Ryan J. Clarkson (SBN 257074)
rclarkson@clarksonlawfirm.com
Yana Hart (SBN 306499)
yhart@clarksonlawfirm.com
CLARKSON LAW FIRM, P.C.
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050
Fax: (213) 788-4070

Tina Wolfson (SBN 174806)
twolfson@ahdootwolfson.com
Andrew W. Ferich (admitted *pro hac vice*)
aferich@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Ave. Suite 500
Burbank, CA 91505
Tel: (310) 474-9111
Fax: (310) 474-8585

[Additional counsel appear on signature page]

Counsel for Plaintiffs and the Proposed Class

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF LOS ANGELES

HEATHER HEATH, BRIAN HEINZ, MATTHEW RUTLEDGE, ROBERT RUMA, and ANDREA HANS, individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

KEENAN & ASSOCIATES, and DOES 1 through 20, inclusive,

Defendant.

Case No. 24STCV03018

SECOND AMENDED CLASS ACTION COMPLAINT

1. NEGLIGENCE
2. NEGLIGENCE PER SE
3. BREACH OF IMPLIED CONTRACT
4. BREACH OF FIDUCIARY DUTY
5. BREACH OF CONFIDENCE
6. VIOLATIONS OF THE CALIFORNIA UNFAIR COMPETITION LAW, BUSINESS AND PROFESSIONS CODE §§ 17200, *et seq.*
7. VIOLATIONS OF THE CALIFORNIA CONSUMER PRIVACY ACT, CAL. CIV. CODE §§ 1798.150, *et seq.*
8. VIOLATIONS OF THE CALIFORNIA CONFIDEDENTIALITY OF MEDICAL INFORMATION ACT, CA. CIV. CODE §§ 56, *et seq.*
9. VIOLATIONS OF THE CALIFORNIA CUSTOMER RECORDS ACT, CAL. CIV. CODE §§ 1798.80, *et seq.*
10. INVASION OF PRIVACY
11. UNJUST ENRICHMENT

DEMAND FOR JURY TRIAL

Plaintiffs Heather Heath, Brian Heinz, Matthew Rutledge, Andrea Hans, and Robert Ruma ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this Action against Defendant Keenan & Associates ("Keenan" or "Defendant") for its failure to properly safeguard their protected health information and personally identifiable information stored within Defendant's information network. Plaintiffs' allegations are based on personal knowledge as to themselves and their own acts, and upon information and belief as to all other matters based on the investigation conducted by and through Plaintiffs' attorneys.

INTRODUCTION

1. This class action arises out of the recent data breach (the "Data Breach") involving Keenan, which collected and stored certain personally identifiable information ("PII") and protected health information ("PHI") (collectively, "Private Information") of Plaintiffs and class members.

2. Keenan was the largest private insurance broker in California before merging with Assured Partners, Inc. in 2017.[1] Today, the Assured Partners family of companies commands over $1 billion in revenue and is the twelfth largest broker in the United States.[2] As a private company and a subsidiary, Keenan—a California based insurance brokerage firm—has maintained its position as an industry leader for a particular brand of insurance: employee benefit coverage in education, healthcare, and public agencies.[3] Keenan's "innovative solutions" are designed "specifically for California educational institutions, public agencies, and health care organizations."[4] Keenan's operations are limited to seven locations, all in California: Torrance, Riverside, San Clemente, Oakland, San Jose, Rancho Cordova, and Pleasanton.[5]

3. To effectively manage coverage for millions of Californians, Keenan stores significant sensitive Private Information. Keenan owes a duty to the individuals whose data Keenan obtains and

[1] *Our History and Background*, KEENAN, https://www.keenan.com/About/History (last visited June 17, 2024).
[2] *Id.*
[3] *K-12 Schools, Community Colleges and Charter School Insurance Specialists*, KEENAN, https://www.keenan.com/Industries/Education (last visited Sept. 6, 2024); *see also Healthcare System, Hospital, and Medical Group Insurance Specialists*, KEENAN, https://www.keenan.com/Industries/Health-Care (last visited Sept. 6, 2024); *Public Agency Insurance Specialists*, KEENAN, https://www.keenan.com/Industries/Public-Agencies (last visited Sept. 6, 2024).
[4] *About Keenan*, KEENAN, www.keenan.com/About (last visited June 17, 2024).
[5] *Office Locations,* KEENAN, www.keenan.com/About/Office-Locations (last visited Sept. 6, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

maintains. This duty arises because it is foreseeable that the exposure of Private Information to unauthorized persons, especially to perpetrators of cyberattacks with nefarious intentions, will result in harm to the affected individuals, including, but not limited to: the invasion of their private data, the sale of their Private Information to facilitate identity theft, exposure to scams or phishing frauds, loss of time, economic damages as affected individuals scramble to protect their identities, and/or the countless ways these individuals' peace of mind is destroyed knowing their information is no longer secured.

4. Given the dire consequences of compromised Private Information, individuals expect their data to be securely protected. Unfortunately, this trust is misplaced and violated when entities, like Defendant, subject themselves to the risk of cyberattacks.

5. The U.S. Department of Health and Human Services ("HHS") has warned organizations who hold PHI of the threat posed by ongoing ransomware attacks. The U.S. Cybersecurity and Infrastructure Agency, the Federal Bureau of Investigation ("FBI"), and the HHS issued a joint alert on a specific cybercrime group targeting organizations that held PHI.[6]

6. Despite being on notice that it was storing sensitive Private Information that is valuable and vulnerable to cyber attackers, Keenan failed to take basic security precautions that could have protected Plaintiffs' and class members' sensitive data.

7. On August 27, 2023, Keenan learned of "certain disruptions" that had occurred on its network servers.[7] After further investigation, Keenan determined that the attack had been initiated by an "unauthorized party" that was able to "gain[] access to" and "obtain[]" data from Keenan's internal computer systems.[8]

[6] Arghire, I. et al., *US Healthcare Organizations Warned of 'Daixin Team' Ransomware Attacks*, SECURITYWEEK (Oct. 24. 2022), https://www.securityweek.com/us-healthcare-organizations-warned-daixin-team-ransomware-attacks.

[7] *Notice of Data Security Incident*, STATE OF CALIFORNIA DEPARTMENT OF JUSTICE (Jan. 26, 2024), https://oag.ca.gov/system/files/EXPERIAN_K7150_KeenanAssociates_Notice%20Letter_Redacted.pdf.

[8] *Id.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

8. Around January 25, 2024, five months after the breach, Defendant mailed a "Notice of Data Breach" to affected individuals.[9] In its Notice, Defendant acknowledged that "an unauthorized party gained access . . . at various times between approximately August 21, 2023, and August 27, 2023, and that the unauthorized party obtained some data from Keenan systems."[10] Additionally, Defendant acknowledged that it was aware of the breach since around August 27, 2023.[11]

9. For six days, perpetrators were able to access Keenan's database, and obtained access to the types of information that federal and state law require companies take security measures to protect, including, but not limited to: names, Social Security numbers ("SSNs"), passport and driver's license numbers, as well as PHI in the form of health insurance information and general health information.

10. Plaintiffs and class members have been victimized by the Data Breach and remain at a continuing and imminent threat of harm, as any combination of this Private Information will forever subject them to being targets of fraud, identity theft, misuse, and other wrongdoings. Passport numbers, government/state IDs, and SSNs cannot easily be changed.

11. The Data Breach was a direct result of Keenan's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect Private Information. Specifically, Keenan disregarded the rights of Plaintiffs and class members by (a) failing to take adequate and reasonable measures to ensure the security of its databases and IT systems; (b) concealing or otherwise omitting the material fact that it did not have systems in place to safeguard Private Information; (c) failing to take available steps to detect and prevent the Data Breach; (d) failing to monitor its databases and IT systems, and to timely detect the Data Breach; and (e) failing to provide Plaintiffs and class members prompt and accurate notice of the Data Breach.

12. Due to Keenan's inadequate security practices, negligence, and other data security shortcomings, affected class members face a constant threat of repeated harm. Further, class members face threats of crimes such as fraudulent opening of new financial accounts in class members' names,

[9] *Notice of Security Incident*, KEENAN (Jan. 25, 2024), https://www.keenan.com/Notice-of-Security-Incident ("Notice").
[10] *Id.*
[11] *Id.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

taking out fraudulent loans, using class members' information to obtain government benefits, filing fraudulent tax returns, and filing false medical claims.

13. Plaintiffs and class members retain a significant interest in ensuring that their Private Information, which remains in Keenan's possession, is protected from further breaches, and seek to remedy the harms suffered as a result of the Data Breach.

14. Plaintiffs, individually, and on behalf of similarly situated persons, seek to recover damages, equitable relief, including injunctive relief designed to prevent a reoccurrence of the Data Breach and resulting injuries, restitution, disgorgement, reasonable costs and attorneys' fees, and all other remedies deemed proper.

PARTIES

Plaintiff Heather Heath

15. Plaintiff Heather Heath is, and at all relevant times was, a California resident. Believing Keenan would implement and maintain reasonable security and practices to protect customers' personal information, Plaintiff Heath provided Keenan with her Private Information including her name, SSN, driver's license and passport number, past and current residences, and her full medical history including, but not limited to, all prescriptions and procedures throughout Plaintiff's life, and personal health insurance policy information in connection with her insurance/worker's compensation plan.

16. Keenan retained Plaintiff Heath's Private Information at least until August 2023, when the Data Breach occurred, despite the fact that Heath was no longer covered by Keenan's policy at that point in time.

