

Exhibit A

1 DAVID M. BERGER (277526)
2 LINDA P. LAM (301461)
3 JEFFREY B. KOSBIE (305424)
4 **GIBBS LAW GROUP LLP**
5 1111 Broadway, Suite 2100
6 Oakland, California 94607
7 Telephone: (510) 350-9700
8 Facsimile: (510) 350-9701
9 *dmb@classlawgroup.com*
10 *lpl@classlawgroup.com*
11 *jbk@classlawgroup.com*

12 RACHELE R. BYRD (190634)
13 ALEX J. TRAMONTANO (276666)
14 **WOLF HALDENSTEIN ADLER**
15 **FREEMAN & HERZ LLP**
16 750 B Street, Suite 1820
17 San Diego, CA 92101
18 Telephone: (619) 239-4599
19 Facsimile: (619) 234-4599
20 *byrd@whafh.com*
21 *tramontano@whafh.com*

22 *Proposed Interim Class Counsel*

23 [Additional counsel on signature page]

24
25 **UNITED STATES DISTRICT COURT**
26 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**
27 **SAN FRANCISCO DIVISION**

28 IN RE: SEQUOIA BENEFITS AND
INSURANCE DATA BREACH LITIGATION

Case No. 3:22-cv-08217-WHO

**CONSOLIDATED AMENDED CLASS
ACTION COMPLAINT**

JURY TRIAL DEMAND

1 Plaintiffs Arnab Mitra; Shelby Mitra; Zarina Abardo; Kevin Mindeguia; Erin McGurk;
2 Adam Enger; Amy Carter; Jialin Jiao; Xuan Pan; A.J., by and through her guardian ad litem,
3 Jialin Jiao; Peter Guagenti; E.G., by and through her guardian ad litem Peter Guagenti, S.G., by
4 and through her guardian ad litem Peter Guagenti; Seth Jones; and Christopher Cottrell
5 (“Plaintiffs”), individually and on behalf of all others similarly situated (“Class Members”),
6 bring this Consolidated Amended Class Action Complaint against Sequoia Benefits and
7 Insurance Services, LLC, dba Sequoia Consulting Group and Sequoia One PEO, LLC
8 (collectively, “Sequoia” or “Defendants”), and allege upon personal knowledge as to their own
9 actions and the investigation of their counsel, and upon information and belief as to all other
10 matters, as follows:

11 **I. INTRODUCTION**

12 1. Plaintiffs bring this class action against Sequoia on behalf of themselves and all
13 other persons harmed by the Data Breach that Sequoia announced in or around December 2022
14 (the “Data Breach”).

15 2. Sequoia offers human resources, employee compensation, and employee benefits
16 management and administrative services to businesses. Sequoia One PEO also offers services
17 for employee onboarding, risk and safety management, and worker training and development.
18 Sequoia is used by businesses of all sizes, ranging from startups to public companies such as
19 BuzzFeed and Peloton. Sequoia boasts over 1,700 corporate clients—meaning it stores sensitive
20 personal data on millions of employees and their family members.

21 3. Despite marketing itself as a safe repository for sensitive information, Sequoia
22 failed to take basic precautions designed to keep that information secure. According to Sequoia,
23 between September 22, 2022, and October 6, 2022, hackers gained access to the cloud system
24 that Sequoia uses to store a wide range of sensitive personal information on its customers’
25 employees and their family members—including names, addresses, dates of birth, employment
26 status, marital status, Social Security numbers, wage data related to benefits, member

1 identification cards, Covid-19 test results, and vaccination cards.

2 4. In December 2022, Sequoia began sending letters to affected individuals
3 notifying them that their information was compromised. In those data breach notification letters,
4 Sequoia admits that information in its cloud storage system was accessed by unauthorized
5 individuals. The particularly sensitive nature of the exposed data, which includes Social Security
6 numbers, driver's license numbers, and medical information, means Plaintiffs and Class
7 Members have suffered irreparable harm and are subject to an increased risk of identity theft for
8 the foreseeable future. Indeed, the information taken in the Sequoia Data Breach already is being
9 used to perpetrate identity theft against Class Members.

10 5. Defendants understand the importance of protecting such information. For
11 example, Sequoia's website includes a Privacy Policy that states:

12 **Protection of Your Information**

13 To prevent unauthorized access or disclosure, maintain data accuracy and
14 facilitate the appropriate use of information, Sequoia uses physical, technological
15 and administrative procedures to attempt to protect the personally identifiable
16 information we collect through the Service.¹

17 6. The Data Breach was the result of Sequoia's failure to implement reasonable
18 policies and procedures to protect the security of the personally identifiable information (PII) it
19 collected as part of its business.

20 7. Plaintiffs and Class Members face an ongoing and lifetime risk of identity theft,
21 which is heightened by the exposure of their Social Security numbers and other PII.

22 8. Plaintiffs and Class Members have suffered and will continue to suffer concrete
23 injuries as a result of Defendants' conduct. These injuries include: (i) fraudulent misuse of the
24 stolen PII that is fairly traceable to this Data Breach; (ii) lost or diminished value of PII; (iii) out-
25 of-pocket expenses associated with the prevention, detection, and recovery from identity theft
26 and/or unauthorized use of their PII; (iv) lost opportunity costs associated with attempting to
27 mitigate the actual consequences of the Data Breach, including but not limited to lost time, and

28 ¹Sequoia Privacy Policy, <https://sequoia.com/legal/privacy-policy> (last visited April. 25, 2023).

(v) the present and immediate risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

II. PARTIES

9. **Plaintiff Arnab Mitra** is a citizen of Utah and resides in Cottonwood Heights, Utah. Plaintiff Arnab Mitra works for an organization that uses Sequoia to manage its employee compensation and benefits. In December 2022, he received a Data Breach notification from Sequoia informing him that PII concerning him, his wife, and their two young children was compromised in the Data Breach. As a consequence of the Data Breach, Plaintiff Arnab Mitra has been forced to and will continue to invest significant time monitoring his and his family's accounts to detect and reduce the consequences of likely identity fraud. Despite the fact that his young children should not yet have credit files, Plaintiff Arnab Mitra is concerned that he will have to freeze their credit reports to ensure that no one can take out credit in their names. Given the highly-sensitive nature of the information stolen, Plaintiff Arnab Mitra suffers present, imminent, and impending risk of injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by his personal and financial information being placed in the hands of criminals.

10. **Plaintiff Shelby Mitra** is a citizen of Utah and resides in Cottonwood Heights, Utah. In December 2022, Plaintiff Shelby Mitra's family received a data breach notification from Sequoia informing them that PII concerning Plaintiff Shelby Mitra, her husband, and their children was compromised in the Data Breach. As a result of the Data Breach, Plaintiff Shelby Mitra has been forced to and will continue to invest significant time dealing with attempted fraud, freezing her children's credit reports, and monitoring her family's financial accounts. Prior to the Data Breach, Plaintiff Shelby Mitra had never knowingly been the victim of actual or attempted identity theft or fraud. Since the Data Breach, Plaintiff Shelby Mitra has twice

1 been the victim of attempted fraud. Around the end of November 2022, Plaintiff Shelby Mitra
2 received a notification from Credit Karma that someone tried to open a Bank of America credit
3 card in her name. As a result of the attempted fraud, she spent several hours on the phone with
4 the bank verifying her identity. During this conversation, the bank advised Plaintiff Shelby
5 Mitra to file a police report regarding the incident, a lengthy process that has taken her months
6 to complete.

7 11. Then, in March 2023, Plaintiff Shelby Mitra received emails from Bank of
8 America notifying her that someone had attempted to open a checking account in her name. She
9 once again spent hours on the phone with the bank to verify her identity and ensure that the
10 fraudulent checking account would not be opened. Plaintiff Mitra will need to continue
11 monitoring her credit for additional instances of attempted fraud or identity theft. Given the
12 highly-sensitive nature of the information stolen, Plaintiff Shelby Mitra suffers present,
13 imminent, and impending risk of injury arising from the substantially increased risk of future
14 fraud, identity theft, and misuse posed by her personal and financial information being placed
15 in the hands of criminals.

16 12. **Plaintiff Zarina Abardo** is a citizen of New York and resides in New York
17 City, New York. Plaintiff Abardo works for an organization that uses Sequoia to manage its
18 employee compensation and benefits. In December 2022, Plaintiff Abardo received a Data
19 Breach notification letter from Sequoia informing her that PII concerning her and her partner
20 was compromised in the Data Breach. Given the highly-sensitive nature of the information
21 stolen, Plaintiff Abardo suffers present, imminent, and impending risk of injury arising from
22 the substantially increased risk of future fraud, identity theft, and misuse posed by her personal
23 and financial information being placed in the hands of criminals.

24 13. **Plaintiff Kevin Mindeguia** is domiciled in California and resides in San
25 Francisco, California. Plaintiff Mindeguia works for an organization that uses Sequoia to
26 manage its employee compensation and benefits. In December 2022, Plaintiff Mindeguia

1 received a Data Breach notification letter from Sequoia informing him that PII concerning him,
2 his wife, and his ex-wife was compromised in the Data Breach. Given the highly-sensitive
3 nature of the information stolen, Plaintiff Mindeguia suffers present, imminent, and impending
4 risk of injury arising from the substantially increased risk of future fraud, identity theft, and
5 misuse posed by his personal and financial information being placed in the hands of criminals.

6 14. **Plaintiff Erin McGurk** is a citizen of California and resides in Novato,
7 California. Plaintiff McGurk works for an organization that uses Sequoia to manage its
8 employee compensation and benefits. In December 2022, Plaintiff McGurk received a Data
9 Breach notification letter from Sequoia informing her that her PII was compromised in the Data
10 Breach. As a consequence of the Data Breach, Plaintiff McGurk has been forced to and will
11 continue to invest significant time monitoring her accounts to detect and reduce the
12 consequences of likely identity fraud. Given the highly-sensitive nature of the information
13 stolen, Plaintiff McGurk suffers present, imminent, and impending risk of injury arising from
14 the substantially increased risk of future fraud, identity theft, and misuse posed by her personal
15 and financial information being placed in the hands of criminals. Plaintiff McGurk plans to add
16 a PIN to access her taxes as soon as she is able to do so.

17 15. **Plaintiff Adam Enger** is a citizen of Illinois and resides in Campton Hills,
18 Illinois. Plaintiff Enger is an employee of one of Defendants' clients. Plaintiff Enger received a
19 Data Breach notification letter from Sequoia dated December 7, 2022, informing him that his
20 PII was compromised in the Data Breach. As a result of the Data Breach, Plaintiff Enger has
21 spent time dealing with the consequences of the Data Breach, which include time spent
22 verifying the legitimacy of the notice he received, exploring credit monitoring and identity theft,
23 protection services, and self-monitoring his accounts and credit reports to ensure no fraudulent
24 activity has occurred. This time has been lost forever and cannot be recaptured. Given the
25 highly-sensitive nature of the information stolen, Plaintiff Enger suffers present, imminent, and
26 impending risk of injury arising from the substantially increased risk of future fraud, identity

1 theft, and misuse posed by his personal and financial information being placed in the hands of
2 criminals.

