024).

24 ³⁷ See <https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet/index.html> (last visited March 18, 2024).

25 ³⁸ See <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html> (last visited
26 March 18, 2024).

27 ³⁹ See <https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet>
28 (last visited March 18, 2024).

1 50. Data Breaches can be prevented. Approximately 80% of ransomware is delivered
2 through email phishing attacks. Other means to deliver ransomware is through brute force attacks
3 on open remote desktop protocol ports. To prevent ransomware attacks, organizations must provide
4 training to its employees for the handling of suspicious emails. They can also disable macros, avoid
5 storing passwords in plain text, and perform hunts and search for suspicious behavior in their
6 networks, among other things.

7 51. This is not the first time that the UHG family has dealt with a data breach. In May
8 2023, United HealthCare, a UHG subsidiary, had to notify members that protective health
9 information may have been compromised due to a credential stuffing attack that occurred on the
10 United Healthcare mobile app in February 2023.⁴⁰

11 52. Accordingly, Defendants knew, given the vast amount of PHI and PII that
12 healthcare providers such as Plaintiff and Class members acquire and transmit to Defendants
13 directly or through vendors and that in turn, Defendants store and maintain, that they were a target
14 for cybercriminals and should have taken all reasonable measures to avoid cyberattacks.
15 Defendants also understood the risks posed by their insecure data security practices and computer
16 networks. Defendants' failure to heed warnings and failure to adequately maintain their computer
17 networks secure resulted in the shutdown and harm to Plaintiff and Class members.

18 **E. Defendants, at all Relevant Times, had a Duty to Plaintiff and Class Members.**

19 53. Defendants marketed their services to Plaintiff and Class members, and were aware,
20 at all relevant times, that healthcare providers such as Plaintiff and Class members handle PHI and
21 PII on a daily basis and that they are required by law to keep such data confidential. Thus,
22 Defendants were required by law to properly secure their computer networks and encrypt and
23 maintain PHI and PII using industry standard methods, utilize available technology to defend their
24 computer networks from invasion, and act reasonably to prevent foreseeable harms.

25
26
27 _____
28 ⁴⁰ See <https://www.hipaajournal.com/credential-stuffing-attack-exposed-united-healthcare-member-data/> (last visited March 18, 2024).

1 54. Defendants’ duty to use reasonable security measures arose as a result of the special
2 relationship that existed between them, on the one hand, and Plaintiff and the other Class members,
3 on the other hand. The special relationship arose because Plaintiff and the members of the Class
4 entrusted Defendants (or their partners who entrusted Defendants) with PHI and PII. Defendants
5 had the resources necessary to prevent the Data Breach and to protect their computer networks but
6 neglected to adequately invest in security measures, despite their obligations to protect such
7 information. Accordingly, Defendants breached their common law, statutory and other owed duties
8 to Plaintiff and Class members.

9 55. Defendants’ duty to use reasonable security measures also arose under HIPAA.
10 UHG is covered by HIPAA and as such is required to comply with the HIPAA Privacy Rule and
11 Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E (“Standards for Privacy of
12 Individually Identifiable Health Information”), and Security Rule (“Security Standards for the
13 Protection of Electronic Protected Health Information”), 45 C.F.R. Part 160 and Part 164, Subparts
14 A and C. Under HIPAA, Defendants were required to “reasonably protect” PHI from “any
15 intentional or unintentional use or disclosure” and to “have in place appropriate administrative,
16 technical, and physical safeguards to protect the privacy of protected health information.” 45
17 C.F.R. § 164.530(c)(1).

18 56. Under HIPAA, Defendants were specifically required to do the following:

- 19 • Ensure the confidentiality and integrity of electronic PHI they created, received,
20 maintained, and/or transmitted. 45 C.F.R. § 164.306(a)(1);
- 21 • Implement technical policies and procedures for electronic information systems
22 that maintain electronic PHI to allow access only to those persons or software
23 programs that have been granted access rights. 45 C.F.R. § 164.312(a)(1);
- 24 • Implement adequate policies and procedures to prevent detect, contain, and
25 correct security violations. 45 C.F.R. § 164.308(a)(1)(i);
- 26 • Implement adequate procedures to review records of information system
27 activity regularly, such as audit logs, access reports, and security incident
28 tracking reports. 45 C.F.R. § 164.308(a)(1)(ii)(D);