17. In January 2024, Plaintiff Heath received a letter from Keenan notifying her that she was affected by the Data Breach. Plaintiff Heath has spent several hours monitoring her accounts as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Heath otherwise would have spent on other activities, such as work and/or recreation. Plaintiff Heath plans to take additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her accounts for any unauthorized activity.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

18. Plaintiff Heath reasonably expected that Keenan would safeguard her Private Information. Plaintiff Heath would not have trusted Keenan with her Private Information if she knew that her information collected by Keenan would be at risk. Plaintiff Heath has suffered irreparable damage and has been placed at a heightened risk of fraud or identity theft as a result of the Data Breach.

Plaintiff Brian Heinz

19. Plaintiff Brian Heinz is an adult citizen of the state of California and resides in West Sacramento, California. Plaintiff Heinz is a customer of Keenan. Believing Keenan would implement and maintain reasonable security and practices to protect customers' personal information, Plaintiff Heinz agreed to have his Private Information provided to Keenan in connection with seeking insurance services from, and transacting with, Keenan.

20. In January of 2024, Plaintiff Heinz received a letter from Keenan notifying him that he was affected by the Data Breach. Had Plaintiff Heinz known that Keenan would not have adequately protected Private Information, he would not have consented to his Private Information being provided to Keenan. Plaintiff Heinz has spent several hours monitoring his accounts as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Heinz otherwise would have spent on other activities, such as work and/or recreation. Plaintiff Heinz plans to take additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his accounts for any unauthorized activity.

21. Plaintiff Heinz has suffered irreparable damage and has been placed at a heightened risk of fraud or identity theft as a result of the Data Breach.

Plaintiff Matthew Rutledge

22. Plaintiff Matthew Rutledge is an adult citizen of the state of California and resides in San Bernardino County, California. Plaintiff Rutledge is a customer of Keenan. Believing Keenan would implement and maintain reasonable security and practices to protect customers' personal information, Plaintiff Rutledge provided his Private Information to Keenan in connection with seeking insurance services from, and transacting with, Keenan.

23. In January of 2024, Plaintiff Rutledge received a letter from Keenan notifying him that he was affected by the Data Breach.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

24. Beginning right around the time the Data Breach occurred in August 2023, Plaintiff Rutledge began to receive notifications that someone had made login attempts and attempted to change his passwords for his existing accounts with credit reporting agencies, online survey websites, and his personal email account. He also received notifications from companies who pulled his credit report, despite that he never made any requests or engaged in transactions that would merit pulling his credit report.

25. Plaintiff Rutledge has spent several hours addressing the unauthorized activity and otherwise monitoring his accounts as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Rutledge otherwise would have spent on other activities, such as work and/or recreation. Plaintiff Rutledge plans to take additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his accounts for any unauthorized activity.

26. Had Plaintiff Rutledge known that Keenan does not adequately protect Private Information, he would not have used Keenan's services, agreed to provide Keenan with his Private Information, or otherwise would not have consented to his Private Information being provided to and received by Keenan. Plaintiff Rutledge has suffered irreparable damage and has been placed at a heightened risk of fraud or identity theft as a result of the Data Breach.

Plaintiff Robert Ruma

27. Plaintiff Robert Ruma is an adult citizen and resident of the state of California. Plaintiff Ruma is a customer of Keenan. Believing Keenan would implement and maintain reasonable security and practices to protect customers' personal information, Plaintiff Ruma provided his Private Information to Keenan in connection with seeking insurance services from, and transacting with, Keenan.

28. In January of 2024, Plaintiff Ruma received a letter from Keenan notifying him that he was affected by the Data Breach. Plaintiff Ruma monitors his credit and identity for fraudulent activity every day since the Data Breach, for at least a couple of hours a day. Had Plaintiff known that Keenan does not adequately protect Private Information, he would not have used Keenan's services, agreed to

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

provide Keenan with his Private Information, or otherwise would not have consented to his Private Information being provided to and received by Keenan.

Plaintiff Andrea Hans

29. Plaintiff Andrea Hans is an adult citizen and resident of Washington, DC. Plaintiff Hans is a customer of Keenan. Believing Keenan would implement and maintain reasonable security and practices to protect customers' personal information, Plaintiff Hans provided her Private Information to Keenan in connection with seeking insurance services from, and transacting with, Keenan.

30. In January of 2024, Plaintiff Hans received a letter from Keenan notifying her that she was affected by the Data Breach. Plaintiff Hans has spent several hours monitoring her credit and identity for fraudulent activity since the Data Breach. Had Plaintiff known that Keenan does not adequately protect Private Information, she would not have used Keenan's services, agreed to provide Keenan with her Private Information, or otherwise would not have consented to her Private Information being provided to and received by Keenan.

Defendant Keenan

31. Keenan & Associates is a California based insurance broker and a member of the Assured Partners family of companies. Keenan is responsible for the benefit coverage policies for millions of individuals, including the employee benefit policies for 80 percent of California's schools.[12] Defendant is registered in the state of California with its principal place of business located at 2355 Crenshaw Blvd., Suite 200 Torrance, California 90501.[13]

JURISDICTION AND VENUE

32. This Court has jurisdiction over this action under California Code of Civil Procedure § 410.10. This is an unlimited complex civil class action where the total damages incurred by Plaintiffs and the Class in the aggregate exceeds the $25,000 jurisdictional minimum of this Court.

33. This Court has jurisdiction over Defendant because it is located within Los Angeles County, California.

[12] *K-12 Schools, Community Colleges and Charter School Insurance Specialists*, KEENAN, https://www.keenan.com/Industries/Education (last visited May 21, 2024).

[13] *Keenan & Associates (671011)*, CALIFORNIA SECRETARY OF STATE (Nov. 1, 2023), https://bizfileonline.sos.ca.gov/search/business.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

34. Venue is proper in this Court under California Bus. & Prof. Code § 17203 and Code of Civil Procedure §§ 395(a) and 395.5 because Defendant is headquartered within this Court's jurisdiction and because a substantial part of the events giving rise to Plaintiffs' claims occurred in this County.

FACTUAL ALLEGATIONS

A. Data Breaches and the Market for Private Information

35. Data breaches in the United States have become ubiquitous, with the goal of criminals being to monetize the stolen data.[14]

36. When a victim's data is compromised in a breach, the victim is exposed to serious ramifications regardless of the sensitivity of the data—including but not limited to identity theft, fraud, decline in credit, inability to access healthcare, as well as legal consequences.[15]

37. The U.S. Department of Justice's Bureau of Justice Statistics has found that "among victims who had personal information used for fraudulent purposes, 29 percent spent a month or more resolving problems" and that resolution of those problems could take more than a year.[16]

38. The U.S. Government Accountability Office ("GAO") has concluded that it is common for data thieves to hold onto stolen data for extended periods of time before utilizing it for identity theft.[17] In the same report, the GAO noted that while credit monitoring services can assist with detecting fraud, those services do not stop it.[18]

[14] Ani Petrosyan, *Number of Data Records Exposed Worldwide From 1st Quarter 2020 to 3rd Quarter 2022*, STATISTA (Aug. 20, 2024), https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide.

[15] *2017 Annual Data Breach Year-End Review*, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter.org/wp-content/uploads/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf (last visited May 21, 2024).

[16] *Victims of Identity Theft, 2014*, U.S. DEPARTMENT OF JUSTICE, BUREAU OF JUSTICE STATISTICS (Nov. 13, 2017) https://bjs.ojp.gov/content/pub/pdf/vit14.pdf.

[17] *Data Breaches: Range of Consumer Risks Highlights Limitations of Identity Theft Services*, U.S. GOV'T ACCOUNTABILITY OFF., https://www.gao.gov/assets/700/697985.pdf (last visited Sept. 6, 2024).

[18] *Id*.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

39. When companies entrusted with consumer data fail to implement industry best practices, cyberattacks and other data exploitations can go undetected for a long period of time. This worsens the ramifications and can even render the harms irreparable.

40. PII is a valuable commodity for which a black market exists on the dark web, among other places. Personal data can be worth from $1,000-$1,200 on the dark web and the legitimate data brokerage industry is valued at more than $250 billion.[19]

41. Medical data is particularly valuable because unlike other personal information, such as credit card numbers which can be quickly changed, medical data is static. This is why companies possessing medical information, like Defendant, are targeted by cyber-criminals.[20]

42. A 2021 report by Invisibly, a team of application developers focused on reclaiming users' data, found that personal medical information is one of the most valuable pieces of information within the market for data. The report noted that "[i]t's worth acknowledging that because health care records often feature a more complete collection of the patient's identity, background, and [PII], health care records have proven to be of particular value for data thieves." While a single SSN might go for $0.53, a complete health care record sells for $250 on average.[21]

[19] Ryan Smith, *Revealed: How Much is Personal Data Worth on the Dark Web?*, INSURANCE BUSINESS MAGAZINE, https://www.insurancebusinessmag.com/ca/news/cyber/revealed--how-much-is-personal-data-worth-on-the-dark-web-444455.aspx (last visited Sept. 6, 2024); *see also* Maria LaMagna, *The Sad Truth About How Much Your Google Data is Worth on the Dark Web*, MARKETWATCH, https://www.marketwatch.com/story/spooked-by-the-facebook-privacy-violations-this-is-how-much-your-personal-data-is-worth-on-the-dark-web-2018-03-20 (last visited Sept. 6, 2024); Emily Wilson, *The Worrying Trend of Children's Data Being Sold on the Dark Web*, THE NEXT WEB (Feb. 23, 2019), https://thenextweb.com/news/children-data-sold-the-dark-web.