3 17. **Plaintiff Amy Carter** is a citizen of California and resides in Rialto, California.
4 Plaintiff Carter was an employee of one of Sequoia's clients until her retirement on September
5 30, 2022. In December 2022, Plaintiff Carter received a Data Breach notification letter from
6 Sequoia informing her that her PII, including potentially those of her emergency contacts and
7 beneficiaries, was compromised in the Data Breach. As a result of the Data Breach, Plaintiff
8 Carter made reasonable efforts to mitigate the impact of the Data Breach, including but not
9 limited to, researching the Data Breach; reviewing credit reports and financial account
10 statements for any indications of actual or attempted identity theft or fraud; and researching
11 credit monitoring and identity theft protection services offered by Defendants. Plaintiff Carter
12 has spent several hours dealing with the Data Breach, valuable time she otherwise would have
13 spent on other activities. Given the highly-sensitive nature of the information stolen, Plaintiff
14 Carter suffers present, imminent, and impending risk of injury arising from the substantially
15 increased risk of future fraud, identity theft, and misuse posed by her personal and financial
16 information being placed in the hands of criminals.

17 18. **Plaintiff Jialin Jiao** is citizen of California and resides in Mountain View,
18 California. Plaintiff Jiao works for an organization that uses Sequoia to manage its employee
19 compensation and benefits. In December 2022, Plaintiff Jiao received a data breach notification
20 letter from Sequoia informing him that PII concerning him, his wife, and their minor child was
21 compromised in the Data Breach. As a result of the Data Breach, Plaintiff Jiao has been forced
22 to and will continue to invest significant time dealing with attempted fraud and monitoring his
23 and his family's financial accounts. Since the Data Breach, Plaintiff Jiao has experienced a
24 significant increase in the volume of spam text messages. Given the highly-sensitive nature of
25 the information stolen, Plaintiff Jiao suffers present, imminent, and impending risk of injury
26

1 arising from the substantially increased risk of future fraud, identity theft, and misuse posed by
2 his personal and financial information being placed in the hands of criminals.

3 19. **Plaintiff Xuan Pan** is citizen of California and resides in Mountain View,
4 California. Plaintiff Pan's husband, Plaintiff Jiao, works for an organization that uses Sequoia
5 to manage its employee compensation and benefits. In December 2022, Plaintiff Jiao and
6 Plaintiff Pan received a Data Breach notification letter from Sequoia informing them that PII
7 concerning them and their minor child was compromised in the Data Breach. As a result of the
8 Data Breach, Plaintiff Pan has been forced to and will continue to invest significant time dealing
9 with attempted fraud and monitoring her and her family's financial accounts. Since the Data
10 Breach, Plaintiff Pan has experienced a significant increase in the volume of spam calls. Given
11 the highly-sensitive nature of the information stolen, Plaintiff Pan suffers present, imminent,
12 and impending risk of injury arising from the substantially increased risk of future fraud,
13 identity theft, and misuse posed by her personal and financial information being placed in the
14 hands of criminals.

15 20. **Plaintiff A.J.** is a five-year-old minor. Plaintiff A.J. is a citizen of California and
16 resides in Mountain View, California. In December 2022, A.J.'s family received a data breach
17 notification from Sequoia informing them that PII concerning A.J. was compromised in the
18 Data Breach. As a result of the breach, A.J. is at a heightened risk for identity fraud. Therefore,
19 her parents will need to monitor her credit for fraud attempts while she is a minor. Resolving
20 identity fraud on behalf of a child takes families an average of 16 hours—seven hours longer
21 than when adults are victimized. In fact, fraudsters need no more than a child's Social Security
22 number paired with unrelated names and addresses to secure fraudulent credit in a minor's
23 name. Plaintiff A.J. will need to continue to monitor her credit for potential fraud and identity
24 theft into her adulthood. Given the highly-sensitive nature of the information stolen, Plaintiff
25 A.J. suffers present, imminent, and impending risk of injury arising from the substantially
26

1 increased risk of future fraud, identity theft, and misuse posed by her personal and financial
2 information being placed in the hands of criminals.

3 21. **Plaintiff Peter Guagenti** is a citizen of California and resides in Novato,
4 California. Mr. Guagenti works for an organization that uses Sequoia to manage its employee
5 compensation and benefits. In December 2022, Mr. Guagenti received a data breach notification
6 letter from Sequoia informing him that PII concerning him, his wife, and their two children was
7 compromised in the Data Breach.

8 22. As a result of the Data Breach, Plaintiff Guagenti has been forced to and will
9 continue to invest significant time dealing with attempted fraud and monitoring his family's
10 financial accounts. Around January 2023, Plaintiff Guagenti received notice that multiple
11 unauthorized charges had been made on his Capital One credit card. Plaintiff Guagenti then
12 spent at least an hour on the phone with the bank verifying his identity and the fraudulent nature
13 of the charges. Because his credit card number had been compromised, Plaintiff Guagenti was
14 forced to cancel his credit card and wait several weeks for the bank to issue a replacement. Since
15 the Data Breach, Plaintiff Guagenti and his wife have also experienced a significant increase in
16 the volume of phishing e-mails and spam calls and text messages. Given the highly-sensitive
17 nature of the information stolen, Plaintiff Guagenti suffers present, imminent, and impending
18 risk of injury arising from the substantially increased risk of future fraud, identity theft, and
19 misuse posed by his personal and financial information being placed in the hands of criminals.

20 23. **Plaintiff E.G.** is a 13-year-old minor. Plaintiff E.G. is a citizen of California and
21 resides in Novato, California. In December 2022, Plaintiff E.G.'s family received a data breach
22 notification from Sequoia informing them that PII concerning Plaintiff E.G. was compromised
23 in the Data Breach. As a result of the breach, Plaintiff E.G. is at a heightened risk for identity
24 fraud. Therefore, her parents will need to monitor her credit for fraud attempts while she is a
25 minor. Resolving identity fraud on behalf of a child takes families an average of 16 hours—
26 seven hours longer than when adults are victimized. In fact, fraudsters need no more than a

1 to a fraudulent charge of \$77.85. Moreover, Plaintiff Seth Jones regularly receives fraud notices
2 from credit monitoring software obtained via Experian.

3 26. Given the highly-sensitive nature of the information stolen, Plaintiff Jones
4 suffers present, imminent, and impending risk of injury arising from the substantially increased
5 risk of future fraud, identity theft, and misuse posed by their personal and financial information
6 being placed in the hands of criminals.

7 27. **Plaintiff Christopher Cottrell** is a citizen of California who resides in Apple
8 Valley, California. Plaintiff Cottrell received a Data Breach notification letter from Sequoia
9 informing him that his PII was compromised in the Data Breach. As a result of the Data Breach,
10 Plaintiff Cottrell spent time and effort investigating the Data Breach, monitoring his financial
11 accounts, and searching for fraudulent activity. Given the highly-sensitive nature of the
12 information stolen, Plaintiff Cottrell suffers present, imminent, and impending risk of injury
13 arising from the substantially increased risk of future fraud, identity theft, and misuse posed by
14 his personal and financial information being placed in the hands of criminals.

15 28. **Defendant Sequoia Benefits and Insurance Services, LLC dba Sequoia**
16 **Consulting Group** (“Sequoia Benefits”) is a California corporation headquartered at 1850
17 Gateway Drive, Suite 700, San Mateo, CA 94404. Sequoia Benefits offers services, including
18 a software platform that allows businesses to manage employee experience, employee statistics,
19 compensation, and benefits.

20 29. **Defendant Sequoia One PEO, LLC** (“Sequoia One”) is a California
21 corporation headquartered at 22 4th Street, 14th Floor, San Francisco, CA 94103. Sequoia One
22 is a corporate affiliate of Sequoia Benefits that manages human resources, payroll, and
23 employee benefits for businesses.

24 30. Defendants Sequoia Benefits and Sequoia One are related entities with Sequoia
25 One specializing in servicing small businesses. Both Defendants issued breach notification
26 letters following the Data Breach. As the precise corporate relationship between the two

1 Defendants and other possible defendants is not fully known, Plaintiffs and Class Members
2 reserve the right to amend the complaint should the facts and the evidence necessitate it.

3 **III. JURISDICTION AND VENUE**

4 31. This Court has subject matter jurisdiction over this action under 28 U.S.C.
5 § 1332(d)(2) and (3) because this is a class action wherein the amount in controversy exceeds
6 the sum or value of \$5 million, exclusive of interest and costs, there are more than 100 members
7 in the proposed class, and at least one member of the class is a citizen of a state different from
8 Defendants, including Plaintiffs Abardo and Enger.

9 32. This Court has personal jurisdiction over Defendants because Defendants have
10 their principal places of business within this District.

11 33. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because both
12 Defendants' headquarters are located in this District, and they conduct much of their business
13 throughout this District.

14 **IV. FACTUAL ALLEGATIONS**

15 **Background**

16 34. Sequoia Benefits is a human resources, payroll, and benefits management
17 company based in California. It provides software that allows businesses to streamline
18 employee compensation, health benefits, retirement plans, and compliance with human
19 resources requirements. Sequoia Benefits also provides consulting services on those same
20 topics.

21 35. Sequoia One provides outsourced human resources, benefits, and payroll
22 services. Sequoia One's services are marketed towards startups and small businesses. Sequoia's
23 website lists Sequoia One under services offered by Sequoia and explains that when a company
24 is ready to move from the outsource model, Sequoia will help the company transition to other
25 Sequoia products and services.

26 36. Sequoia promotes itself as being able to help businesses "establish secure
27

processes for uploading health information, storing medical verification documents, and ensuring only the right people have access to this sensitive data.”²

37. Sequoia also markets itself as an authority on cybersecurity. For example, it publishes articles to advise its customers and other employers on cybersecurity, including a “Guide to Cyber Protection,”³ “Cyber Liability in the Time of Covid: Ransomware,”⁴ and “Policies for Remote Work: Cybersecurity.”⁵

38. Plaintiffs and Class Members relied on these sophisticated Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their sensitive PII.

39. Defendants had a duty to adopt reasonable measures to protect Plaintiffs’ and Class Members’ PII from involuntary disclosure to third parties.

The Data Breach

40. According to Defendants, between September 22, 2022 and October 6, 2022, unauthorized third-party cybercriminals infiltrated the cloud storage system that Sequoia uses to store sensitive personal information on its customers’ employees and their dependents (the “Data Breach”). For more than two weeks, these cybercriminals went undetected as they accessed PII including names, addresses, dates of birth, gender, employment status, marital status, Social Security numbers, work email address, wage data related to benefits, member identification cards, attachments that may have been provided for advocate services, ID cards including drivers’ licenses, COVID-19 test results, vaccination cards, and emergency contact and beneficiary information.

² <https://www.sequoia.com/platform/workplace/> (last accessed Apr. 25, 2023).

³ <https://www.sequoia.com/2017/08/guide-cyber-protection/> (last accessed Apr. 25, 2023).

⁴ <https://www.sequoia.com/2020/11/cyber-liability-in-the-time-of-covid-ransomware/> (last accessed Apr. 25, 2023).

⁵ <https://www.sequoia.com/2020/11/policies-for-remote-work-cybersecurity/> (last accessed Apr. 25, 2023).

41. It is unclear how long the cybercriminals had access to Plaintiffs' and Class Members' PII before Defendants discovered the Data Breach. On or about December 12, 2022, Defendants transmitted to Plaintiffs and Class Members the notice letter (the "Data Breach Notice") informing them of the Data Breach in which their PII was compromised.

42. The Data Breach Notice stated that between September 22, 2022 and October 6, 2022, an unauthorized actor accessed certain information (their PII) stored on Defendants' cloud storage system network through the cyber-attack or "hacking" incident. This means that not only did the cybercriminals view and access the PII without authorization, but they also downloaded Plaintiffs' and Class Members' PII. In the Data Breach, these criminals acquired the most damaging kind of PII that can be exposed to unauthorized third parties, which included Social Security numbers, sensitive medical information, and highly personal wage data and marital status.