- 1 • Protect against reasonably anticipated threats or hazards to the security or
2 integrity of electronic PHI. 45 C.F.R. § 164.306(a)(2);
- 3 • Protect against reasonably anticipated uses or disclosures of electronic PHI that
4 are not permitted under the privacy rules regarding individually identifiable
5 health information. 45 C.F.R. § 164.306(a)(3);
- 6 • Ensure compliance with HIPAA security standard rules by its workforces. 45
7 C.F.R. § 164.306(a)(4);
- 8 • Train all members of its workforces effectively on the policies and procedures
9 regarding PHI as necessary and appropriate for the members of its workforces
10 to carry out their functions and to maintain security of PHI. 45 C.F.R. §
11 164.530(b); and/or
- 12 • Render the electronic PHI they maintained unusable, unreadable, or
13 indecipherable to unauthorized individuals, as Defendants had not encrypted
14 the electronic PHI as specified in the HIPAA Security Rule by “the use of an
15 algorithmic process to transform data into a form in which there is a low
16 probability of assigning meaning without use of a confidential process or key”
17 (45 CFR § 164.304 definition of encryption).

18 57. Defendants’ duty to use reasonable security measures also arose under Section 5 of
19 the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or
20 affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of
21 failing to use reasonable measures to protect confidential data by entities like Defendants.

22 58. The Data Breach and resulting shutdown of the Change Healthcare networks were
23 a direct and proximate result of Defendants’ failure to: (1) properly safeguard and protect computer
24 networks with PHI and PII from unauthorized access, use, and disclosure, as required by various
25 state and federal regulations, industry practices, and common law; (2) establish and implement
26 appropriate safeguards to ensure the security and confidentiality of PHI and PII; and (3) protect
27 against reasonably foreseeable threats to the security or integrity of such information and computer
28 networks.

F. Plaintiff’s Experience

1
2 59. Plaintiff Bay Area Therapy Group a Marriage and Family Counseling Corp.
3 (“BATG”) is a licensed healthcare provider serving patients in the Bay Area.

4 60. Plaintiff BATG contracts with ICANotes, an integrated practice management
5 system that provides healthcare providers with tools to streamline their operations.

6 61. ICANotes, in turn, partners with Change Healthcare to process insurance claims
7 submitted by its clients, among other things. Specifically, healthcare providers such as Plaintiff
8 BATG submit their claims to ICANotes, which in turn uses Change Healthcare to process them
9 with insurance and healthcare plans who then issue payments to providers.

10 62. Beginning on or around February 21, 2024, when Defendants’ systems were shut
11 down as a result of the Data Breach, Plaintiff BATG could no longer submit claims through
12 ICANotes and obtain payments for those claims. Moreover, Plaintiff BATG has been unable to
13 receive payments for claims submitted on February 20, 2024. Since the shutdown, Plaintiff BATG
14 has not been paid for any claims despite continuing to treat patients. Plaintiff BATG relies on the
15 payments it receives from submitted claims to pay basic business expenses, including salaries and
16 wages to employees, and to further grow the practice, including hiring additional therapists to treat
17 patients.

18 63. As a result of Defendants’ failure to maintain the security of their computer
19 networks, Plaintiff BATG has had to take out emergency loans with interest rates of 50% to meet
20 payroll and pay other basic expenses. Plaintiff BATG’s staff resources have also been diverted
21 from treating patients at full capacity to trying to resolve the cash flow problems caused by the
22 shutdown of Defendants’ computer networks. Plaintiff BATG has also had to contract with another
23 vendor to replace ICANotes, which has increased Plaintiff BATG’s administrative costs.

24 64. Plaintiff BATG was eligible for only \$500 from Defendants’ assistance program,
25 which was woefully insufficient to run its practice.

V. CLASS ACTION ALLEGATIONS

65. Plaintiff brings this action individually and on behalf of all other persons similarly situated (the “Nationwide Class”) pursuant to the Federal Rule of Civil Procedure 23(b)(2), (b)(3), and (c)(4).

66. The Nationwide Class is initially defined as follows:

All healthcare providers in the United States whose use of Change Healthcare’s services was disrupted by the Data Breach.

67. Additionally, pursuant to the Federal Rule of Civil Procedure 23(b)(2), (b)(3), and (c)(4), Plaintiff brings this action on behalf of the following California Class initially defined as:

All healthcare providers in the state of California whose use of Change Healthcare’s services was disrupted by the Data Breach.

68. The Nationwide Class and the California Class are referred to herein as “Class,” unless otherwise stated.

69. Excluded from the proposed Class are Defendants, any entity in which Defendants have a controlling interest, is a parent or subsidiary, or which is controlled by Defendants, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendants; and judicial officers to whom this case is assigned and their immediate family members.