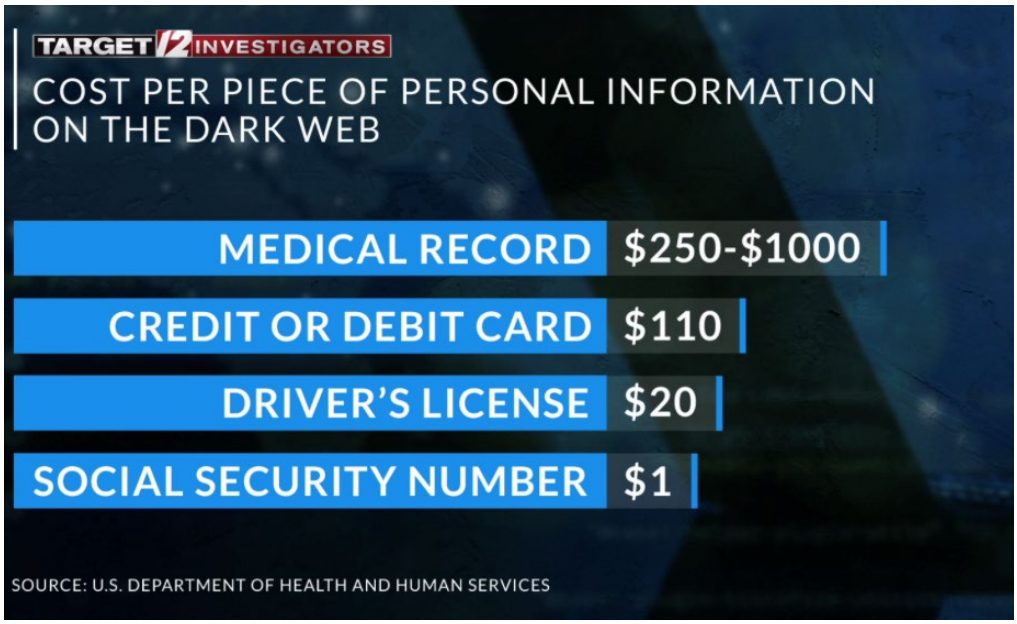
[20] Caroline Humer & Jim Finkle, *Your Medical Record is Worth More to Hackers Than Your Credit Card*, REUTERS (Sept. 24, 2014), https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924.

[21] *How Much is Your Data Worth? The Complete Breakdown for 2024*, INVISIBLY (Jul. 13, 2021), https://www.invisibly.com/learn-blog/how-much-is-data-worth/.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Record Type	Average Price
Health Care Record	$250.15
Payment Card Details	$5.40
Banking Records	$4.12
Access Credentials	$0.95
Social Security Number	$0.53
Credit Record	$0.31
Basic PII	$0.03

43. Medical records are even worth more than an SSN, credit card, and driver's license combined, according to federal officials. They estimate that medical records can go for anywhere between $250 to $1,000.[22]



44. In this black market, criminals seek to sell stolen data to identity thieves who desire the data to extort and harass victims, take over victims' identities in order to open financial accounts, and otherwise engage in illegal financial transactions under the victims' names.

[22] Kate Wilkinson, *RI Hospitals Fight Cyberattacks on 'Almost a Daily Basis'*, WPRI (Oct. 10, 2023), https://www.wpri.com/target-12/ri-hospitals-fight-cyberattacks-on-almost-a-daily-basis/.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

45. PII has a distinct, high value—which is why legitimate companies and criminals seek to obtain and sell it. As alleged in more detail below, a growing market is for children's data.[23]

46. Medical information in particular is extremely valuable to identity thieves, and thus, the medical industry has also experienced disproportionally higher numbers of data theft events than other industries. According to a report by the Health Insurance Portability and Accountability Act ("HIPAA") Journal, "healthcare data breach statistics clearly show there has been an upward trend in data breaches over the past nine (9) years, with 2018 seeing more data breaches reported than any other year since records first started being published."[24]

47. A study done by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that most victims of medical identity theft were forced to pay out of pocket costs for healthcare they did not receive to restore coverage.[25] Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.

B. <u>The Sensitivity of Customers' Private Information Demands Heightened Protection</u>

48. Entities in the healthcare industry are popular targets for cyberattacks and require top-tier security measures to protect Private Information, especially given that these databases store sensitive patient records.

49. Ponemon Institute, an expert in the annual state of cybersecurity, indicated in 2020 that organizations storing PHI were top targets for cyber-attacks. In fact, Defendant has been on notice for years that PHI is a prime target for scammers due to the amount and value of confidential patient information maintained. In 2019 alone, numerous entities in the healthcare sector suffered high-profile data breaches, including Quest Diagnostics and LabCorp. Defendant had resources for years to address its data security: Keenan commands approximately $701 million in annual revenue.[26]

[23] *The Worrying Trend of Children's Data Being Sold on the Dark Web*, THE Next WEB (Feb. 23, 2019), https://thenextweb.com/contributors/2019/02/23/children-data-sold-the-dark-web/.

[24] Steve Adler, *Healthcare Data Breach Statistics*, HIPAA JOURNAL (Aug. 23, 2024), https://www.hipaajournal.com/healthcare-data-breach-statistics/.

[25] See Elinor Mills, Study: *Medical Identity Theft is Costly for Victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/.

[26] *Keenan & Associates Experiences Data Breach Following Ransomware Attack*, JD SUPRA (Dec. 15, 2023), https://www.jdsupra.com/legalnews/keenan-associates-experiences-data-1137265/.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

50. In a survey released by Ponemon Institute in January 2023, nearly half of respondents (47 percent) said their organizations experienced a ransomware attack in the past two years, up from 43% in 2021. And 45 percent of respondents reported complications from medical procedures due to ransomware attacks, up from 36 percent in 2021.[27]

51. Countless victims impacted by the Data Breach now face a constant threat of being repeatedly harmed, including but not limited to living the rest of their lives knowing that criminals can compile, build, and amass profiles on them for decades – exposing them to a continuing threat of identity theft, disclosure of Private Information, threats, extortion, harassment and phishing scams, and the attendant anxiety from not knowing how one's information will be used when it comes into nefarious individuals' hands.

52. Data breaches of this caliber can result in the exposure of extremely sensitive information about children's private medical histories, medical conditions, psychological assessments, psychiatric evaluations, location of schools and residences, and much more, which poses great dangers on its own. The FBI has warned that "widespread collection of student data could have privacy and safety implications if compromised or exploited."[28] According to the FBI, malicious use of sensitive student data "could result in social engineering, bullying, tracking, identity theft, or other means for targeting children."[29] On top of privacy and safety implications, children must also live their entire lives knowing private, sensitive information about their medical histories or conviction records is subject to public exposure at any time.

53. Due to the special risks associated with individuals' data breaches and the increasing frequency with which they are occurring, it is imperative for entities like Defendant to routinely: (a) monitor for system breaches, cyberattacks and other exploitations; and (b) update their software, security procedures, and firewalls.

[27] Ron Southwick, *California Medical Group Discloses Ransomware Attack, More Than 3 Million Affected*, CHIEF HEALTHCARE EXECUTIVE (Feb. 10, 2023), https://www.chiefhealthcareexecutive.com/view/california-medical-group-discloses-ransomware-attack-more-than-3-million-affected.

[28] *Education Technologies: Data Collection and Unsecured Systems Could Pose Risks to Children*, FEDERAL BUREAU OF INVESTIGATION (Sept. 13, 2018), https://www.ic3.gov/media/2018/180913.aspx.

[29] *Id*.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

C. Defendant's Duty to Safeguard Private Information

54. Defendant is one of the largest insurance brokers in California, and therefore collects and processes the personal data for millions of individuals.

55. Defendant collects, receives, and accesses consumers' extensive individually identifiable information. These records include names, SSNs, passport and driver's license numbers, as well as PHI in the form of health insurance information and general health information.

56. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all decision-making.[30]

57. The FTC has issued numerous guides for entities engaged in commerce highlighting the importance of reasonable data security practices.

58. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[31] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

59. The FTC further recommends that entities not maintain Private Information longer than needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[32]

60. The FTC has brought enforcement actions against entities engaged in commerce 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

[30] *Start With Security: Lessons Learned from FTC Cases*, FEDERAL TRADE COMMISSION (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[31] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.
[32] *Start With Security: Lessons Learned from FTC Cases*, FEDERAL TRADE COMMISSION (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

61. Beyond legal applications, upon information and belief, Keenan included privacy policies and commitments to maintain the confidentiality of employees' sensitive information as terms of its contracts with its clients (the corporate entities). Keenan has failed to adhere to its promises and uphold its duty to safeguard individuals' Private Information. The schools, healthcare providers, public agencies, and other clients Defendant contracted with sought to provide their employees with coverage in the event of injury, and as such, these employees were the intended third-party beneficiaries of Keenan's contracts. Through contract terms and representations to employers and the public, Keenan promised to take specific measures to protect their members' information, consistent with best practices and federal and state law. However, Keenan failed.

62. Plaintiffs and class members provided their Private Information to Keenan with the reasonable expectation and mutual understanding that Keenan and any of their affiliates would comply with their obligations to keep such information confidential and secure from unauthorized access.

63. Data security is purportedly a critical component of Keenan's business model. On a section of its website entitled "Privacy Policy" Keenan makes the following statements[33]:

- Keenan & Associates (including our affiliates and subsidiaries) ("Keenan", "we", "us" or "our") respects your privacy and takes our privacy responsibility very seriously and is committed to protecting it in a manner consistent with applicable law and this statement.
- This Policy and notice applies to your Personal Information that we may collect, use, receive, and disclose and describes our practices for collecting, using, maintaining, protecting and disclosing that information in the course of providing our services.
- We have implemented measures reasonably designed to protect and secure your Personal Information from accidental loss, misuse, and from unauthorized access, use, alteration, and disclosure.