43. Due to Defendants' inadequate and insufficient data security measures, Plaintiffs and Class Members now face an increased risk of fraud and identity theft, and must live with that threat forever. Plaintiffs' PII was both stolen in the Data Breach and is still in the hands of the cybercriminal "hackers." Based on subsequent identity theft incidents, Plaintiffs' PII was distributed through illicit criminal networks, likely including the dark web, as that is the *modus operandi* of cybercriminals who perpetrate cyberattacks of the type that occurred here.

44. Defendants had obligations to Plaintiffs and Class Members to safeguard their PII and to protect it from unauthorized access and disclosure.

45. Plaintiffs and Class Members provided their PII to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

46. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches of major companies preceding the date of the Data Breach.

1 47. In 2021, a record 1,862 data breaches occurred, resulting in approximately
2 293,927,708 sensitive records being exposed, a 68% increase from 2020.⁶

3 48. Indeed, cyberattacks have become so notorious that the Federal Bureau of
4 Investigation (FBI) and U.S. Secret Service have issued a warning to potential targets so they
5 are aware of, and prepared for, a potential attack. As one report explained, “[e]ntities like
6 smaller municipalities . . . are attractive to ransomware criminals . . . because they often have
7 lesser IT defenses and a high incentive to regain access to their data quickly.”⁷

8 49. The increase in such attacks, and attendant risk of future attacks, was widely
9 known to the public and to anyone in the Defendants’ industry, including Defendants. Because
10 Defendants are sophisticated corporations in a data heavy industry, they knew they were at risk
11 and should have shown heightened vigilance around information security concerns.

12 ***Defendants Did Not Use Reasonable Security Procedures***

13 50. Despite this knowledge, Defendants did not use reasonable security procedures
14 and practices appropriate to the nature of the sensitive, non-encrypted information they were
15 maintaining for Plaintiffs and Class Members, causing Plaintiffs’ and Class Members’ PII to be
16 exposed.

17 51. To prevent and detect cyber-attacks, Defendants could and should have
18 implemented adequate information security controls.

19 52. The occurrence of the Data Breach indicates that Defendants failed to adequately
20 implement reasonable and adequate information security controls which resulted in the Data
21 Breach and the exposure of the PII of an undisclosed amount of current and former consumers,
22 including Plaintiffs and Class Members.

23
24
25 ⁶ See 2021 Data Breach Annual Report (ITRC, Jan. 2022) (*available at*:
<https://notified.idtheftcenter.org/s/>), at 6 (last visited on Apr. 25, 2023).

26 ⁷ FBI, Secret Service Warn of Targeted, Law360 (Nov. 18, 2019), *available at*:
27 <https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware>
(last visited Apr. 25, 2023).

1 ***Securing PII and Preventing Breaches***

2 53. Defendants could have prevented this Data Breach by properly securing and
3 encrypting the PII of Plaintiffs and Class Members. Alternatively, Defendants could have
4 destroyed the data that was no longer useful, especially outdated data.

5 54. Defendants' negligence in safeguarding the PII of Plaintiffs and Class Members
6 was exacerbated by the repeated warnings and alerts directed to businesses to protect and secure
7 sensitive data.

8 55. Despite the prevalence of public announcements of data breach and data security
9 compromises, Defendants failed to take appropriate steps to protect the PII of Plaintiffs and
10 Class Members from being compromised.

11 ***Defendants Failed to Comply with FTC Guidelines***

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

16 57. In 2016, the FTC updated its publication, *Protecting Personal Information: A*
17 *Guide for Business*, which established cyber-security guidelines for businesses. The guidelines
18 note that businesses should protect the personal customer information that they keep; properly
19 dispose of personal information that is no longer needed; encrypt information stored on
20 computer networks; understand their network's vulnerabilities; and implement policies to
21 correct any security problems.⁸ The guidelines also recommend that businesses use an intrusion
22 detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity
23 indicating someone is attempting to hack the system; watch for large amounts of data being
24

25 _____
26 ⁸ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016).
27 Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Apr. 25, 2023).

transmitted from the system; and have a response plan ready in the event of a breach.⁹

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

59. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

60. Defendants failed to properly implement basic data security practices.

61. Defendants’ failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs’ and Class Members’ PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

62. Defendants were at all times fully aware of their obligation to protect the PII of Plaintiffs and Class Members. Defendants were also aware of the significant repercussions that would result from their failure to do so.

Defendants Failed to Comply with Industry Standards

63. Federal and state regulators have established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. There are a number of state and federal laws and requirements and industry standards governing the protection of PII.

64. For example, at least 24 states have enacted laws addressing data security

⁹ *Id.*

practices that require that businesses that own, license or maintain personal information, or PII, about a resident of that state to implement and maintain “reasonable security procedures and practices” and to protect PII from unauthorized access.

65. California is one such state. For example, the California Consumer Privacy Act requires Defendants to implement and maintain reasonable security procedures and practices appropriate to the nature of the information that they stored. Cal. Civ. Code § 1798.150(a)(1). Similarly, the California Customer Records Act mandates that “[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use modification or disclosure.” Cal. Civ. Code § 1798.81.5(b).

66. Similarly, the U.S. Government’s National Institute of Standards and Technology (NIST) provides a comprehensive cybersecurity framework that companies of any size can use to evaluate and improve their information security controls.¹⁰

67. NIST publications include substantive recommendations and procedural guidance pertaining to a broad set of cybersecurity topics including risk assessments, risk management strategies, access controls, training, data security controls, network monitoring, breach detection, and incident response.¹¹

68. Information security standards organizations have promulgated many analogous cybersecurity standards that provide businesses with a roadmap to achieve compliance with their common law and statutory obligations to protect PII. These include the HITRUST standard applicable to health information, the COBIT standard for achieving Sarbanes-Oxley compliance, the Center for Internet Security’s Critical Security Controls, and the ISO 27000

¹⁰ See Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology (April 16, 2018), Appendix A, Table 2, *available at*: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> (last visited Apr. 26, 2023).

¹¹ *Id.* at Table 2 pp. 26-43.

1 Series of standards. The ISO standards provide broad based cyber security guidance under ISO
2 27001 and 27002 standards and specific advice for cloud computing security under ISO 27018.

3 69. Sequoia was aware of these guidelines and industry best practices. Had Sequoia
4 followed these best practices, hackers would not have been able to access Plaintiffs' and Class
5 Members' PII. In short, many roadmaps to security existed, but Sequoia failed to follow them,
6 and Plaintiffs and the Class Members now are suffering the consequences of Sequoia's failure.

7 ***Value of Personally Identifiable Information***

8 70. The FTC defines identity theft as "a fraud committed or attempted using the
9 identifying information of another person without authority."¹² The FTC describes "identifying
10 information" as "any name or number that may be used, alone or in conjunction with any other
11 information, to identify a specific person," including, among other things, "[n]ame, Social
12 Security number, date of birth, official State or government issued driver's license or
13 identification number, alien registration number, government passport number, employer or
14 taxpayer identification number."¹³

15 71. The PII of individuals remains of high value to criminals, as evidenced by the
16 prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen
17 identity credentials. For example, Personal Information can be sold at a price ranging from \$40
18 to \$200, and bank details have a price range of \$50 to \$200.¹⁴ Experian reports that a stolen
19 credit or debit card number can sell for \$5 to \$110 on the dark web.¹⁵ Criminals can also

20
21
22
23 ¹² 17 C.F.R. § 248.201 (2013).

24 ¹³ *Id.*

25 ¹⁴ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited Apr. 25, 2023).

26 ¹⁵ *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Apr. 25, 2023).

1 purchase access to entire company data breaches from \$900 to \$4,500.¹⁶

2 72. Social Security numbers, for example, are among the worst kind of PII to have
3 stolen because they may be put to a variety of fraudulent uses and are difficult for an individual
4 to change. The Social Security Administration stresses that the loss of an individual's Social
5 Security number, as is the case here, can lead to identity theft and extensive financial fraud:

6 A dishonest person who has your Social Security number can use it to get other
7 personal information about you. Identity thieves can use your number and your
8 good credit to apply for more credit in your name. Then, when they use the credit
9 cards and don't pay the bills, it damages your credit. You may not find out that
10 someone is using your number until you're turned down for credit, or you begin
11 to get calls from unknown creditors demanding payment for items you never
12 bought. Someone illegally using your Social Security number and assuming your
13 identity can cause a lot of problems.¹⁷

14 73. What is more, it is no easy task to change or cancel a stolen Social Security
15 number. An individual cannot obtain a new Social Security number without significant
16 paperwork and evidence of actual misuse. In other words, preventive action to defend against
17 the possibility of misuse of a Social Security number is not permitted; an individual must show
18 evidence of actual, ongoing fraud activity to obtain a new number.

19 74. Even then, a new Social Security number may not be effective. According to
20 Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able
21 to link the new number very quickly to the old number, so all of that old bad information is
22 quickly inherited into the new Social Security number."¹⁸

23 75. Based on the foregoing, the information compromised in the Data Breach is

24 ¹⁶ *In the Dark*, VPNOverview, 2019, available at:
25 <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Apr. 25,
26 2023).

27 ¹⁷ Social Security Administration, *Identity Theft and Your Social Security Number*, available
28 at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Apr. 25, 2023).

¹⁸ Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR
(Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last visited Apr. 25, 2023).

significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—Social Security number, Driver’s License number, addresses, and financial information.

76. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”¹⁹

77. Among other forms of fraud, identity thieves may use Social Security numbers to obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

78. Driver’s license numbers are also incredibly valuable. “Hackers harvest license numbers because they’re a very valuable piece of information. A driver’s license can be a critical part of a fraudulent, synthetic identity – which go for about \$1200 on the Dark Web. On its own, a forged license can sell for around \$200.”²⁰

79. According to cybersecurity specialty publication CPO Magazine, “[t]o those unfamiliar with the world of fraud, driver’s license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation.”²¹ However, this is not the case.

¹⁹ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Apr. 25, 2023).

²⁰ See Lee Mathews, *Hackers Stole Customers’ License Numbers From Geico In Months-Long Breach* (Apr. 20, 2021), available at: <https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658> (last visited Apr. 25, 2023).

²¹ Scott Ikeda, *Geico Data Breach Leaks Driver’s License Numbers, Advises Customers to Watch out for Fraudulent Unemployment Claims*, CPO Magazine (Apr. 23, 2021), available at: <https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license->

As cybersecurity experts point out:

It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks.²²

80. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.²³

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

82. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("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.²⁴

numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last visited Apr. 26, 2023).

²² *Id.*

²³ *How Identity Thieves Took My Wife for a Ride*, NY Times, April 27, 2021 <https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html> (last visited Apr. 26, 2023).

²⁴ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last visited Apr. 25, 2023).

CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

CASE NO. 3:22-cv-08217-WHO

83. The PII stolen in the Data Breach has significant value, as PII is a valuable property right.²⁵ Sensitive PII can sell for as much as \$363 per record according to the Infosec Institute.²⁶

84. There is also an active and robust legitimate marketplace for PII. In 2019, the data brokering industry was worth roughly \$200 billion.²⁷ In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker, who in turn aggregates the information and provides it to marketers or app developers.²⁸ Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.²⁹

85. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and black markets, has been damaged and diminished by its unauthorized release to third party actors, to whom it holds significant value. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of Plaintiffs' and Class Members' PII has been lost, thereby causing additional loss of value.

86. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, including names, addresses,

²⁵ See, e.g., John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets." (citations omitted)).

²⁶ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last visited Feb. 22, 2023).

²⁷ David Lazarus, *Shadowy Data Brokers Make the Most of Their Invisibility Cloak* (Nov. 5, 2019), <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>.