70. Plaintiff reserves the right to re-define the Class definitions after conducting discovery.

71. **Numerosity (Fed. R. Civ. P. 23(a)(1)).** The Class members are so numerous that joinder of all members is impracticable. Based on information and belief, the Class includes over one million licensed healthcare providers. The parties will be able to identify the exact size of the Class through discovery and Defendants’ records.

72. **Commonality and Predominance (Fed. R. Civ. P. 23(a)(2); 23(b)(3)).** Common questions of law and fact exist for each of the claims and predominate over questions affecting only individual members of the Class. Questions common to the Class include, but are not limited to, the following:

- 1 a. Whether Defendants breached their legal duty to Plaintiff and Class members;
- 2 b. Whether Defendants had a special relationship with Plaintiff and Class members;
- 3 c. Whether Defendants are liable for negligence to Plaintiff and Class members;
- 4 d. Whether Defendants negligently interfered with Plaintiff and Class members’
- 5 prospective economic advantage;
- 6 e. Whether Defendants committed unfair business practices in violation of
- 7 California’s UCL;
- 8 f. Whether Defendants committed unlawful business practices in violation of
- 9 California’s UCL;
- 10 g. Whether Plaintiff and Class members suffered legally cognizable damages as a
- 11 result of Defendants’ conduct; and
- 12 h. Whether Plaintiff and Class members are entitled to relief, including damages and
- 13 equitable relief.

14 **73. Typicality (Fed. R. Civ. P. 23(a)(3)).** Pursuant to Rule 23(a)(3), Plaintiff’s
15 claims are typical of the claims of the Class members. Plaintiff, like all Class members, suffered
16 harm as a result of the Data Breach and ensuing shutdown of Defendants’ computer networks.

17 **74. Adequacy of Representation (Fed. R. Civ. P. 23(a)(4)).** Pursuant to Rule
18 23(a)(4), Plaintiff and its counsel will fairly and adequately protect the interests of the Class.
19 Plaintiff has no interest antagonistic to, or in conflict with, the interests of the Class members.
20 Plaintiff has retained counsel experienced in prosecuting class actions and data breach cases.

21 **75. Superiority (Fed. R. Civ. P. 23(b)(3)).** Pursuant to Rule 23(b)(3), a class
22 action is superior to individual adjudications of this controversy. Litigation is not economically
23 feasible for individual Class members because the amount of monetary relief available to
24 individual plaintiffs is insufficient in the absence of the class action procedure. Separate litigation
25 could yield inconsistent or contradictory judgments and increase the delay and expense to all
26 parties and the court system. A class action presents fewer management difficulties and provides
27 the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single
28 court.

1 80. Defendants' duty to use reasonable security measures arose as a result of
2 the special relationship that existed between them and Plaintiff and Class members, which is
3 recognized by state and federal law, including but not limited to HIPAA. Only Defendants,
4 however, were in a position to ensure that their computer networks were sufficient to protect
5 against the harm to Plaintiff and the Class members that resulted from the Data Breach and ensuing
6 shutdown.

7 81. Defendants violated these standards and duties by failing to exercise reasonable
8 care in safeguarding and protecting PHI and PII on their network systems by failing to design,
9 adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security
10 processes, controls, policies, procedures, protocols, and software and hardware systems to
11 safeguard and protect PHI and PII entrusted to them. It was reasonably foreseeable to Defendants
12 that their failure to exercise reasonable care in safeguarding and protecting PHI and PII by failing
13 to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data
14 security processes, controls, policies, procedures, protocols, and software and hardware systems
15 would result in harm to Plaintiff and Class members.

16 82. Defendants, by and through their negligent actions, inaction, omissions, and want
17 of ordinary care, unlawfully breached their duties to Plaintiff and Class members by, among other
18 things, failing to exercise reasonable care in safeguarding and protecting their data networks and
19 PHI and PII within their possession, custody and control, which resulted in the shutdown of
20 Defendants' computer networks and disrupted Plaintiff and Class members' businesses.

21 83. Defendants, by and through their negligent actions, inactions, omissions, and want
22 of ordinary care, further breached their duties to Plaintiff and Class members by failing to design,
23 adopt, implement, control, direct, oversee, manage, monitor and audit their processes, controls,
24 policies, procedures, protocols, and software and hardware systems for complying with the
25 applicable laws and safeguarding and protecting PHI and PII.