64. Keenan also maintains a "California Privacy Policy", which contains information concerning the requirements of California Consumer Privacy Act ("CCPA") as it relates to the storage

[33] *Privacy Policy*, KEENAN, https://www.keenan.com/Privacy-Policy (last visited Sept. 6, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

of the data of California residents.[34] A section of the California Privacy Policy, under the header "Why We Collect Personal Information and How We Use It," delineates the various circumstances under which Keenan may share Private Information for legitimate business purposes. It does not include providing that data to "unauthorized third parties"; to the contrary, the Policy states that "[w]e may disclose your personal information to a third party for a business or legal purpose" and "[w]e do not sell your personal information to third parties."[35]

65. Keenan's failure to provide adequate security measures to safeguard customers' Private Information is especially egregious because they operate in a field which has recently been a frequent target of scammers attempting to fraudulently gain access to customers' highly confidential Private Information.

66. Since the Data Breach, class members face a constant threat of continued harm. Now that their sensitive personal and medical information - their names, SSNs, passport and driver's license numbers, health insurance information and general health information – is in possession of third parties, class members must worry about being victimized throughout the rest of their lives. Furthermore, data breaches affecting minors' private information compromises children's whereabouts and routines, subjecting them to the danger of potential attacks, embarrassment, or even kidnapping.

67. Plaintiffs and other similarly situated individuals trusted Keenan with sensitive and valuable Private Information. Had Keenan disclosed to Plaintiffs and class members that its data systems were not secure and were vulnerable, Plaintiffs would not have trusted Keenan with such sensitive information. In fact, Keenan would have been forced to adopt reasonable data security measures and to comply with state and federal law.

68. Keenan knew or should have known that Plaintiffs and class members would reasonably rely upon, and trust Keenan's express and implied promises regarding the security and safety of its data and systems.

[34] *CCPA Disclosure*, KEENAN, https://www.keenan.com/CCPA (last visited Sept. 6, 2024).
[35] *Id.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

69. By collecting victims' sensitive Private Information and failing to protect it by maintaining inadequate security systems, failing to properly archive the Private Information, allowing access of third parties, and failing to implement security measures, Keenan caused harm to Plaintiffs and all affected individuals.

D. Keenan's Failure to Protect Against the Data Breach and its Impact on the Class

70. At all material times, Keenan failed to maintain proper security measures despite its promises of safety and security to consumers.

71. In August of 2023, Keenan faced a cyberattack which placed the private data of affected individuals in the hands of criminals for at least six days (August 21-27).

72. Keenan first detected unusual activity on August 27, 2023, when it experienced disruptions on its network servers. Keenan did not release a statement to affected individuals until January 25, 2024, five months after the Data Breach occurred and it became aware that individuals' data had been accessed and exfiltrated.[36]

73. Keenan knew that Private Information was valuable on the dark web and therefore knew that Keenan was a potential target for cybercrime. Despite Keenan's knowledge of the sensitivity of its stored data, Keenan failed to implement proper security measures to secure and protect the Private Information of their members. As a result of Keenan's negligent, and/or wanton disregard in, protection of consumers' Private Information, affected individuals now must live the rest of their lives knowing that criminals are able to compile, build, and amass their profiles for decades to come, exposing them to a never-ending threat of targeted extortion, identity theft, and harassment.

74. Plaintiffs and class members have suffered actual harm as a result of Keenan's conduct. Keenan failed to institute adequate security measures and neglected system vulnerabilities that led to the Data Breach. This breach allowed hackers to access Private Information for Plaintiffs and class members.

75. As explained above, exposure of this information to the wrong people can have profound consequences. The impact of identity theft can have ripple effects, which can adversely affect

[36] *Notice of Security Incident*, KEENAN (Jan. 25, 2024), https://www.keenan.com/Notice-of-Security-Incident.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that identity theft can impact an individual's ability to get credit cards and obtain loans, such as student loans or mortgages.[37] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

76. The U.S. GAO found that, "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[38]

77. There may also be a significant time lag between when personal information is stolen and when it is actually misused. According to the GAO, which conducted a study regarding data breaches:

> *"[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."*[39]

78. As a direct and proximate result of Keenan's breach of confidence and failure to protect the Private Information of individuals, Plaintiffs and class members have been injured by facing ongoing, imminent, impending threats of identity theft crimes, fraud, scams, and other misuse of this Private Information, resulting in ongoing monetary loss and economic harm, loss of value of privacy and confidentiality of the stolen Private Information, illegal sales of the compromised Private Information on the black market, mitigation expenses and time spent on credit monitoring, identity theft insurance, credit freezes/unfreezes, expenses and time spent in initiating fraud alerts, contacting third parties, decreased credit scores, lost work time, and other injuries. Keenan, through its

[37] *Identity Theft: The Aftermath 2017*, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf (last visited Sept. 6, 2024).

[38] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOV'T ACCOUNTABILITY OFF. (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[39] *Id.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

misconduct, has enabled numerous bad actors to sell and profit from Private Information that belongs to Plaintiffs and class members.

79. But for Keenan's unlawful conduct, scammers would not have access to Plaintiffs' and class members' Private Information. Keenan's unlawful conduct has directly and proximately resulted in a widespread threat of digital attacks against Plaintiffs and class members.

80. This Data Breach creates a heightened security concern for the affected individuals, including Plaintiffs, because their Private Information and health-related information, including unique medical records and other sensitive health information is disclosed. Medical privacy is among the most important tenets of American healthcare. Patients/customers must be able to trust their physicians, insurers, and pharmacies to protect their medical information from improper disclosure including, but not limited to, their health conditions and courses of treatment. Indeed, numerous state and federal laws require this. And these laws are especially important when protecting individuals with highly sensitive or private medical conditions disclosure of which can and do subject them to regular discrimination or ridicule.

81. Plaintiffs and class members face ongoing, imminent threats of similar fraud claims and scams, resulting in ongoing monetary loss and economic harm; mitigation expenses and time spent on credit monitoring, credit freezes/unfreezes; expenses and time spent in initiating fraud alerts; contacting third parties; decreased credit scores; lost work time; and other injuries.

82. As a result of the Data Breach, Plaintiffs and class members also suffered unauthorized email solicitations and experienced a significant increase in suspicious phishing scam activity via email, phone calls, text messages, all following the breach. In addition, Plaintiffs and class members have spent significant time and effort researching the breach, monitoring their accounts for fraudulent activity, reviewing unsolicited emails and texts, and answering telephone calls.

83. Breach victims have spent significant time monitoring personal accounts (banking, credit monitoring, financial applications, and even other applications/accounts that may be attacked) for fraudulent activity. Many breach victims have had to change their passwords and associated accounts which may be connected to various pieces of stolen Private Information. Plaintiffs have been monitoring their credit activity, living in constant fear and apprehension of further attacks.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

84. Plaintiffs and other class members also have spent significant time researching and comparing various identity protection services, such as Equifax and Experian. Plaintiffs have been placed on hold or have been speaking to representatives for hours each day in anticipation of taking their data protection into their own hands, a measure which should be unnecessary. Had Plaintiffs and class members been able to trust that Keenan would vigilantly protect their data, they would not have to take drastic action, and invest significant time and energy, to protect their Private Information themselves.

85. Phishing and other targeted attacks result from data breaches that disclose Private Information. Phishing scammers use emails and text messages to trick people into giving them their personal information, including but not limited to passwords, account numbers, and social security numbers. Phishing scams are frequently successful, and the FBI reported that Americans lost approximately $57 million to such scams in 2019 alone.[40]

86. As a result of the Data Breach, Plaintiffs and class members have received a high-volume of phishing emails and spam telephone calls. Such scams trick consumers into giving account information, passwords, and other valuable personal information to scammers. This significantly increases the risk of further substantial damage to Plaintiffs and class members, including, but not limited to, monetary and identity theft. On average, Plaintiffs have received dozens of phishing emails since the Data Breach and have noticed a substantial increase in spam telephone calls. Many of the phishing emails received by Plaintiffs and class members are disguised as originating from reputable companies but are traps to further steal their Private Information. Due to the Breach, Plaintiffs and class members now need to spend a substantial amount of time and effort discerning genuine emails from emails trying to phish their Private Information.

87. Plaintiffs and other class members are suffering ongoing fraud and phishing attacks from various individuals who were able to get ahold of Plaintiffs' personal data because of this Data Breach. Plaintiffs are receiving ongoing attacks by persons posing as various companies or providers,

[40] *How to Recognize and Avoid Phishing Scams*, FEDERAL TRADE COMMISSION (Sept. 2022), https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

attempting to seek further personal identifying information, attempting to reset their passwords, and gain access to other accounts.

88. The data leak also caused an increased number of fraudulent calls and text messages to Plaintiffs and the class members. Plaintiffs have already received numerous digital attacks because of the Data Breach.

89. Plaintiffs are suffering ongoing phishing attacks from *various individuals* who were able to get ahold of their data. Therefore, this data appears to be shared with other fraudsters across the dark web, as Plaintiffs' ongoing attacks are increasing.

90. Given the highly sensitive nature of the information stolen, and its dissemination to unauthorized parties, Plaintiffs have already suffered injury and remain at a substantial and imminent risk of future harm.

91. Plaintiffs and class members are now forced to research and subsequently acquire credit monitoring and reasonable identity theft defensive services and maintain these services to avoid further impact. Plaintiffs anticipate substantial out-of-pocket expenses to pay for these services.