²⁸ See, e.g., <https://datacoup.com/>; <https://worlddataexchange.com/about>.

²⁹ Computer & Mobile Panel, NIELSEN, available at <https://computermobilepanel.nielsen.com/ui/US/en/sdp/landing> (last visited Feb. 22, 2023).

1 dates of birth, gender, employment status, marital status, Social Security numbers, work email
 2 address, wage data related to benefits, member identification cards, attachments that may have
 3 been provided for advocate services, ID cards including drivers' licenses, COVID-19 test results,
 4 and vaccination cards, and of the foreseeable consequences that would occur if Defendants' data
 5 security system and network was breached, including, specifically, the significant costs that
 6 would be imposed on Plaintiffs and Class Members as a result of a breach.

7 87. Plaintiffs and Class Members now face years of constant surveillance of their
 8 financial and personal records, monitoring, and loss of rights. The Class is incurring and will
 9 continue to incur such damages in addition to any fraudulent use of their PII.

10 88. Defendants were, or should have been, fully aware of the unique type and the
 11 significant volume of data on Defendants' server(s), amounting to potentially millions of
 12 individuals' detailed PII, and, thus, the significant number of individuals who would be harmed
 13 by the exposure of the unencrypted data.

14 89. The injuries to Plaintiffs and Class Members were directly and proximately
 15 caused by Defendants' failure to implement or maintain adequate data security measures for the
 16 PII of Plaintiffs and Class Members. The ramifications of Defendants' failure to keep secure the
 17 PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen, particularly
 18 Social Security numbers, fraudulent use of that information and damage to victims may continue
 19 for years.

20 **V. CLASS ALLEGATIONS**

21 90. Pursuant to Federal Rules of Civil Procedure 23(b)(2), (b)(3) and (c)(4), Plaintiffs
 22 seek certification of the following nationwide class ("Nationwide Class"):

23 **All persons in the United States whose personal information was**
 24 **compromised in the data breach publicly announced by Sequoia in**
 25 **December 2022.**

26 91. Plaintiff Abardo also seeks certification of a New York Subclass, defined as
 27 follows:

All California residents whose personal information was compromised in the data breach publicly announced by Sequoia in December 2022.

94. Excluded from the proposed Class are Defendants, including any entity in which any Defendant has a controlling interest, is a subsidiary, or which is controlled by any Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of any Defendant. Also excluded from the proposed Class are the judge to whom this case is assigned and any members of his or her judicial staff and immediate family.

96. This action is brought and may be maintained as a class action because there is a well-defined community of interest among many persons who comprise a readily ascertainable class. A well-defined community of interest exists to warrant class wide relief because Plaintiffs and all members of the Class were subjected to the same wrongful practices by Defendants, entitling them to the same relief.

97. **Numerosity.** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, given Defendants have 1,700 corporate clients whose employees and their families may have been impacted, the potential number of persons who had their PII compromised in this Data Breach likely numbers in the millions. The identities of Class Members are ascertainable through

1 Defendants' records, Class Members' records, publication notice, self-identification, and other
2 means.

3 98. **Commonality.** There are questions of law and fact common to the Class, which
4 predominate over any questions affecting only individual Class Members. These common
5 questions of law and fact include, without limitation:

- 6 a. Whether and to what extent Defendants had a duty to protect the PII of Plaintiffs
7 and Class Members;
- 8 b. Whether Defendants had a duty not to disclose the PII of Plaintiffs and Class
9 Members to unauthorized third parties;
- 10 c. Whether Defendants had a duty not to use the PII of Plaintiffs and Class Members
11 for non-business purposes;
- 12 d. Whether Defendants failed to adequately safeguard the PII of Plaintiffs and Class
13 Members;
- 14 e. When Defendants actually learned of the Data Breach;
- 15 f. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and
16 Class Members that their PII had been compromised;
- 17 g. Whether Defendants violated the law by failing to promptly notify Plaintiffs and
18 Class Members that their PII had been compromised;
- 19 h. Whether Defendants failed to implement and maintain reasonable security
20 procedures and practices appropriate to the nature and scope of the information
21 compromised in the Data Breach;
- 22 i. Whether Defendants adequately addressed and fixed the vulnerabilities which
23 permitted the Data Breach to occur;
- 24 j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing
25 to safeguard the PII of Plaintiffs and Class Members;
- 26 k. Whether Plaintiffs and Class Members are entitled to actual damages, nominal

1 damages, and/or statutory damages as a result of Defendants' wrongful conduct;

2 1. Whether Plaintiffs and Class Members are entitled to restitution as a result of
3 Defendants' wrongful conduct; and

4 m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress
5 the imminent and currently ongoing harm faced as a result of the Data Breach.

6 99. **Typicality.** Plaintiffs' claims are typical of those of other Class Members
7 because Plaintiffs' PII, like that of every other Class member, was compromised in the Data
8 Breach.

9 100. **Adequacy of Representation.** Plaintiffs will fairly and adequately represent and
10 protect the interests of the Members of the Class. Plaintiffs' Counsel is competent and
11 experienced in litigating Class actions, including data privacy litigation of this kind.

12 101. **Predominance.** Defendants have engaged in a common course of conduct
13 toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was
14 stored on the same computer systems and unlawfully accessed in the same way. The common
15 issues arising from Defendants' conduct affecting Class Members set out above predominate
16 over any individualized issues. Adjudication of these common issues in a single action has
17 important and desirable advantages of judicial economy.

18 102. **Superiority.** A class action is superior to other available methods for the fair
19 and efficient adjudication of this controversy. Class treatment of common questions of law and
20 fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most
21 Class Members would likely find that the cost of litigating their individual claims is
22 prohibitively high and would therefore have no effective remedy. The prosecution of separate
23 actions by individual Class Members would create a risk of inconsistent or varying
24 adjudications with respect to individual Class Members, which would establish incompatible
25 standards of conduct for Defendants. In contrast, treating this action as a class action presents
26 far fewer management difficulties, conserves judicial resources and the parties' resources, and

protects the rights of each Class Member.

103. Defendants have acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

104. Likewise, particular issues under Federal Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendants owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;
- b. Whether Defendants' security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;
- c. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;
- d. Whether Defendants failed to take commercially reasonable steps to safeguard consumer PII; and
- e. Whether adherence to FTC data security recommendations and measures recommended by data security experts would have reasonably prevented the data breach.

105. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendants.

FIRST CAUSE OF ACTION

Negligence

(On Behalf of Plaintiffs and the Nationwide Class)

106. Plaintiffs incorporate by reference all previous allegations as though fully set

1 forth herein.

2 107. Defendants knowingly collected, came into possession of, and maintained
3 Plaintiffs' and Class Members' PII, and had a duty to exercise reasonable care in safeguarding,
4 securing, and protecting such information from being compromised, lost, stolen, misused, and/or
5 disclosed to unauthorized parties.

6 108. Defendants had a duty under common law to have procedures in place to detect
7 and prevent the loss or unauthorized dissemination of Plaintiffs' and Class Members' PII.

8 109. Defendants had full knowledge of the sensitivity of the PII and the types of harm
9 that Plaintiffs and Class Members could and would suffer if the data were wrongfully disclosed.

10 110. By assuming responsibility for collecting and storing this data, and in fact doing
11 so, and sharing it and using it for commercial gain, Defendants had a duty of care to use
12 reasonable means to secure and safeguard their computer property—and Class Members' PII
13 held within it—to prevent disclosure of the information, and to safeguard the information from
14 theft. Defendants' duty included a responsibility to implement processes by which they could
15 detect a breach of their security systems in a reasonably expeditious period of time and to give
16 prompt notice to those affected in the case of a data breach.

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

21 112. Defendants were subject to an “independent duty,” untethered to any contract
22 between Defendants and Plaintiffs or Class Members.

23 113. A breach of security, unauthorized access, and resulting injury to Plaintiffs' and
24 Class Members' PII was reasonably foreseeable, particularly in light of Defendants' inadequate
25 security practices, including sharing and/or storing the PII of Plaintiffs and Class Members on
26 its computer systems.

1 114. Plaintiffs and Class Members were the foreseeable and probable victims of any
2 inadequate security practices and procedures. Defendants knew or should have known of the
3 inherent risks in collecting and storing the PII of Plaintiffs and Class Members, the critical
4 importance of providing adequate security of that data, and the necessity for encrypting all data
5 stored on Defendants' systems.

6 115. Defendants' own conduct created a foreseeable risk of harm to Plaintiffs and
7 Class Members. Defendants' misconduct included, but was not limited to, their failure to take
8 the steps and opportunities to prevent the Data Breach as set forth herein. Defendants'
9 misconduct also included their decisions not to comply with industry standards for the
10 safekeeping of the PII of Plaintiffs and Class Members, including basic encryption techniques
11 freely available to Defendants.

12 116. Plaintiffs and Class Members had no ability to protect their PII that was in, and
13 probably remains in, Defendants' possession.

14 117. Defendants were in a position to protect against the harm suffered by Plaintiffs
15 and Class Members as a result of the Data Breach.

16 118. Defendants had and continue to have a duty to adequately disclose that the PII of
17 Plaintiffs and Class Members within Defendants' possession might have been compromised,
18 how it was compromised, and precisely the types of data that were compromised and when. Such
19 notice is necessary to allow Plaintiffs and Class Members to take steps to prevent, mitigate, and
20 repair any identity theft and the fraudulent use of their PII by third parties.

21 119. Defendants had a duty to comply with the industry standards set out above.

22 120. Defendants, through their actions and/or omissions, unlawfully breached their
23 duties to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and
24 safeguarding Plaintiffs' and Class Members' PII within Defendants' possession.

1 121. Defendants, through their actions and/or omissions, unlawfully breached their
2 duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect
3 and prevent dissemination of Plaintiffs' and Class Members' PII.

4 122. Defendants, through their actions and/or omissions, unlawfully breached their
5 duty to timely disclose to Plaintiffs and Class Members that the PII within Defendants'
6 possession might have been compromised and precisely the type of information compromised.

7 123. Defendants' breach of duties owed to Plaintiffs and Class Members caused
8 Plaintiffs' and Class Members' PII to be compromised.

9 124. As a result of Defendants' ongoing failure to notify Plaintiffs and Class Members
10 regarding the type of PII that has been compromised, Plaintiffs and Class Members are unable
11 to take the necessary precautions to mitigate damages by preventing future fraud.

12 125. Defendants' breaches of duty caused Plaintiffs and Class Members to suffer from
13 identity theft, fraud, loss of time and money to monitor their finances for fraud, and loss of
14 control over their PII.

15 126. As a result of Defendants' negligence and breach of duties, Plaintiffs and Class
16 Members are in danger of present and continuing harm in that their PII, which is still in the
17 possession of third parties, will be used for fraudulent purposes. Plaintiffs and Class Members
18 will need identity theft protection services and credit monitoring services for their respective
19 lifetimes, considering the immutable nature of the PII at issue, which includes Social Security
20 numbers and Driver's License numbers.

21 127. There is a close causal connection between Defendants' failure to implement
22 security measures to protect the PII of Plaintiffs and Class Members and the harm, or risk of
23 imminent harm, suffered by Plaintiffs and Class Members. The PII of Plaintiffs and Class
24 Members was stolen and accessed as the proximate result of Defendants' failure to exercise
25 reasonable care in safeguarding such PII, by adopting, implementing, and maintaining
26 appropriate security measures.