26 84. But for Defendants' negligent breach of the above-described duties owed to
27 Plaintiff and Class members, Defendants would not have experienced the Data Breach and would
28 not have had to shutdown the Change Healthcare networks, thereby preventing Plaintiff and Class

1 members from (i) timely receiving payments for previously submitted claims, (ii) submitting new
2 claims for payment, and (iii) obtaining insurance authorization for patient medical treatment,
3 among other things. The harms to Plaintiff and Class members were foreseeable given the types
4 of services Defendants provide and the statutory obligations shared by all to protective computer
5 networks and confidential PHI and PII.

6 85. Defendants' wrongful actions, inaction, omissions, and want of ordinary care that
7 directly and proximately caused the Data Breach and resulted in the shutdown of the Change
8 Healthcare computer networks constitute negligence.

9 86. As a direct and proximate result of Defendants' wrongful actions, inaction,
10 omissions, and want of ordinary care that directly and proximately caused the Data Breach and the
11 related shutdown, Plaintiff and Class members have suffered (and will continue to suffer) monetary
12 losses and economic harms and seek all available damages.

13 **COUNT II**
14 **NEGLIGENT INTERFERENCE WITH PROSPECTIVE ECONOMIC ADVANTAGE**
15 **(On Behalf of Plaintiff and the California Class)**

16 87. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth
17 herein.

18 88. Plaintiff had an ongoing business relationship with ICANotes that would have
19 likely resulted in future economic benefits to Plaintiff.

20 89. Defendants knew or should have known about Plaintiff's relationship with
21 ICANotes due to the integration of Change Healthcare's services and processes with ICANotes.

22 90. Defendants knew or should have known that Plaintiff's relationship with ICANotes
23 and Plaintiff's operations would be disrupted if Defendants failed to act with reasonable care in
24 properly maintaining the security of their computer networks from cyberattack.

25 91. The harm to Plaintiff resulting from the Data Breach and shutdown was foreseeable.

26 92. Defendants failed to act with reasonable care and engaged in wrongful conduct,
27 including by violating like the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C.
28 § 1302d, *et. seq.*), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), California's Confidentiality

1 of Medical Information Act (Civil Code §56, *et seq.*), and California’s Insurance Information and
2 Privacy Protection Act (Ins. Code §791, *et seq.*).

3 93. The relationship between Plaintiff and ICANotes has been disrupted, resulting in
4 economic harm to Plaintiff.

5 94. Defendants’ wrongful conduct was a substantial factor in causing the harm to
6 Plaintiff and Class members. Plaintiff and Class members seek all available damages.

7 **COUNT III**
8 **UNJUST ENRICHMENT**
9 **(On Behalf of Plaintiff and the Nationwide Class)**

10 95. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set
11 forth herein.

12 96. Plaintiff and Class members conferred benefits on Defendants in the form of
13 payments for claims management and processing, insurance verification, authorization and
14 medical necessity reviews, and disbursement of payments, among other things, both directly and
15 indirectly. Defendants had knowledge of the benefits conferred by Plaintiff and Class members
16 and appreciated such benefits. Defendants should have used, in part, the monies Plaintiff and Class
17 members paid to it, directly and indirectly, to pay the costs of reasonable data privacy and security
18 practices and procedures.

19 97. Plaintiff and Class members have suffered actual damages and harm as a
20 result of Defendants’ conduct, inactions, and omissions. Defendants should be required to disgorge
21 into a common fund for the benefit of Plaintiff and Class members all unlawful or inequitable
22 proceeds received from Plaintiff and Class members.

23 **COUNT IV**
24 **VIOLATION OF CALIFORNIA’S UNFAIR COMPETITION LAW, CAL. BUS. & PROF.**
25 **CODE §§ 17200, ET SEQ.**
26 **(On Behalf of Plaintiff and the California Class)**

27 98. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth
28 herein.

99. Defendants have violated Cal. Business and Professions Code §17200, *et seq.* by
engaging in unlawful and unfair practices as defined in Cal. Bus. Prof. Code §17200.

1 100. Defendants engaged in unfair acts and practices by failing to maintain reasonable
2 security practices and procedures as alleged herein and as required by law. These unfair acts and
3 practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially
4 injurious to Plaintiff and California Class Members. Defendants' practices were also contrary to
5 legislatively declared and public policies that call for the protection of consumer data and ensure
6 that entities who are entrusted with PHI and PII utilize appropriate security measures, as reflected
7 by laws like the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d, *et*
8 *seq.*), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), California's Confidentiality of Medical
9 Information Act (Civil Code §56, *et seq.*), and California's Insurance Information and Privacy
10 Protection Act (Ins. Code §791, *et seq.*). The harm these practices caused to Plaintiff and the
11 California Class Members outweighed their utility, if any.