92. In sum, Plaintiffs and similarly situated consumers have been injured as follows due to the Data Breach:

a. Theft of their Private Information and the resulting loss of privacy rights in that information;

b. Improper disclosure of their Private Information;

c. Loss of value of their Private Information;

d. The amount of ongoing reasonable identity defense and credit monitoring services made necessary as mitigation measures;

e. Keenan's retention of profits attributable to Plaintiffs' and other class members' Private Information that Keenan failed to adequately protect;

f. Economic and non-economic impacts that flow from imminent, and ongoing threat of fraud and identity theft to which Plaintiffs and class members are now exposed to;

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

g. Ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of this Data Breach;

h. Emotional distress, and fear associated with the imminent threat of harm from the continued phishing scams and attacks as a result of this Data Breach.

CLASS ALLEGATIONS

93. Plaintiffs bring this action on their own behalf and on behalf of a nationwide class defined as follows:

Nationwide Class

> All residents of the United States who were notified by Keenan that their PII was or may have been affected in the Data Security Incident. Excluded from the Settlement Class are: (1) the Judges presiding over the Action, Class Counsel, and members of their families; (2) Keenan and its subsidiaries, parent companies, successors, predecessors, and any entity in which Keenan or its parents, have a controlling interest, and its current or former officers and directors; (3) Persons who properly execute and submit a Request for Exclusion prior to the expiration of the Opt-Out Period; and (4) the successors or assigns of any such excluded Persons.

The class may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

94. Numerosity: the class is so numerous that joinder of all members is impracticable and the disposition of their claims in a class action will benefit the parties and the Court. Per Keenan's disclosures, there are approximately 1,780,595 class members. A significant majority of class members are California residents.

95. Commonality and Predominance: there is a well-defined community of interest in the questions of law and fact involved affecting the parties to be represented in that the class was exposed to the same common and uniform breach of Keenan's duty and reliance on Keenan's ability to protect class members' data. The questions of law and fact common to the class predominate over questions which may affect individual Plaintiffs and class members. Common questions of law and fact include, but are not limited to, the following:

a. Whether Keenan's conduct is an unlawful business act or practice within the meaning of Business and Professions Code §§ 17200, *et seq*.;

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

b. Whether Keenan's conduct is an unfair business act or practice within the meaning of Business and Professions Code §§ 17200, *et seq*.;

c. Whether Keenan's conduct is in violation of California Civil Code §§ 1798, *et seq.*;

d. Whether Keenan's conduct is in violation of California Civil Code §§ 56, *et seq.*;

e. Whether Keenan's failure to implement effective security measures to protect Plaintiffs' and class members' Private Information was negligent;

f. Whether Keenan represented to Plaintiffs and the class that it would protect Plaintiffs' and class members' Private Information;

g. Whether Keenan owed a duty to Plaintiffs and the class to exercise due care in collecting, storing, and safeguarding their Private Information;

h. Whether Keenan breached a duty to Plaintiffs and the class to exercise due care in collecting, storing, and safeguarding their Private Information;

i. Whether class members' Private Information was accessed, compromised, or stolen in the breach;

j. Whether Keenan's conduct caused or resulted in damages to Plaintiffs and class members;

k. Whether Keenan failed to notify the public of the breach in a timely and adequate manner;

l. Whether Keenan knew or should have known that its systems were vulnerable to a data breach;

m. Whether Keenan adequately addressed the vulnerabilities that allowed for the Data Breach; and

n. Whether, as a result of Keenan's conduct, Plaintiffs and the class are entitled to injunctive relief.

96. Typicality: Plaintiffs' claims are typical of the claims of the proposed class, as Plaintiffs and class members were harmed by Keenan's uniform unlawful conduct.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

97. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests of the proposed class. Plaintiffs have retained competent and experienced counsel in class action and other complex litigation.

98. Superiority: a class action is superior to other available methods for fair and efficient adjudication of this controversy. The expense and burden of individual litigation would make it impracticable or impossible for proposed class members to prosecute their claims individually.

99. The litigation and resolution of class members' claims are manageable. Individual litigation of the legal and factual issues raised by Keenan's conduct would increase delay and expense to all parties and the court system. The class action device presents far fewer management difficulties and provides the benefits of a single, uniform adjudication, economies of scale, and comprehensive supervision by a single court.

100. Plaintiffs and class members have suffered injury in fact as a result of Keenan's false, deceptive, and misleading representations. Plaintiffs would not have sought services from, provided Private Information to, or otherwise have their Private Information provided to Keenan but for the reasonable belief that Keenan would safeguard their Private Information.

101. The class is identifiable and readily ascertainable. Notice can be provided to such affected individuals using techniques and a form of notice similar to those customarily used in class actions, and by internet publication, radio, newspapers, and magazines. Further, Keenan already has identified and sent a letter to each affected class member.

102. Keenan has acted on grounds generally applicable to the entire class, thereby making final and/or corresponding declaratory relief appropriate with respect to the class as a whole. The prosecution of separate actions by individual class members would create the risk of inconsistent or varying adjudications with respect to individual class members that would establish incompatible standards of conduct for Keenan.

103. Absent a class action, Keenan will likely retain the benefits of its wrongdoing. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Keenan's conduct. It would be virtually impossible for class members individually to redress effectively the

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

wrongs done to them by Keenan. Even if class members could afford such individual litigation, the court system could not. Absent a representative action, the class members will continue to suffer losses and Keenan (and similarly situated companies) will be allowed to continue these violations of law and to retain the proceeds of its ill-gotten gains.

CAUSES OF ACTION

COUNT ONE

NEGLIGENCE

104. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

105. Keenan owed a duty to Plaintiffs and the class to exercise due care in collecting, storing, and safeguarding their Private Information. This duty included but was not limited to: (a) designing, implementing, and testing security systems to ensure that individuals' Private Information was consistently and effectively protected; (b) implementing security systems that are compliant with state and federal mandates; (c) implementing security systems that are compliant with industry practices; and (d) promptly detecting and notifying affected parties of a data breach.

106. Keenan also had a duty to destroy Plaintiffs' and class members' Private Information within an appropriate amount of time after it was no longer required by Keenan, in order to mitigate the risk of the stale Private Information being compromised in a data breach.

107. Keenan's duties to use reasonable care arose from several sources, including those described below. Keenan had a common law duty to prevent foreseeable harm to others, including Plaintiffs and members of the class, who were the foreseeable and probable victims of any inadequate security practices.

108. Keenan had a special relationship with Plaintiffs and class members, which is recognized by laws and regulations, as well as common law. Keenan was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to class members from a data breach. Plaintiffs and class members were compelled to entrust Keenan with their Private Information. At relevant times, Plaintiffs and class members understood that Keenan would take adequate security

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

precautions to safeguard that information. Only Keenan had the ability to protect Plaintiffs' and class members' Private Information stored on Keenan's servers.

109. Keenan knew or should have known that Plaintiffs' and the class members' Private Information is information that is frequently sought after by hackers.

110. Keenan knew or should have known that Plaintiffs and the class members would suffer harm if their Private Information was leaked.

111. Keenan knew or should have known that its security systems were not adequate to protect Plaintiffs' and the class members' Private Information from a data breach, especially in light of the increase in data breaches in the insurance and financial institutions sectors.

112. Keenan knew or should have known that adequate and prompt notice of the Data Breach was required such that Plaintiffs and the class could have taken more swift and effective action to change or otherwise protect their Private Information, rather than waiting six days to become aware of the breach and notifying affected individuals five months later. Keenan failed to provide timely notice upon discovery of the Data Breach.

113. Keenan's conduct as described above constituted an unlawful breach of its duty to exercise due care in collecting, storing, and safeguarding Plaintiffs' and the class members' Private Information by failing to design, implement, and maintain adequate security measures to protect this information. Moreover, Keenan did not implement, design, or maintain adequate measures to detect a data breach when it occurred or adopt sufficient measures to notify affected parties in the event of a data breach.

114. Keenan's conduct as described above constituted an unlawful breach of its duty to provide adequate and prompt notice of the Data Breach.

115. Keenan entered a special relationship when Plaintiffs and class members entrusted Keenan to protect their Private Information. Plaintiffs and the class trusted Keenan and, in doing so, provided Keenan with their Private Information, based upon Keenan's representations that it would implement adequate systems to secure their information to the affected parties' employers and to the affected parties themselves.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

116. Keenan breached its duty in this relationship to implement and maintain reasonable measures to protect Plaintiffs' and class members' Private Information.

117. Plaintiffs' and class members' PII would have remained private and secure had it not been for Keenan's wrongful and negligent breach of their duties. The leak of Plaintiffs' and class members' Private Information, and all subsequent damages, was a direct and proximate result of Keenan's negligence.

118. Keenan's negligence was, at least, a substantial factor in causing Plaintiffs' and class members' Private Information to be improperly accessed, disclosed, and otherwise compromised, and in causing the class members' other injuries because of the Data Breach.

119. The damages suffered by Plaintiffs and class members was the direct and reasonably foreseeable result of Keenan's negligent breach of its duties to adequately design, implement, and maintain security systems to protect Plaintiffs' and class members' Private Information. Keenan knew or should have known that its security for safeguarding Plaintiffs' and class members' Private Information was vulnerable to a data breach.

120. Keenan's negligence directly caused significant harm to Plaintiffs and the class. Specifically, Plaintiffs and the class are now subject to numerous attacks, including various phishing scams and identity theft.

121. Keenan had a fiduciary duty to protect the confidentiality of their communications with Plaintiffs and class members by virtue of the explicit privacy representations Keenan made in dealing with intended beneficiaries' employers through terms of contract and to Plaintiffs and class members when they sought any additional Private Information to effectuate claims.

122. Keenan had information relating to Plaintiffs and class members that it knew or should have known to be confidential.

123. Plaintiffs' and class members' communications with Keenan about sensitive Private Information and their status as patients/customers were not matters of general knowledge.

124. Keenan breached its fiduciary duty of confidentiality by designing its data protection systems in a way to allow for a data breach of massive caliber.