1 support services, website services, delivering promotional materials, answering customer
2 questions about our services and new services.” Sequoia further promised that it would “*only*
3 provide those third party partners with the personally identifiable information they need to
4 deliver the services to us and/or on our behalf, and they will be contractually prohibited from
5 using that information for any other purpose.”³⁰

6 143. By permitting unauthorized third parties to access and exfiltrate the PII of
7 Plaintiffs and the Class, Defendants breached their contracts with their customers, and their
8 promise to “only provide” certain third party partners with the PII “they need to deliver the
9 services to us and/or on [Defendants’] behalf.”

10 144. Defendants knew that if they were to breach these contracts with their clients, the
11 clients’ customers—Plaintiffs and Class Members—would be harmed.

12 145. Defendants and their clients intended at the time the contracts were made that
13 Defendants would assume a direct obligation to protect Plaintiffs’ and the Class Members’ PII.

14 146. Defendants and their clients also intended that Defendants’ performance under
15 their contracts would necessarily and directly benefit Plaintiffs and the Class. Defendants would
16 collect payment from Plaintiffs’ and Class Members’ employers in exchange for providing
17 employee compensation and benefits management for the benefit of Plaintiffs and Class
18 Members.

19 147. Defendants breached these contracts with their clients by, among other things,
20 failing to (i) use reasonable data security measures and (ii) implement adequate protocols and
21 employee training sufficient to protect Plaintiffs’ and Class Members’ PII from unauthorized
22 disclosure to third parties.

23 148. As foreseen, Plaintiffs and the Class were harmed by Defendants’ breach of their
24 contracts with their clients, as such breach is alleged herein, and are entitled to compensatory
25 damages they have sustained as a direct and proximate result thereof.

26
27 ³⁰ <https://www.sequoia.com/legal/privacy-policy/>.

FOURTH CAUSE OF ACTION

Invasion of Privacy

(On Behalf of Plaintiffs and the Nationwide Class)

149. Plaintiffs incorporate by reference all previous allegations as though fully set forth herein.

150. Plaintiffs and Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

151. Defendants owed a duty to Plaintiffs and Class Members to keep their PII confidential.

152. Defendants intentionally failed to protect and released to unknown and unauthorized third parties the non-redacted and non-encrypted PII of Plaintiffs and Class Members.

153. Defendants allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiffs and Class Members, by way of Defendants' failure to protect the PII.

154. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiffs and Class Members is highly offensive to a reasonable person.

155. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and Class Members disclosed their PII to Defendants as part of their relationships with Defendants, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

156. The Data Breach at the hands of Defendants constitutes an intentional interference with Plaintiffs' and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

157. Defendants acted with intention and a knowing state of mind when they permitted the Data Breach to occur because it was with actual knowledge that their information security practices were inadequate and insufficient.

158. Because Defendants acted with this knowing state of mind, they had notice and knew their inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and Class Members.

159. As a proximate result of the above acts and omissions of Defendants, PII of Plaintiffs and Class Members was disclosed to third parties without authorization, causing Plaintiffs and Class Members to suffer damages.

160. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the PII maintained by Defendants can be viewed, distributed, and used by unauthorized persons for years to come. 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 Class Members.

FIFTH CAUSE OF ACTION
Violation of New York General Business Law
N.Y. Gen. Bus. Law § 349
(on behalf of Plaintiff Abardo and the New York Subclass)

161. Plaintiff Abardo incorporates by reference all previous allegations as though fully set forth herein.

162. New York Gen. Bus. Law § 349(a) states: “Deceptive acts or practices in the conduct of any business, trade or commerce in the furnishing of any service in this state are hereby declared unlawful.”

163. Defendants engaged in deceptive acts or practices in the furnishing of services in New York in violation of N.Y. Gen. Bus. Law § 349(a) by, among other things:

a. Omitting and concealing the material fact that they did not employ reasonable

1 measures to secure the PII of Plaintiff Abardo and the New York Subclass.
2 Defendants could and should have made a proper disclosure of their failure to
3 employ reasonable safeguards prior to contracting to provide services to the
4 companies that employ Plaintiff Abardo and the New York Subclass. Defendants
5 also could and should have made a proper disclosure of their failure to employ
6 reasonable safeguards directly to consumers at the time that their requested or
7 received their PII, or by any other means reasonably calculated to inform the New
8 York Subclass of the inadequate data security.

9 b. Making implied or implicit representations that their data security practices were
10 sufficient to protect the PII of Plaintiff Abardo and the New York Subclass.
11 Defendants required members of the New York Subclass to provide their PII,
12 either directly or through their employers. In doing so, Defendants made implied
13 or implicit representations that their data security practices were sufficient to
14 protect consumers' PII. By virtue of accepting the PII of Plaintiff Abardo and the
15 New York Subclass, Defendants implicitly represented that their data security
16 procedures were sufficient to safeguard their PII. Those representations were
17 false and misleading.

18 c. Failing to adopt reasonable safeguards to protect the New York Subclass
19 members' PII in violation of N.Y. Gen. Bus. Law § 899-bb, which states: "Any
20 person or business that owns or licenses computerized data which includes
21 private information of a resident of New York shall develop, implement, and
22 maintain reasonable safeguards to protect the security, confidentiality, and
23 integrity of the private information. . . . Any person or business that fails to
24 comply with this subdivision shall be deemed to have violated section three
25 hundred forty-nine of this chapter."

26 d. Omitting and concealing the material fact that they did not comply with common
27

1 law and statutory duties pertaining to data security, including but not limited to
2 duties imposed by the FTC Act, 15 U.S.C. § 45.

3 164. Defendants' representations and omissions were material because they were
4 likely to deceive reasonable consumers about the adequacy of Defendants' data security and
5 ability to protect the confidentiality of the New York Subclass's PII.

6 165. N.Y. Gen. Bus. Law § 349(h) states:

7 [A]ny person who has been injured by reason of any violation of this section may
8 bring an action in his own name to enjoin such unlawful act or practice, an action
9 to recover his actual damages or fifty dollars, whichever is greater, or both such
10 actions. The court may, in its discretion, increase the award of damages to an
amount not to exceed three times the actual damages up to one thousand dollars,
if the court finds the defendant willfully or knowingly violated this section. The
court may award reasonable attorney's fees to a prevailing plaintiff.

11 166. The various types of damages suffered by Plaintiff Abardo and the New York
12 Subclass alleged herein satisfy both the "injured" and "actual damages" requirements of N.Y.
13 Gen. Bus. Law § 349(h). Plaintiff Abardo and the New York Subclass have suffered and will
14 continue to suffer injury, ascertainable losses of money or property, and monetary and non-
15 monetary damages, including from fraud and identity theft, time and expenses related to
16 monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud
17 and identity theft, loss of value of their PII, and loss of the benefit of the bargain that Defendants
18 agreed to provide to Plaintiffs and Class Members.

19 167. Plaintiff Abardo and the New York Subclass are entitled to treble damages of up
20 to \$1,000 under N.Y. Gen. Bus. Law § 349(h) because Defendants "willfully or knowingly"
21 violated N.Y. Gen. Bus. Law § 349(a). Defendants knew or should have known that their data
22 security practices were deficient. Given the volume and sensitivity of the PII in Defendants'
23 possession, Defendants knew or should have known that they would be a likely target for
24 sophisticated cyberattacks. Defendants should have taken adequate measures to protect against
25 such cyberattacks and should have been aware of any shortcomings. Defendants also willfully
26 and knowingly failed to encrypt or redact the PII.

168. Defendants' deceptive and unlawful practices affected the public interest and consumers at large, including thousands or more of New York residents affected by the Data Breach.

169. Defendants' deceptive and unlawful practices caused substantial injury to Plaintiff Abardo and New York Subclass members that those individuals could not reasonably avoid.

170. Plaintiff Abardo and the New York Subclass are entitled to the injunctive relief sought herein because, among other things, Defendants continue to retain their PII and may subject that PII to further data breaches unless injunctive relief is granted.

171. Plaintiff Abardo and the New York Subclass seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of \$50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

SIXTH CAUSE OF ACTION

Violation of the California Consumer Privacy Act

Cal. Civ. Code §§ 1798.100, *et seq.* (CCPA)

(On behalf the CCPA Plaintiffs and the California Subclass)

172. California Plaintiffs Mindeguia, McGurk, Carter, Jiao, Pan, A.J., Guagenti, E.G. S.G., and Cottrell (the "CCPA Plaintiffs") incorporate by reference all previous allegations as though fully set forth herein.

173. CCPA Plaintiffs and the members of the California Subclass are consumers as that term is defined in Cal. Civ. Code § 1798.140(g).

174. Defendants are businesses as that term is defined in Cal. Civ. Code § 1798.140(c). Defendants are organized or operated for the profit or financial benefit of their owners. Defendants collect consumers' personal information (including that of CCPA Plaintiffs and the California Subclass) or such information is collected on Defendants' behalf, and Defendants determine the purposes and means of the processing of consumers' personal information. Defendants are corporations organized or operated for the profit or financial benefit

1 of its owners with annual gross revenues in excess of \$25,000,000.

2 175. The information accessed during the Data Breach constitutes “personal
3 information” as that term is defined in Cal. Civ. Code § 1798.140(o)(1). At a minimum, that
4 information included names, Social Security numbers, driver’s license numbers, dates of birth,
5 marital status, employment status, and wage data related to benefits.

6 176. Under the CCPA, Defendants had a duty to implement and maintain reasonable
7 security procedures and practices appropriate to the nature of the information that they stored.
8 Cal. Civ. Code § 1798.150(a)(1).

9 177. Defendants’ failure to prevent the Data Breach by implementing and maintaining
10 reasonable security procedures and practices constitutes a breach of their duty under the CCPA.

11 178. As a result of the Data Breach, the nonencrypted and nonredacted personal
12 information of CCPA Plaintiffs and the California Subclass was subject to unauthorized access
13 and exfiltration, theft, or disclosures. The personal information accessed in the Data Breach was
14 nonencrypted and nonredacted as evidenced by the fact that Defendants were required to provide
15 notification letters under the laws of several states that require notification of unauthorized
16 access to nonencrypted and nonredacted information.

17 179. In accordance with Cal. Civ. Code § 1798.150(b), CCPA Plaintiffs provided
18 Defendants with written notice of their alleged violation of Cal. Civ. Code § 1798.150(a).
19 Plaintiffs Mindeguia and McGurk mailed notice by certified mail, return receipt requested, on
20 December 23, 2022. *See Exhibit A.* Defendants responded to Plaintiffs Mindeguia and
21 McGurk’s notice on January 20, 2023.

22 180. On January 11, 2023, Plaintiff Carter provided Defendants with written notice of
23 Defendants’ violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). *See Exhibit B.*
24 Defendants responded to Plaintiff Carter’s notice on January 26, 2023.

25 181. On April 10, 2023, Plaintiffs Jiao, Pan and A.J. provided Defendants with written
26 notice of Defendants’ violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). *See*

1 **Exhibit C.** Defendants have not responded to Plaintiffs Jiao, Pan and A.J.’s notice.

2 182. On April 14, 2023, Plaintiffs Guagenti, E.G. and S.G. provided Defendants with
3 written notice of Defendants’ violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1).

4 *See Exhibit D.* Defendants have not responded to Plaintiffs Guagenti, E.G. and S.G.’s notice.

5 183. On January 12, 2023, Plaintiff Cottrell provided Defendants with written notice
6 of Defendants’ violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). *See Exhibit*
7 **E.** Defendants did not respond to Plaintiff Cottrell’s notice.

8 184. Defendants did not actually cure the noticed violations. Defendants asserted,
9 without evidence or proof, that they “cured” the above failures to implement reasonable security
10 procedures to prevent unauthorized access of Plaintiff Carter’s and California Subclass
11 members’ PII through “steps taken by Sequoia in the aftermath of the breach.” These post- attack
12 actions that Defendants allegedly took did not retroactively cure the unauthorized access, as they
13 provide no assurance that CCPA Plaintiffs’ and California Subclass members’ PII was not
14 viewed by—and/or is not still in the hands of—unauthorized third parties.