12 101. Defendants engaged in unlawful business practices by violating the Federal Trade
13 Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d, *et seq.*), the Gramm-Leach-Bliley
14 Act (15 U.S.C. § 6801), California's Confidentiality of Medical Information Act (Civil Code § 56
15 *et seq.*), and California's Insurance Information and Privacy Protection Act (Ins. Code §791, *et*
16 *seq.*).

17 102. As a result of Defendants' acts of unfair and unlawful practices and acts,
18 Plaintiff was injured and lost money or property.

19 103. Defendants knew or should have known that their computer networks and data
20 security practices were inadequate to safeguard against ransomware attacks, would result in the
21 Data Breach, and ultimately in the shutdown of Defendants' computer networks. Defendants'
22 actions in engaging in the unfair practices and unlawful acts alleged herein were negligent,
23 knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and members
24 of the California Class.

25 104. Plaintiff and California Class Members seek relief under Cal. Bus. & Prof. Code §
26 17200, *et seq.*, including, but not limited to, restitution to Plaintiff and Class Members of money
27 or property that the Defendants may have acquired by means of their unlawful and unfair business
28 practices, restitutionary disgorgement of all profits accruing to Defendants because of their

1 unlawful and unfair business practices, declaratory relief, attorney’s fees and costs (pursuant to
2 Cal. Code Civil Pro. §1021.5), and injunctive or other equitable relief.

3 105. Plaintiff and the proposed Class members are entitled to equitable relief, including
4 restitution to compensate Plaintiff and the Class as a result of Defendants’ unlawful and unfair
5 practices, and an injunction enjoining Defendants’ misconduct as alleged herein and directing
6 Defendants to implement reasonable security policies and practices to protect their computer
7 networks and PHI and PII. Plaintiff, the Class, and members of the public will suffer irreparable
8 injury if an injunction is not ordered because they are at risk of incurring additional losses,
9 including due to the disruption of their businesses and the increased risk of harm of identity theft
10 to patients. Plaintiff and Class members will also suffer irreparable injury if Defendants’ unlawful
11 and unfair practices are not enjoined. Plaintiff and Class members entrusted confidential PHI and
12 PII to Defendants and therefore they have an interest in ensuring that Defendants take the necessary
13 steps to protect their computer networks and the PHI and PII stored thereon, but absent an
14 injunction they have no way of determining whether Defendants are complying with state and
15 federal laws and reasonable standards of care.

16 106. Plaintiff brings this claim on behalf of the Class in the alternative to any claims
17 brought for legal remedies and expressly alleges that for purposes of this claim that it lacks
18 adequate remedies at law. In addition, the restitution that may be available under this claim,
19 including for restitutionary disgorgement of revenues attributable to the challenged practices, may
20 not be recoverable as damages or otherwise at law. Plaintiff, individually and as a member of the
21 Class, has no adequate remedy at law for the future unlawful acts, methods, or practices as set
22 forth above absent an injunction. Moreover, future damages are not certain or prompt and thus are
23 an inadequate remedy to address the conduct that injunctions are designed to prevent.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the members of the Class defined above, respectfully request that this Court enter:


- (a) An order certifying this case as a class action under Federal Rule of Civil Procedure 23, appointing Plaintiff as the Class representative, and appointing the undersigned as Class counsel;
- (b) A judgment awarding Plaintiff and Class members appropriate monetary relief, including actual damages, equitable relief, restitution, and disgorgement;
- (c) An order entering injunctive and declaratory relief as appropriate under the applicable law;
- (d) An order awarding Plaintiff and the Class pre-judgment and/or post-judgment interest as prescribed by law;
- (e) An order awarding reasonable attorneys’ fees and costs as permitted by law; and
- (f) Any and all other and further relief as may be just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial.

Dated: March 18, 2024

GIBBS LAW GROUP LLP



Rosemary M. Rivas
David M. Berger
Rosanne L. Mah
1111 Broadway, Suite 2100
Oakland, California 94607
(510) 350-9700 (tel.)
(510) 350-9701 (fax)
rmr@classlawgroup.com
dmb@classlawgroup.com
rlm@classlawgroup.com

Attorneys for Plaintiff