125. At no time did Plaintiffs or class members give consent to Keenan's conduct.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

126. As a direct and proximate cause of Keenan's actions, Plaintiffs and the class suffered damage in that the information they intended to remain private is no longer so and their Private Information was disclosed without their knowledge or consent.

COUNT TWO

NEGLIGENCE PER SE

127. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

128. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted, and enforced by the FTC, the unfair act or practice by entities such as Keenan or failing to use reasonable measures to protect Private Information. Various FTC publications and orders also form the basis of Keenan's duty.

129. Keenan violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Private Information and not complying with the industry standards. Keenan's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of a data breach that disclosed Plaintiffs, class members', and beneficiaries' Private Information to unauthorized third parties.

130. Keenan's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se. This negligence was, at least, a substantial factor in causing class members' Private Information to be improperly accessed, disclosed, and otherwise compromised, and in causing class members' other injuries as a result of the Data Breach.

131. Plaintiffs and class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect as they are natural persons. In addition, the harm that class members have suffered is the type of harm that the FTC Act (and similar state statutes) were intended to prevent. Indeed, the FTC has pursued over fifty enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same or similar harm suffered by class members.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

132. Keenan also violated other laws in allowing and as a result of the Data Breach, including HIPAA, the California Unfair Competition Law, the California Consumer Privacy Act, the California Customer Records Act, and the California Confidentiality of Medical Information Act.

133. As a direct and proximate result of Defendant's violation of law and its negligence, Plaintiffs and class members have been injured, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT THREE

BREACH OF IMPLIED CONTRACT

141. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

142. Keenan provided or provides insurance-related risk management and claims services to Plaintiffs and class members, or Plaintiffs and class members otherwise provided their Private Information to Keenan as prospective customers or in some other capacity.

143. In connection with their business relationship, Plaintiffs and class members entered implied contracts with Keenan.

144. Pursuant to these implied contracts, Plaintiffs and class members provided Keenan with their Private Information. In exchange, Keenan agreed, among other things: (1) to take reasonable measures to protect the security and confidentiality of Private Information; and (2) to protect Private Information in compliance with federal and state laws and regulations and industry standards.

145. The protection of Private Information was a material term of the implied contracts between Plaintiffs and class members, on the one hand, and Keenan, on the other hand. Had Plaintiffs and class members known that Keenan would not adequately protect Private Information they would not have done business with Keenan.

146. Plaintiffs and class members performed their obligations under the implied contract when they provided Keenan with their Private Information.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

147. Keenan breached its obligations under its implied contracts with Plaintiffs and class members by failing to implement and maintain reasonable security measures to protect their Private Information.

148. The damages sustained by Plaintiffs and class members as described above were the direct and proximate result of Keenan's material breaches of its agreements.

149. Plaintiffs and class members were damaged by Keenan's breach of implied contracts because: (i) they have suffered actual harm or identity theft; (ii) they face a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their Private Information was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their Private Information has been breached; (v) they were deprived of the value of their Private Information, for which there is a well-established national and international market; (vi) they were deprived of the benefit of their bargain; and/or (vii) they lost time and money incurred to mitigate and remediate the effects of the breach, including the increased risks of identity theft they face and will continue to face.

COUNT FOUR

BREACH OF FIDUCIARY DUTY

150. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

151. A relationship existed between Plaintiffs and class members, on the one hand, and Defendant on the other hand, in which Plaintiffs and class members put their trust in Defendant to protect the Private Information of Plaintiffs and class members and Defendant accepted that trust.

152. Defendant breached the fiduciary duties that it owed to Plaintiffs and class members by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect the Private Information of Plaintiffs and class members.

153. Defendant's breach of fiduciary duty was a legal cause of damage to Plaintiffs and class members.

154. But for Defendant's breach of fiduciary duty, the damage to Plaintiffs and class members would not have occurred.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

155. Defendant's breach of fiduciary duty contributed substantially to producing the damage to Plaintiffs and class members.

156. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiffs are entitled to and demand actual, consequential, and nominal damages, and injunctive relief.

COUNT FIVE

BREACH OF CONFIDENCE

157. Plaintiffs herein repeat, reallege, and fully incorporate all allegations in all preceding paragraphs.

158. At all times during Plaintiffs' and class members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and class members' Private Information it held.

159. Defendant's relationships with Plaintiffs and class members were governed by terms and expectations that Plaintiffs' and class members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

160. Plaintiffs and class members provided their Private Information to Defendant with the explicit and implicit understanding that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized third parties.

161. Plaintiffs and class members provided their Private Information to Defendant with the explicit and implicit understanding that Defendant would take reasonable and industry standard precautions to protect their Private Information from unauthorized disclosure.

162. Defendant voluntarily received in confidence Plaintiffs' and class members' Private Information with the understanding that Private Information would not be disclosed or disseminated to unauthorized third parties or to the public.

163. Due to Defendant's failure to prevent or avoid the Data Breach, Plaintiffs' and class members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and class members' confidence, and without their express permission.

164. As a proximate result of such unauthorized disclosures, Plaintiffs and class members suffered damages.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

165. But for Defendant's disclosure of Plaintiffs' and class members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, access, and used by unauthorized third parties.

166. The injury and harm suffered by Plaintiffs and class members was the reasonably foreseeable result of Defendant's inadequate security of Plaintiffs' and class members' Private Information. Defendant knew or should have known that its methods of accepting, storing, transmitting, and using Plaintiffs' and class members' Private Information were inadequate.

167. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and class members have suffered injury, including but not limited to: (i) threat of identity theft; (ii) the loss of the opportunity in how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) the continued risk to their Private Information, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect it; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the rest of Plaintiffs' and the class members' lives.

168. As a direct proximate result of such unauthorized disclosures, Plaintiffs and class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT SIX

VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW ("UCL")

BUSINESS & PROFESSIONS CODE §§ 17200, *et seq.*

169. Plaintiffs herein repeat, reallege, and fully incorporate all allegations in all preceding paragraphs.

170. This claim is pleaded on behalf of Plaintiffs and Class Members in the State of California.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

A. "Unfair" Prong

171. Under California's Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.*, a challenged activity is "unfair" when "any injury it causes outweighs any benefits provide to consumers and the injury is one that the consumers themselves could not reasonably avoid.

172. Defendant's conduct as alleged herein does not confer any benefit to the intended third-party beneficiaries of its contracts. It is especially questionable why Defendant would continue to store individual's data when those individuals are no longer employed by the institution with which Defendant originally contracted. Plaintiffs' Private Information was held by Defendant, leaving it available to cybercriminals who breached Defendant's paltry defenses, until at least August 21, 2023, even though some Plaintiffs were no longer in the contracting party's employ as of January 2023. Mishandling this data and a failure to archive and purge this unnecessary data shows blatant disregard for beneficiaries' privacy and security.

173. Defendant did not need to collect the full gamut of Private Information from the affected parties to effectuate coverage for a specific injury which occurred at work. It did so to track and target beneficiaries so that Defendant could arm itself with any ammunition obtainable in its fight to deny claims.

174. Defendant could have furthered its legitimate business interests by focusing on matters related to the circumstances of a specific injury or other benefits requested, rather than extracting and storing individuals' entire medical histories, their SSNs, past residences, government-issued identification information, their children's medical history and identifying information, and much more. Defendant unreasonably gathered affected individuals' entire lives' worth of data to effectuate employee benefit coverage for specific purposes.

175. Defendant's conduct as alleged herein causes injuries to intended beneficiaries, who entrusted Defendant with their Private Information and whose Private Information was leaked as a result of Defendant's unlawful conduct.

176. Defendant's failure to implement and maintain reasonable security measures was also contrary to legislatively declared public policy that seeks to protect beneficiaries' data and ensure entities that are trusted with it use appropriate security measures. These policies are reflected in laws,

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

including the FTC Act, 15 U.S.C. § 45, California's Consumer Records Act, Cal. Civ. Code §1798.81.5, California's Confidentiality of Medical Information Act, Cal. Civ. Code § 56, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100.

177. Beneficiaries cannot avoid any of the injuries caused by Defendant's conduct as alleged herein.

178. The injuries caused by Defendant's conduct as alleged herein outweigh any benefits.

179. Defendant's conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes an unfair business practice within the meaning of California Business and Professions Code Section 17200.

180. Defendant's conduct also threatens other companies, large and small, who play by the rules. Defendant's conduct stifles competition and has a negative impact on the marketplace.

181. All the conduct alleged herein occurs and continues to occur in Defendant's business. Defendant's wrongful conduct is part of a pattern or generalized course of conduct repeated on approximately thousands of occasions daily.

182. Pursuant to Business and Professions Code Sections 17203, Plaintiffs seek an order of this Court enjoining Defendant from continuing to engage, use, or employ its unfair business practices.

183. Plaintiffs and class members have suffered injury-in-fact and have lost money or property as a result of Defendant's unfair conduct. Plaintiffs relied on Defendant's representations and implied promises regarding their security measures and trusted that Defendant would keep their Private Information safe and secure. Plaintiffs accordingly provided their Private Information to Defendant, in exchange for coverage pursuant to either their respective employer's policy or Defendant's customer policy, reasonably believing and expecting that their Private Information would be safe and secure. Plaintiffs and the class members would not have invoked Defendant's coverage or would not have given Defendant their Private Information, had they known that their Private Information was vulnerable to a data breach. Likewise, Plaintiffs and class members seek an order mandating that Defendant implement adequate security practices to protect beneficiaries' Private Information.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

184. Plaintiffs and class members seek and request an order awarding Plaintiffs and the class restitution of the money wrongfully acquired by Defendant by means of Defendant's unfair and unlawful practices. Plaintiffs and members of the class are employed in a variety of industries with different practices regarding the payment of premiums on their employers' contracts with Defendant. In the event of, and in anticipation of discovery, Plaintiffs and class members seek this order with respect to any withheld wages or buy-in programs that Defendant and their employers put in place.