15 185. Furthermore, none of the steps Defendants assert in their response demonstrates
16 an actual cure of their failure to implement reasonable security measures to protect CCPA
17 Plaintiffs’ and California Subclass members’ PII, as the vague steps they assert they have taken
18 are not sufficient to protect CCPA Plaintiffs’ and California Subclass members’ PII into the
19 future.

20 186. Defendants’ response is wholly insufficient to demonstrate any “actual cure” of
21 their failure to implement reasonable security to protect Plaintiffs’ and California Subclass
22 members’ information.

23 187. As Defendants have not “actually cured” the violation, CCPA Plaintiffs and the
24 California Subclass seek statutory damages in an amount not less than one hundred dollars
25 (\$100) and not greater than seven hundred and fifty (\$750) per consumer per incident, or actual
26 damages, whichever is greater. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

SEVENTH CAUSE OF ACTION

Violation of the California Unfair Competition Law (UCL)

Cal. Bus. & Prof. Code §§ 17200, *et seq.*

(On behalf of Plaintiffs and the Nationwide Class)

188. Plaintiffs incorporate by reference all previous allegations as though fully set forth herein.

189. Plaintiffs and Defendants are “persons” as defined by Cal. Bus. & Prof. Code § 17201.

190. The UCL prohibits “unlawful, unfair, or fraudulent business acts or practices.”

191. By failing to take reasonable precautions to protect the PII of Plaintiffs and the Class, Defendants have engaged in “unlawful,” “unfair,” and “fraudulent” business practices in violation of the UCL.

192. First, Defendants engaged in “unlawful” acts or practices because they violated multiple laws, including the California Consumer Records Act, Cal. Civ. Code § 1798.81.5; the FTC Act; and the common law, all as alleged herein.

193. Second, Defendants engaged in “unfair” acts or practices, including the following:

a. Defendants failed to implement and maintain reasonable data security measures to protect the Class Members’ PII. Defendants failed to identify foreseeable security risks and adequately maintain their data security in light of the known risk of cyber intrusions, especially in light of the highly sensitive nature of the information which Defendants stored. Defendants’ conduct, with little if any social utility, is unfair when weighed against the harm to the Class Members whose PII has been compromised.

b. Defendants’ failure to implement and maintain reasonable data security measures was contrary to legislatively-declared public policy that seeks to protect consumers’ personal information and ensures that entities entrusted with PII adopt appropriate security measures. These policies are reflected in various laws,

1 including the CCPA (Cal. Civ. Code §§ 1798.100 *et seq.*); the FTC Act (15
2 U.S.C. § 45); and the California Consumer Records Act (Cal. Civ. Code
3 § 1798.81.5).

- 4 c. Defendants' failure to implement and maintain reasonable data security measures
5 led to the substantial consumer injuries described herein. These injuries are not
6 outweighed by countervailing benefits to consumers or competition. Moreover,
7 because consumers could not have reasonably known of Defendants' inadequate
8 data security, consumers could not have reasonably avoided the harms that
9 Defendants' conduct caused.

10 194. *Third*, Defendants engaged in "fraudulent" acts or practices, including but not
11 limited to the following:

- 12 a. Defendants omitted and concealed the fact that they did not employ reasonable
13 safeguards to protect the PII of Plaintiffs and the Class. Defendants could and
14 should have made a proper disclosure of their failure to employ reasonable
15 safeguards prior to contracting to provide services to the companies that employ
16 Plaintiffs and the Class Members. Defendants also could and should have made
17 a proper disclosure of their failure to employ reasonable safeguards directly to
18 Plaintiffs at the time that it requested or received their PII, or by any other means
19 reasonably calculated to inform the Class of the inadequate data security.
- 20 b. Defendants required consumers to provide their PII, either directly or through
21 their employers, in order to administer their benefits and payroll. In doing so,
22 Defendants made implied or implicit representations that its data security
23 practices were sufficient to protect consumers' PII. By virtue of accepting
24 consumers' PII, Defendants implicitly represented that their data security
25 procedures were sufficient to safeguard the PII. Those representations were false
26 and misleading.

1 195. As a direct and proximate result of Defendants’ acts of unlawful, unfair, and
2 fraudulent practices and acts, Plaintiffs and the Class were injured and lost money or property,
3 and suffered the various types of damages alleged herein.

4 196. The UCL states that an action may be brought by any person who has “suffered
5 injury in fact and has lost money or property as a result of the unfair competition.” Cal. Bus. &
6 Prof. Code § 17204. Plaintiffs and the Class Members suffered injury in fact and lost money or
7 property, including in the form of the loss of value of their breached PII, as a result of
8 Defendants’ unfair competition as set forth herein. PII is valuable which is demonstrated by the
9 fact that Defendants’ business is built in part by managing the PII of the Class.

10 197. Plaintiffs and the Class are entitled to injunctive relief to address Defendants’
11 past and future acts of unfair competition.

12 198. Plaintiffs and the Class are entitled to restitution of money and property that
13 Defendants obtained by means of unlawful, unfair, or fraudulent practices, and restitutionary
14 disgorgement of all profits accruing to Defendants as a result of their unlawful and unfair
15 business practices.

16 199. Plaintiffs lack an adequate remedy at law because the injuries here include an
17 imminent risk of identity theft and fraud that can never be fully remedied through damages.

18 200. Further, if an injunction is not issued, Plaintiffs and Class Members will suffer
19 irreparable injury. The risk of another such breach is real, immediate, and substantial. Plaintiffs
20 lack an adequate remedy at law that will reasonably protect them against the risk of such further
21 breach.

22 201. Plaintiffs and the Class seek all monetary and non-monetary relief available to
23 them under the UCL, including reasonable attorney’s fees as allowed under Cal. Code Civ. Proc.
24 §1021.5.

EIGHTH CAUSE OF ACTION

Violation of the California Customer Records Act (CCRA)

Cal. Civ. Code §§ 1798.80, *et seq.*

(On behalf of California Plaintiffs and the California Subclass)

202. California Plaintiffs incorporate by reference all previous allegations as though fully set forth herein.

203. The California legislature enacted the California Customer Records Act (“CCRA”) to “ensure that personal information about California residents is protected.” Cal. Civ. Code § 1798.81.5.

204. The CCRA states that any business which “owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.” Cal. Civ. Code § 1798.81.5(b) (emphasis added).

205. Under the CCRA, personal information includes “[a]n individual’s first name or first initial and the individual’s last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: Social Security number, Driver’s license number . . . [or] medical information.”

206. The personal information compromised in the Data Breach includes information that meets this definition. The information was unencrypted and unredacted as evidenced by the fact that Defendants were required to provide notification letters under the laws of several states that require notification of unauthorized access to unencrypted and unredacted information.

207. Defendants failed to maintain reasonable data security procedures appropriate to the nature of the personal information. Accordingly, Defendants violated Cal. Civ. Code § 1798.81.5(b).

208. California Plaintiffs and the California Subclass were injured by Defendants’ violation of Cal. Civ. Code § 1798.81.5(b) and seek damages pursuant to Cal. Civ. Code § 1798.84(b). California Plaintiffs and the California Subclass were injured in the various ways

1 alleged herein. They seek all monetary and non-monetary relief allowed by the CCRA to
2 compensate for their various types of damages alleged herein.

3 209. California Plaintiffs and the California Subclass are also entitled to injunctive
4 relief pursuant to Cal. Civ. Code § 1798.84(e), including substantial improvements to
5 Defendants' data security systems.

6 **NINTH CAUSE OF ACTION**
7 **Unjust Enrichment**
8 **(On Behalf of Plaintiffs and the Nationwide Class)**

9 210. Plaintiffs incorporate by reference all previous allegations as though fully set
10 forth herein.

11 211. This claim is pleaded in the alternative to the breach of third party beneficiary
12 contract claim above.

13 212. Plaintiffs and Class Members, and Plaintiffs' and Class Members' employers on
14 Plaintiffs' and Class Members' behalf, conferred a monetary benefit to Defendants by paying
15 Defendants for their services.

16 213. Defendants knew that Plaintiffs and Class Members conferred a monetary benefit
17 to Defendants when they accepted and retained that benefit.

18 214. Defendants were supposed to use some of the monetary benefit provided to them
19 from Plaintiffs and Class Members and Plaintiffs' and Class Members' employers to secure the
20 PII belonging to Plaintiffs and Class Members by paying for costs of adequate data management
21 and security.

22 215. Defendants should not be permitted to retain any monetary benefit as a result of
23 their failure to implement necessary security measures to protect the PII of Plaintiffs and Class
24 Members.

25 216. Defendants gained access to the Plaintiffs' and Class Members' PII through
26 inequitable means because Defendants failed to disclose that it used inadequate security
27 measures.

217. Plaintiffs and Class Members were unaware of the inadequate security measures and would not have provided their PII to Defendants had they known of the inadequate security measures.

218. To the extent that this cause of action is pled in the alternative to the others, Plaintiffs and Class Members have no adequate remedy at law.

219. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of Plaintiffs and Class Members; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

220. As a direct and proximate result of Defendants' conduct, 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.

221. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds from the monetary benefit that they unjustly received from them.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendants and that the Court grant the following:

- A. For an Order certifying the Class, and appointing Plaintiffs and their counsel to represent the Class;
- B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members;
- C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:
 - i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
 - iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;
 - iv. requiring Defendants to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiffs' and Class Members' respective lifetimes;
 - v. requiring Defendants to implement and maintain a comprehensive

1 Information Security Program designed to protect the confidentiality and
2 integrity of the PII of Plaintiffs and Class Members;

3 vi. prohibiting Defendants from maintaining the PII of Plaintiffs and Class
4 Members on a cloud-based database;

5 vii. requiring Defendants to engage independent third-party security
6 auditors/penetration testers as well as internal security personnel to conduct
7 testing, including simulated attacks, penetration tests, and audits on
8 Defendants' systems on a periodic basis, and ordering Defendants to
9 promptly correct any problems or issues detected by such third-party security
10 auditors;

11 viii. requiring Defendants to engage independent third-party security auditors and
12 internal personnel to run automated security monitoring;

13 ix. requiring Defendants to audit, test, and train their security personnel
14 regarding any new or modified procedures;

15 x. requiring Defendants to segment data by, among other things, creating
16 firewalls and controls so that if one area of Defendants' network is
17 compromised, hackers cannot gain access to portions of Defendants'
18 systems;

19 xi. requiring Defendants to conduct regular database scanning and securing
20 checks;

21 xii. requiring Defendants to establish an information security training program
22 that includes at least annual information security training for all employees,
23 with additional training to be provided as appropriate based upon the
24 employees' respective responsibilities with handling personal identifying
25 information, as well as protecting the personal identifying information of
26 Plaintiffs and Class Members;

- xiii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xiv. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;
- xv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
- xvi. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;
- xvii. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, statutory, treble,

consequential, and punitive damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

DATED: April 26, 2023

GIBBS LAW GROUP LLP

David M. Berger (277526)
Linda P. Lam (301461)
Jeffrey B. Kosbie (305424)
1111 Broadway, Suite 2100
Oakland, California 94607
Telephone: (510) 350-9700
Facsimile: (510) 350-9701
dmb@classlawgroup.com
lpl@classlawgroup.com
jbk@classlawgroup.com