B. "Unlawful" Prong

185. California Business and Professions Code Section 17200, *et seq.*, identifies violations of any state or federal law as "unlawful practices that the unfair competition law makes independently actionable." (*Velazquez v. GMAC Mortg. Corp.* (C.D. Cal. 2008) 605 F. Supp. 2d 1049, 1068.)

186. Defendant's unlawful conduct, as alleged in the preceding paragraphs, violates California Civil Code Section 1750, *et seq.*

187. Defendant's conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes unlawful conduct.

188. Defendant has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), the FTC Act, 15 U.S.C. § 45, California's Confidentiality of Medical Information Act, Cal. Civ. Code § 56, California's Consumer Privacy Act, Cal. Civ. Code § 1798.100, and California common law. Defendant failed to notify all its affected customers regarding said Breach in a timely manner, failed to take reasonable security measures, or comply with the FTC Act, and California common law.

189. Furthermore, Defendant failed to post the proper notice with the California Attorney General, and to date, it has not adequately notified the affected customers of the full extent of the Data Breach, seeking to disguise the substantial and impeding threat of identity theft that it caused and continues to cause to consumers.

190. Defendant knew or should have known of its unlawful conduct.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

191. As alleged in the preceding paragraphs, the misrepresentations by Defendant detailed above constitute an unlawful business practice within the meaning of California Business and Professions Code section 17200.

192. Defendant could have furthered its legitimate business interests in ways other than by its unlawful conduct.

193. All the conduct alleged herein occurs and continues to occur in Defendant's business. Defendant's unlawful conduct is part of a pattern or generalized course of conduct repeated on approximately thousands of occasions daily.

194. Pursuant to Business and Professions Code Sections 17203, Plaintiffs seek an order of this Court enjoining Defendant from continuing to engage, use, or employ its unlawful business practices.

195. Plaintiffs and class members have suffered injury-in-fact and have lost money or property as a result of Defendant's fraudulent conduct. Plaintiffs relied on Defendant's representations and implied promises regarding their security measures and trusted that Defendant would keep their Private Information safe and secure. Plaintiffs accordingly provided their Private Information to Defendant, in exchange for coverage pursuant to either their employer's policy or Defendant's customer policy, reasonably believing and expecting that their Private Information would be safe and secure. Plaintiffs and the class members would not have invoked Defendant's coverage or would not have given Defendant their Private Information, had they known that their Private Information was vulnerable to a data breach.

196. Plaintiffs and the members of the class seek an order mandating that Defendant implement adequate security practices to protect consumers' Private Information. Additionally, Plaintiffs and the members of the class seek and request an order awarding Plaintiffs and the class restitution of the money wrongfully acquired by Defendant by means of Defendant's unfair and unlawful practices.

///

///

///

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

COUNT SEVEN

VIOLATION OF CALIFORNIA CONSUMER PRIVACY ACT ("CCPA")

CAL. CIV. CODE SECTION 1798.150, *et seq*.

197. Plaintiffs herein repeat, reallege, and fully incorporate all allegations in all preceding paragraphs.

198. This claim is pleaded on behalf of Plaintiffs and Class Members in the State of California.

199. The CCPA, Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically provides: any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following: (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater; (B) Injunctive or declaratory relief; (C) Any other relief the court deems proper.

200. Defendant is a "business" under § 1798.140(d) in that it is a corporation organized for profit or financial benefit of their shareholders or other owners, with indeterminate gross revenue. The only publicly available revenue information relates to Defendant's parent company, the Assured Partners family of companies, which in aggregate generates greater than $1 billion annually.

201. Plaintiffs and class members are covered "consumers" under § 1798.140(i) in that they are natural persons, whose records were maintained in California, by a California based entity, and on California-based servers.

202. The personal information of Plaintiffs and class members at issue in this lawsuit constitutes "personal information" under § 1798.150(a) and 1798.81.5.

203. Defendant knew or should have known that its data security systems and practices were inadequate to safeguard the Plaintiffs' and class members' Private Information and that the risk of a

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the Private Information of Plaintiffs and class members. Specifically, Defendant subjected Plaintiffs' and class members' Private Information to an unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

204. As a direct and proximate result of Defendant's conduct, Plaintiffs and class members were injured and lost money or property, including but not limited to the loss of Plaintiffs' and the class member's legally protected interest in the confidentiality and privacy of their Private Information, and additional losses described herein. In accordance with Cal. Civ. Code § 1798.150(b), Plaintiffs provided Defendant with written notices of its alleged violations of Cal. Civ. Code § 1798.150(a).

205. As Defendant did not timely respond to Plaintiffs' CCPA notices, Defendant failed to "actually cure" the violations. Thus, Plaintiffs and the class seek statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident, or actual damages, whichever is greater. (*See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).) In addition to actual or statutory damages, Plaintiffs seek injunctive relief, including public injunctive relief, declaratory relief, and any other relief as deemed appropriate by the Court.

COUNT EIGHT

VIOLATION OF CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT ("CMIA") CAL. CIV. CODE §§ 56, *et seq*.

206. Plaintiffs herein repeat, reallege, and fully incorporate all allegations in all preceding paragraphs.

207. This claim is pleaded on behalf of Plaintiffs and Class Members in the State of California.

208. Defendant is subject to the requirements and mandates of the CMIA.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

209. CMIA section 56.36 allows an individual to bring an action against a "person or entity who has negligently released confidential information or records concerning him or her in violation of this part."

210. As a direct result of its negligent failure to adequately protect the data it collected from the Plaintiffs and class members, Defendant allowed for a data breach which released the Private Information of the Plaintiffs and the class to criminals and/or third parties.

211. The CMIA defines "medical information" as "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care ... regarding a patient's medical history, mental or physical condition, or treatment."

212. The CMIA defines individually identifiable information as "medical information [that] includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the [customers]' name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity." (Cal. Civ. Code § 56.050.)

213. Defendant is in possession of affected individuals' entire medical history and insurance information, including, but not necessarily limited to, diagnosis and treatment of patients/customers, laboratory test results, prescription data, radiology reports, health plan member number. Further, the compromised data was individually identifiable because it was accompanied by elements sufficient to allow identification of the Plaintiffs by the third parties to whom the data was disclosed.

214. Defendant lawfully came into possession of the Plaintiffs' and class members' medical information and had a duty pursuant to Section 56.06 and 56.101 of the CMIA to maintain, store and dispose of the Plaintiffs' and class members' medical records in a manner that preserved their confidentiality. Sections 56.06 and 56.101 of the CMIA prohibit the negligent creation, maintenance, preservation, store, abandonment, destruction, or disposal of confidential medical information.

215. Defendant further violated the CMIA by failing to use reasonable care, and in fact, negligently maintained Plaintiffs' and class members' medical information.

216. As a direct and proximate result of Defendant's violations of the CMIA, Plaintiffs and class members have been injured and are entitled to compensatory damages, punitive damages, and

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

nominal damages of one-thousand dollars ($1,000) for each of Defendant's violations of the CMIA, as well as attorneys' fees and costs pursuant to Cal. Civ. Code § 56.36.

COUNT NINE

VIOLATIONS OF THE CALIFORNIA CUSTOMER RECORDS ACT ("CCRA")

CAL. CIV. CODE §§ 1798.80, *et seq.*

217. Plaintiffs herein repeat, reallege, and fully incorporate all allegations in all preceding paragraphs.

218. This claim is pleaded on behalf of Plaintiffs and Class Members in the State of California.

219. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Civil Code § 1798.81.5, which requires that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

220. By failing to implement reasonable measures to protect Plaintiffs' Private Information, Defendant violated Civil Code § 1798.81.5.

221. In addition, by failing to promptly notify all affected class members that their Personal Information had been exposed, Defendant violated Civil Code § 1798.82.

222. As a direct or proximate result of Defendant's violations of Civil Code §§ 1798.81.5 and 1798.82, Plaintiffs and California-based class members were (and continue to be) injured and have suffered (and will continue to suffer) the damages and harms described herein.

223. In addition, by violating Civil Code §§ 1798.81.5 and 1798.82, Defendant "may be enjoined" under Civil Code Section 1798.84(e).

224. Defendant's violations of Civil Code §§ 1798.81.5 and 1798.82 also constitute unlawful acts or practices under the UCL, which affords the Court discretion to enter whatever orders may be necessary to prevent future unlawful acts or practices.

225. Plaintiffs accordingly request that the Court enter an injunction requiring Defendant to implement and maintain reasonable security procedures, including, but not limited to: (1) ordering that

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Defendant utilize strong industry standard data security measures for the collection, storage, and retention of customer data; (2) ordering that Defendant, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis; (3) ordering that Defendant engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (4) ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures; (5) ordering that Defendant, consistent with industry standard practices, segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems are compromised, hackers cannot gain access to other portions of those systems; (6) ordering that Defendant purge, delete, and destroy in a reasonably secure manner class member data not necessary for its provisions of services; (7) ordering that Defendant, consistent with industry standard practices, conduct regular database scanning and security checks; (8) ordering that Defendant, consistent with industry standard practices, evaluate all software, systems, or programs utilized for collection and storage of sensitive Private Information for vulnerabilities to prevent threats to customers; (9) ordering that Defendant, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (10) ordering Defendant to meaningfully educate its customers about the threats they face as a result of the loss of their Private Information.

226. Plaintiffs further request that the Court require Keenan to identify and notify all members of the class who have not yet been informed of the Data Breach, and to notify affected persons of any future data breaches by email within 24 hours of discovery of a breach or possible breach and by mail within 72 hours.