**WOLF HALDENSTEIN ADLER
FREEMAN & HERZ LLP**

By, /s/ Rachele R. Byrd
Rachele R. Byrd (190634)
Alex J. Tramontano (276666)
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: (619) 239-4599
Facsimile: (619) 234-4599
byrd@whafh.com
tramontano@whafh.com

Interim Class Counsel

**CLAYEO C. ARNOLD
A PROFESSIONAL LAW CORP.**

M. Anderson Berry (262879)
Gregory Haroutunian (330263)
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Fax: (916) 924-1829

aberry@justice4you.com
gharoutunian@justice4you.com

TOUSLEY BRAIN STEPHENS PLLC

Kaleigh N. Boyd (*pro hac vice*)
1200 Fifth Ave., Ste 1700
Seattle, WA 98101
Telephone: (206) 682-5600
kboyd@tousley.com

Interim Class Counsel Executive Committee

29531

EXHIBIT A



December 23, 2022

VIA CERTIFIED U.S. MAIL
RETURN RECEIPT REQUESTED

Sequoia Benefits and Insurance Services, LLC
1850 Gateway Drive, Suite 700
San Mateo, CA 94404

Sequoia One PEO, LLC
22 4th Street, 14th Floor
San Francisco, CA 94103

**Re: Notice of Violation of the California Consumer Legal Remedies Act and
Demand for Relief Pursuant to California Civil Code § 1782**

To Whom It May Concern:

We write on behalf of our clients Kevin Mindeguia and Erin McGurk (“Plaintiffs”) regarding claims against Sequoia Benefits and Insurance Services, LLC and Sequoia One PEO, LLC (collectively, “Sequoia”) arising from the Data Breach that Sequoia announced in or around early December 2022 (“Data Breach”). This letter constitutes notice to, and demand upon, Sequoia for the remedies identified below, pursuant to the California Consumers Legal Remedies Act (“CLRA”), Cal. Civ. Code §§ 1750, *et seq.* If the CLRA violations—described below and in the attached complaint (*Mitra v. Sequoia Benefits & Insurance Services, LLC*, Case No. 3:22-cv-08217-WHO (N.D. Cal.))—are not corrected within 30 days of receipt of this letter, Plaintiffs intend to amend the complaint to seek actual and punitive damages under the CLRA.

Beginning in or around early December 2022, Sequoia announced that it had failed to prevent a data breach, which Sequoia says occurred between September 22 and October 6, 2022. Sequoia’s statements indicate that an unauthorized party was able to access a cloud storage system containing extremely sensitive information about our Client and others. Personal information stored on the breached cloud system included names, addresses, dates of birth, gender, marital status, employment status, Social Security numbers, work email addresses, wage data, member IDs, COVID-19 test results, and vaccine cards. Given the obvious danger of leaving such personal information exposed in cloud storage, Sequoia’s failure to take reasonable precautions is self-evident.

Sequoia represents its products and services as secure. Sequoia’s representations include but are not limited to its representation that it “establish[es] secure process for uploading health

1111 Broadway, Suite 2100, Oakland, CA 94607

📞 510 350 9700

📠 510 350 9701

www.ClassLawGroup.com

To: Sequoia
Re: Notice pursuant to Cal. Civ. Code § 1782(a)
Date: December 23, 2022
Page: 2 of 3

information” and “ensure[s] only the right people have access to this sensitive data.”¹ Sequoia also represents itself as an authority on cybersecurity, including via articles it publishes to advise its customers and other employers on cybersecurity.²

Sequoia’s Conduct Violates the CLRA

Sequoia’s conduct, as described above and in the attached complaint, violates the CLRA, for at least the following reasons:

- By misrepresenting the strength of Sequoia’s data security and by failing to provide notice to affected consumers, Defendants represented that their goods or services are of a particular standard, quality, or grade when they were, in fact, of another standard, quality, or grade, in violation of Cal. Civ. Code § 1770(a)(7).
- By advertising their services as including adequate safeguards for consumer data when Defendants knew that their data security was *not* adequate, Defendants advertised goods or services with intent not to sell them as advertised, in violation of Cal. Civ. Code § 1700(a)(9).

Demand For Relief

Plaintiffs, on behalf of themselves and all others similarly situated, demand that Defendants remedy the above-described violations within 30 days of receiving this notice by doing the following:

- Implement reasonable and adequate security controls to protect consumers’ personal information, subject to approval by undersigned counsel.
- Implement a risk management program for data security that will be adequate to ensure the safety of consumer information as technology and hacking methodologies change, subject to approval by undersigned counsel.
- Disseminate a notice in a form approved by undersigned counsel to all individuals affected by the Data Breach disclosing the breach and providing details regarding how the breach occurred, what data was exposed, and what steps individuals should take.
- Remunerate victims of the data breach for all out-of-pocket costs incurred as a result of the breach, all lost time dealing with the aftermath of the breach, and all losses due to fraud associated with the Data Breach.

¹ <https://www.sequoia.com/platform/workplace/>

² See, e.g., <https://www.sequoia.com/2017/08/guide-cyber-protection/>

1111 Broadway, Suite 2100, Oakland, CA 94607

☎ 510 350 9700

📠 510 350 9701

www.ClassLawGroup.com

To: Sequoia
Re: Notice pursuant to Cal. Civ. Code § 1782(a)
Date: December 23, 2022
Page: 3 of 3

- Compensate victims of the Data Breach for the diminished value of their personal information and for the lost benefit of the bargain based on Sequoia's failure to implement reasonable security measures.
- Disseminate a notice reasonably designed to reach all class members in a form approved by the undersigned counsel setting forth:
 - The existence and a description of this lawsuit, including a summary of the subject matter and the claims asserted;
 - Each class member's right to participate in the lawsuit; and,
 - Information about the Data Breach and how it affects class members.
- Reimburse Plaintiffs and Class members for their reasonable attorney's fees and expenses incurred in bringing this claim.

Please contact us within thirty days to discuss Sequoia's implementation of these remedies.

Very truly yours,

/s/ David M. Berger

David M. Berger

Linda P. Lam

Jeffrey Kosbie

GIBBS LAW GROUP LLP

1111 Broadway, Suite 2100

Oakland, California 94607

Tel: (510) 350-9700

Fax: (510) 350-9701


dmb@classlawgroup.com

lp1@classlawgroup.com

jbk@classlawgroup.com

1111 Broadway, Suite 2100, Oakland, CA 94607

 510 350 9700

 510 350 9701

www.ClassLawGroup.com

EXHIBIT B



ARNOLD LAW FIRM

865 Howe Avenue, Sacramento, CA 95825
7B Corporate Center Court, Greensboro, NC 27408
P: 916-777-7777 | F: 916-924-1829 | justice4you.com

CLAYEO C. ARNOLD
ANTHONY M. ONTIVEROS
JOHN T. STRALEN*
*The Board-Certified Civil
Trial Advocate by the
National Board of Trial
Advocacy

M. ANDERSON BERRY
JOSHUA H. WATSON
ANDREW G. MINNEY
GREGORY HAROUTUNIAN
JEFFREY J.A. HINRICHSEN
MICHAEL WELLS
GINA M. BOWDEN**
**Of Counsel

CLASS ACTION
QUI TAM
DATA BREACH
PERSONAL INJURY
WRONGFUL DEATH
EMPLOYMENT LAW
PRODUCT LIABILITY

January 11, 2023

VIA EMAIL

Sequoia Benefits & Insurance Services, LLC
1850 Gateway Drive, Suite 700
San Mateo, CA 94404

Sequoia One PEO, LLC
22 4th Street, 14th Floor
San Francisco, CA 94103

Sequoia Benefits & Insurance Services, LLC
c/o Agent for Service
CT Corporation System
28 Liberty Street
New York, NY 10005

Sequoia One PEO, LLC
c/o Agent for Service
CT Corporation System
28 Liberty Street
New York, NY 10005

RE: Statutory 30 Day Notice of Claim – Cal. Civil Code 1798.100, et seq.

This letter constitutes notice under the California Consumer Privacy Act (“CCPA”), California Civil Code §1798.100, *et seq.* Pursuant to Civil Code §1798.150(b), we are hereby notifying Sequoia Benefits & Insurance Services, LLC and Sequoia One PEO, LLC (collectively “Sequoia”) that they have violated the CCPA, and we demand that, to the extent any cure exists, Sequoia “actually cures” such violation within thirty (30) calendar days from the date of this letter.

Our client, Amy Carter, resident of Rialto, California, received a Notice of Data Breach from Sequoia on or about December 7, 2022, stating that her personally identifiable information (“PII”) was accessed and no longer secure. The PII exposed includes, at least, her name, address, date of birth, gender, marital status, employment status, Social Security numbers, work email addresses, member ID’s, wage data for benefits, attachments (if any) that may have been provided for advocate services, ID Cards, COVID test results or a vaccine card she may have uploaded. *See* CCPA §1798.81.5(d)(1). Based upon further investigation, and upon information and belief, we have discovered that the PII accessed through Sequoia was stored, unencrypted and insecurely, by, and accessed through Sequoia.

Please be advised that the failure to prevent Mrs. Carter’s and other California residents’ nonencrypted and nonredacted PII from unauthorized access and exfiltration, theft, or disclosure, is a result of Sequoia’s failure to meet its duty to implement and maintain reasonable security procedures and practices, which is a violation of Civil Code §§ 1798.81.5 and 1798.150. These failures include the lack of adequate encryption to sufficiently maintain California residents’ PII and to protect this PII from being accessed by third parties without authorization.

Sequoia Benefits & Insurance Services, LLC

January 11, 2023

Page 2

To the extent there is any possible cure, we request that Sequoia cure this violation which exposed Mrs. Carter's PII and provide an express written statement that the violations have been cured and that no further violations will occur. A cure, if possible, would require Sequoia to, for example, recover all of the stolen PII and eliminate any future risk that Mrs. Carter's stolen PII is misused.

A failure to comply with this request within thirty (30) calendar days will subject Sequoia to statutory damages on an individual and/or class-wide basis.

Thank you for your time and cooperation.

Very truly yours,

A handwritten signature in blue ink, appearing to read 'M. Anderson Berry', is positioned above the typed name and contact information.

M. Anderson Berry, Esq.
aberry@justice4you.com
(916) 239-4778

MAB:lm

EXHIBIT C

**ARNOLD LAW FIRM**

865 Howe Avenue, Sacramento, CA 95825
 7B Corporate Center Court, Greensboro, NC 27408
 P: 916-777-7777 | F: 916-924-1829 | justice4you.com

CLAYEO C. ARNOLD
 ANTHONY M. ONTIVEROS
 JOHN T. STRALEN*
 *The Board-Certified Civil
 Trial Advocate by the
 National Board of Trial
 Advocacy

M. ANDERSON BERRY
 JOSHUA H. WATSON
 ANDREW G. MINNEY
 GREGORY HAROUTUNIAN
 JEFFREY J.A. HINRICHSEN
 BRANDON P. JACK
 GINA M. BOWDEN**
 **Of Counsel

CLASS ACTION
 QUI TAM
 DATA BREACH
 PERSONAL INJURY
 WRONGFUL DEATH
 EMPLOYMENT LAW
 PRODUCT LIABILITY

April 10, 2023

VIA CERTIFIED MAIL
RETURN RECEIPT REQUESTED

Sequoia Benefits & Insurance Services, LLC
 1850 Gateway Drive, Suite 700
 San Mateo, CA 94404

Sequoia One PEO, LLC
 22 4th Street, 14th Floor
 San Francisco, CA 94103

Sequoia Benefits & Insurance Services, LLC
 c/o Agent for Service
 CT Corporation System
 28 Liberty Street
 New York, NY 10005

Sequoia One PEO, LLC
 c/o Agent for Service
 CT Corporation System
 28 Liberty Street
 New York, NY 10005

RE: Statutory 30 Day Notice of Claim – Cal. Civil Code 1798.100, et seq.