COUNT TEN

INVASION OF PRIVACY

227. Plaintiffs herein repeat, reallege, and fully incorporate all allegations in all preceding paragraphs.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

228. Plaintiffs and class members had a reasonable and legitimate expectation of privacy in their Private Information that Defendant failed to adequately protect against compromise from unauthorized third parties.

229. Defendant owed a duty to Plaintiffs and class members to keep their Private Information confidential.

230. Defendant failed to protect, and released to unknown and unauthorized third parties, the Private Information of Plaintiffs and class members.

231. By failing to keep Plaintiffs' and class members' Private Information safe, knowingly utilizing unsecure systems and practices, Defendant unlawfully invaded Plaintiffs' and class members' privacy by, among others, (i) intruding into Plaintiffs' and class members' private affairs in a manner that would be highly offensive to a reasonable person; (ii) failing to adequately secure their Private Information from disclosure to unauthorized persons and/or third parties; and (iii) enabling the disclosure of Plaintiffs' and class members' Private Information without consent.

232. Defendant knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' and class members' position would consider its actions highly offensive.

233. Defendant knew, or acted with reckless disregard of the fact that, organizations handling PHI are highly vulnerable to cyberattacks and that employing inadequate security software would render them especially vulnerable to data breaches.

234. As a proximate result of such unauthorized disclosures, Plaintiffs' and class members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted, thereby causing Plaintiffs and the class members' undue harm.

235. Plaintiffs seek injunctive relief on behalf of the class, restitution, as well as any and all other relief that may be available at law or equity. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause irreparable injury to Plaintiffs and class members. Plaintiffs and class members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the class.

///

///

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

COUNT ELEVEN

UNJUST ENRICHMENT

236. Plaintiffs herein repeat, reallege, and fully incorporate all allegations in all preceding paragraphs. This claim is pleaded in the alternative to the contract-based counts.

237. Plaintiffs and class members conferred a monetary benefit on Defendant—namely, they provided and entrusted Defendant with their valuable Private Information. Upon information and belief, Defendant funds its data security measures entirely from payments made on behalf of Plaintiffs and the class members, who are the intended beneficiaries of a contract between Defendant and its clients. Accordingly, a portion of such payments made on behalf of Plaintiffs and the class members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

238. In exchange for this payment, Plaintiffs and class members were entitled to reasonable measures to protect their Private Information.

239. Defendant appreciated, accepted, and retained the benefit bestowed upon it under inequitable and unjust circumstances arising from Defendant's conduct toward Plaintiffs and class members as described herein – namely, (a) Plaintiffs and class members conferred a benefit on Defendant, and Defendant accepted or retained that benefit; and (b) Defendant used Plaintiffs' and class members' Private Information for business purposes.

240. Defendant failed to secure Plaintiffs' and class members' Private Information and, therefore, did not provide full compensation for the benefit provided on behalf of Plaintiffs and class members provided.

241. Defendant acquired the Private Information through inequitable means in that it failed to disclose its inadequate security practices previously alleged.

242. Plaintiffs and class members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the class.

243. Under the circumstances, it would be unjust and unfair for Defendant to be permitted to retain any of the benefits conferred on behalf of Plaintiffs and the class.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

244. Under the principles of equity and good conscience, Defendant should not be permitted to retain the Private Information belonging to Plaintiffs and class members because Defendant failed to implement the data management and security measures that industry standards mandate.

245. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and class members, proceeds that they unjustly received on behalf of and for the benefit of Plaintiffs and the class.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf themselves and all others similarly situated, pray for judgment and relief on all cause of action as follows:

A. That the Court determines that this action may be maintained as a class action, that Plaintiffs be appointed as Class Representatives, that the undersigned be named as Class Counsel, and that notice of this action be given to class members;

B. That the Court enter an order declaring that Defendant's actions, as set forth in this complaint, violate the laws set forth above;

C. An order: 1) prohibiting Defendant from engaging in the wrongful acts stated herein (including Defendant's utter failure to provide notice to all affected consumers); 2) requiring Defendant to implement adequate security protocols and practices to protect consumers' Private Information consistent with the industry standards, applicable regulations, and federal, state, and/or local laws; 3) mandating the proper notice be sent to all affected parties, and posted publicly; 4) requiring Defendant to protect all data collected through its account creation requirements; 5) requiring Defendant to delete, destroy, and purge the Private Information of Plaintiffs and class members unless Defendant can provide reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and class members; 6) requiring Defendant to implement and maintain a comprehensive security program designed to protect the confidentiality and integrity of Plaintiffs' and class members' Private Information; 7) requiring Defendant to engage independent third-party security auditors and conduct internal security audit and testing, including

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis; 8) requiring Defendant to engage independent third-party security auditors and/or internal personnel to run automated security monitoring; 9) requiring Defendant to create the appropriate firewalls, and implement the necessary measures to prevent further disclosure and leak of any additional information; 10) requiring Defendant to conduct systematic scanning for data breach related issues; 11) requiring Defendant to train and test its employees regarding data breach protocols, archiving protocols, and conduct any necessary employee background checks to ensure that only individuals with the appropriate training and access may be allowed to access the Private Information data; and 12) requiring all further and just corrective action, consistent with permissible law and pursuant to only those causes of action so permitted.

D. That the Court award Plaintiffs and the class damages (both actual damages for economic and non-economic harm and statutory damages) in an amount to be determined at trial;

E. That the Court issue appropriate equitable and any other relief (including monetary damages, restitution, and/or disgorgement) against Defendant to which Plaintiffs and the class are entitled, including but not limited to restitution and an Order requiring Defendant to cooperate and financially support civil and/or criminal asset recovery efforts;

F. That the Court award Plaintiffs and the class pre- and post-judgment interest (including pursuant to statutory rates of interest set under state law);

G. That the Court award Plaintiffs and the class their reasonable attorneys' fees and costs of suit;

H. That the Court award treble and/or punitive damages insofar as they are allowed by applicable laws; and

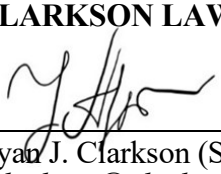
I. That the Court award any and all other such relief as the Court may deem just and proper under the circumstances.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

DATED: September 13, 2024

Respectfully submitted,

CLARKSON LAW FIRM, P.C.



Ryan J. Clarkson (SBN 257074)
rclarkson@clarksonlawfirm.com
Yana Hart (SBN 306499)
yhart@clarksonlawfirm.com
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050

Tina Wolfson (SBN 174806)
twolfson@ahdootwolfson.com
Andrew W. Ferich*
aferich@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Ave. Suite 500
Burbank, CA 91505
Tel: (310) 474-9111

Benjamin F. Johns*
Samantha E. Holbrook*
SHUB & JOHNS LLC
Four Tower Bridge
200 Barr Harbor Drive, Suite 400
Conshohocken, PA 19428
(610) 477-8380
bjohns@shublawyers.com
sholbrook@shublawyers.com

M. Anderson Berry (SBN 262879)
aberry@justice4you.com
Gregory Haroutunian (SBN 330263)
gharoutunian@justice4you.com
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
12100 Wilshire Boulevard, Suite 800
Los Angeles, CA 90025
Tel: (747) 777-7748
Fax: (916) 924-1829

Attorneys for Plaintiffs and the Proposed Class

**admitted pro hac vice*

PROOF OF SERVICE

Heather Heath, et al., v. Keenan & Associates
Case No. 24STCV03018

I am employed in the County of Los Angeles, State of California. I am over the age of 18 and not a party to the within action; my business address is **[X]** 22525 Pacific Coast Highway, Malibu, CA 90265.

On September 25, 2024, I served the foregoing document(s) described as:

SECOND AMENDED CLASS ACTION COMPLAINT

on the interested party(ies) in this action as follows:

JONES DAY John A. Vogt, Esq. *javogt@jonesday.com* Ryan D. Ball, Esq. *rball@jonesday.com* Matthew T. Billeci, Esq. *mbilleci@jonesday.com* 3161 Michelson Drive, Suite 800 Irvine, California 92612.4408 Tel: (949) 851-3939 Fax: (949) 553-7539 *Attorneys for Defendant Keenan & Associates*	**AHDOOT & WOLFSON, P.C.** Tina Wolfson (SBN 174806) *twolfson@ahdootwolfson.com* 2600 W. Olive Ave. Suite 500 Burbank, CA 91505 Tel: (310) 474-9111 Fax: (310) 474-8585 *Attorneys for Plaintiffs*
CLAYEO C. ARNOLD, PROFESSIONAL LAW CORP. M. Anderson Berry, Esq. *aberry@justice4you.com* 865 Howe Avenue Sacramento, CA 95825 Tel: (916) 239-4778 *Attorneys for Plaintiffs*	**SHUB & JOHNS LLC** Andrea Bonner, Esq. *abonner@shublawyers.com* Samantha Holbrook, Esq. *sholbrook@shublawyers.com* Benjamin Johns, Esq. *bjohns@shublawyers.com* Jonathan Shub, Esq. *jshub@shublawyers.com* Four Tower Bridge 200 Barr Harbor Drive, Suite 400 Conshohocken, PA 19428 Tel: (610) 477-8380 *Attorneys for Plaintiffs*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

[X] (VIA ELECTRONIC MAIL) I caused a true and correct copy of the document(s) described above to be electronically served on counsel of record at the electronic service addresses listed above by transmission through third-party CASE ANYWHERE.

[X] (STATE) I declare under penalty of perjury under the laws of the State of California that the above is true and correct.

Executed on September 25, 2024, at Norwalk, California.

Nestor Castillo

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com