This letter constitutes notice under the California Consumer Privacy Act (“CCPA”), California Civil Code §1798.100, *et seq.* Pursuant to Civil Code §1798.150(b), we are hereby notifying Sequoia Benefits & Insurance Services, LLC and Sequoia One PEO, LLC (collectively “Sequoia”) that they have violated the CCPA, and we demand that, to the extent any cure exists, Sequoia “actually cures” such violation within thirty (30) calendar days from the date of this letter.

Our clients, Jialin Jiao, Xuan Pan, and A [REDACTED] J [REDACTED], residents of Mountain View, California, received a Notice of Data Breach from Sequoia on or about December 7, 2022, stating that their personally identifiable information (“PII”) was accessed and no longer secure. The PII exposed includes, at least, their name, address, date of birth, gender, marital status, employment status, Social Security numbers, work email addresses, member ID’s, wage data for benefits, attachments (if any) that may have been provided for advocate services, ID Cards, COVID test results or a vaccine card she may have uploaded. *See* CCPA §1798.81.5(d)(1). Based upon further investigation, and upon information and belief, we have discovered that the PII accessed through Sequoia was stored, unencrypted and insecurely, by, and accessed through Sequoia.

Please be advised that the failure to prevent our clients’ and other California residents’ nonencrypted and nonredacted PII from unauthorized access and exfiltration, theft, or disclosure, is a result of Sequoia’s failure to meet its duty to implement and maintain reasonable security procedures and practices, which is a violation of Civil Code §§1798.81.5 and 1798.150. These failures include the lack of adequate encryption to sufficiently maintain California residents’ PII and to protect this PII from being accessed by third parties without authorization.

Sequoia Benefits & Insurance Services, LLC

April 10, 2023

Page 2

To the extent there is any possible cure, we request that Sequoia cure this violation which exposed Jialin Jiao, Xuan Pan, and A [REDACTED] J [REDACTED]' PII and provide an express written statement that the violations have been cured and that no further violations will occur. A cure, if possible, would require Sequoia to, for example, recover all of the stolen PII and eliminate any future risk that Jialin Jiao, Xuan Pan, and A [REDACTED] J [REDACTED]' stolen PII is misused.

A failure to comply with this request within thirty (30) calendar days will subject Sequoia to statutory damages on an individual and/or class-wide basis.

Thank you for your time and cooperation.

Very truly yours,

A handwritten signature in blue ink, appearing to read "M. Anderson Berry".

M. Anderson Berry, Esq.
aberry@justice4you.com
(916) 239-4778

MAB:lm

EXHIBIT D



April 14, 2023

VIA CERTIFIED U.S. MAIL

RETURN RECEIPT REQUESTED

Sequoia Benefits and Insurance Services, LLC
1850 Gateway Drive, Suite 700
San Mateo, CA 94404

Sequoia One PEO, LLC
350 W Washington Street, Suite 301
Tempe, AZ 85288

Sequoia Benefits & Insurance Services, LLC
c/o C T Corporation System
330 N Brand Blvd.,
Glendale, CA 91203

Sequoia One PEO, LLC
c/o C T Corporation System
330 N Brand Blvd.,
Glendale, CA 91203

Re: Notice of Violation of California Consumer Privacy Act

To Whom It May Concern:

We write on behalf of Peter Guagenti and on behalf of E.G. and S.G., through their guardian, Peter Guagenti, ("Clients") to provide Sequoia Benefits and Insurance Services, LLC and Sequoia One PEO, LLC (collectively, "Sequoia") with pre-filing notice in accordance with the California Consumer Privacy Act, Cal. Civ. Code § 1798.100, *et seq.* ("CCPA"). Clients hereby give notice that Sequoia violated Cal. Civ. Code § 1798.150(a)(1) when Sequoia violated its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information it stored, which led to the unauthorized access and exfiltration, theft, or disclosure of our Clients' nonencrypted and nonredacted personal information.

Beginning in or around early December 2022, Sequoia announced that it had failed to prevent a data breach, which Sequoia says occurred between September 22 and October 6, 2022. Sequoia's statements indicate that an unauthorized party was able to access a cloud storage

1111 Broadway, Suite 2100, Oakland, CA 94607

 510 350 9700

 510 350 9701

www.ClassLawGroup.com

To: Sequoia
Re: Sequoia Data Breach
Date: April 14, 2023
Page: 2 of 3

system containing extremely sensitive information about our Clients and others. Personal information stored on the breached cloud system included names, addresses, dates of birth, gender, marital status, employment status, Social Security numbers, work email addresses, wage data, member IDs, COVID-19 test results, and vaccine cards. Given the obvious danger of leaving such personal information exposed in cloud storage, Sequoia's failure to take reasonable precautions is self-evident.

Sequoia violated § 1798.150(a)(1) of the CCPA for the following reasons:

- Sequoia failed to implement security controls that were adequate to prevent the data breach.
- Each Client's data was accessed without authorization and disclosed to an unauthorized individual or individuals.
- The data breach resulted from a misconfigured cloud storage system, indicating a lack of reasonable security procedures and practices, especially for the highly sensitive nature of the data.
- The stolen data was not encrypted or redacted, as evidenced by the data breach notification letters sent by Sequoia.

Each Client is domiciled in and resides in the State of California, and hereby demands that Sequoia fully cure its § 1798.150(a)(1) violations within 30 days of receiving this CCPA letter. If Sequoia fails to cure its violations of the CCPA, Clients will seek statutory damages as authorized under Cal. Civ. Code § 1798.150(a)(1)(A). In addition, Clients will seek actual damages and any other relief the Court deems proper.

If you have any questions regarding this notice, please do not hesitate to contact me at (510) 350-9713 or dmb@classlawgroup.com.

Very truly yours,

/s/ David M. Berger

David M. Berger

Linda P. Lam

Jeffrey Kosbie

GIBBS LAW GROUP LLP

1111 Broadway, Suite 2100

Oakland, California 94607

Tel: (510) 350-9700

Fax: (510) 350-9701

1111 Broadway, Suite 2100, Oakland, CA 94607

☎ 510 350 9700

☎ 510 350 9701

www.ClassLawGroup.com

To: Sequoia
Re: Sequoia Data Breach
Date: April 14, 2023
Page: 3 of 3

dmb@classlawgroup.com
lpl@classlawgroup.com
jbk@classlawgroup.com

1111 Broadway, Suite 2100, Oakland, CA 94607

 510 350 9700

 510 350 9701

www.ClassLawGroup.com

EXHIBIT E



1990 N. CALIFORNIA BLVD., SUITE 940
WALNUT CREEK, CA 94596
www.bursor.com

JULIA K. VENDITTI
Tel: 925.300.4455
Fax: 925.407.2700
jvenditti@bursor.com

January 12, 2023

Via Certified Mail – Return Receipt Requested

Sequoia Benefits and Insurance Services, LLC
1850 Gateway Drive, Suite 700
San Mateo, CA 94404

Sequoia One PEO, LLC
22 4th Street, 14th Floor
San Francisco, CA 94103

Re: Notice And Demand Letter Pursuant To California Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750; California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100., et seq.; and all other state and local laws

To Whom It May Concern:

This letter serves as a preliminary notice and demand for corrective action by Sequoia Benefits and Insurance Services, LLC (“Sequoia Benefits”) and Sequoia One PEO, LLC (“Sequoia One”) (collectively, “Defendants” or “Sequoia”) pursuant to numerous provisions of California law, including the California Consumers Legal Remedies Act (“CLRA”), Civil Code § 1782(a), the California Consumer Privacy Act (“CCPA”), Cal. Civ. Code. §§ 1798.100, *et seq.*, and any other state law cause of action requiring pre-suit notice, on behalf of our client, Christopher Cottrell (“Client”). This letter also serves as notice for claims of negligence and negligence per se. Mr. Cottrell is acting on behalf of himself as well as a class defined as all similarly situated persons in the United States whose personally identifying information (“PII”) was exposed in Defendants’ December 2022 Data Breach (the “Nationwide Class”). Mr. Cottrell is also acting on behalf of himself as well as a class defined as all similarly situated persons in the State of California who whose PII was exposed in Defendants’ December 2022 Data Breach (the “California Subclass”).

In December 2022, Sequoia announced that between September 22, 2022, and October 6, 2022, Sequoia experienced a data security incident in which an unauthorized party gained access to the cloud storage system, from which the unauthorized party was able to access the sensitive PII maintained on Sequoia’s systems relating to certain of Sequoia’s customers’ employees, former employees, and their dependents and beneficiaries.¹ The information compromised may

¹ See Wired, *Popular HR and Payroll Company Sequoia Discloses a Data Breach* (Dec. 8, 2022), <https://www.wired.com/story/sequoia-hr-data-breach/>; see also <https://www.oag.ca.gov/privacy/databreach/list>;

have included sensitive categories of documents and data, including but not limited to names, addresses, dates of birth, gender, marital status, employment status, Social Security numbers, work email addresses, wage data related to benefits, and member identification cards (as well as any other ID cards), Covid-19 test results, vaccination cards that individuals uploaded to the employment system, and other information contained in the relevant forms. While Sequoia indicates that it learned of the Data Breach as early as October 2022, Sequoia failed to disclose this Data Breach to the California Attorney General until December 12, 2022. However, the victims have not themselves been informed until well after December 12, 2022. Sequoia also failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, and to protect the personal information from unauthorized access, use, and disclosure. Because of these failure on Sequoia's part, customer, employee, and beneficiary information has been compromised.

Our client, Christopher Cottrell, was employed by LegalZoom, one of Sequoia's business customers, as of the time of the Data Breach. Mr. Cottrell faces a substantial and imminent risk of fraud and long-term adverse effects as a result of his PII being compromised.

The acts and practices of Sequoia as described herein violated, and continue to violate, the CLRA in at least the following respects:

- a. in violation of Section 1770(a)(5), Sequoia has represented that its products and services have characteristics and benefits they do not have;
- b. in violation of Section 1770(a)(7), Sequoia has represented that its products and services are of a particular standard, quality, or grade, when in fact they are of another; and
- c. in violation of Section 1770(a)(16), Sequoia has represented that its products and services have been supplied in accordance with a previous representation, when they have not.

Further, Mr. Cottrell also intends to seek relief on behalf of a subclass of similarly situated California consumers under the CCPA, Cal. Civ. Code. §§ 1798.100, *et seq.* Pursuant to the CCPA, "any consumer whose nonencrypted and nonredacted personal information . . . 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." Cal. Civ. Code § 1798.150(a)(1). Here, as a result of Defendants' failure to implement and maintain reasonable security procedures and practices, Mr. Cottrell's personal information² was subject to unauthorized access and disclosure. Pursuant to the CCPA, Mr. Cottrell will seek statutory damages in an amount not less than one hundred dollars (\$100), injunctive or declaratory relief, and any other relief the court deems proper. *See* Cal. Civ. Code

<https://oag.ca.gov/ecrime/databreach/reports/sb24-559929>; <https://oag.ca.gov/system/files/Sequoia%20-%20Sample%20Notices.pdf>.

² "Personal information" is defined to include, among other things, "[a]n individual's first name or first initial and the individual's last name in combination with . . . [m]edical information." Cal. Civ. Code. § 1798.81.5(d)(1)(A)(iv).

§ 1798.150(a)(1)(A-C). This letter likewise serves as notice under the CCPA, pursuant to Cal. Civ. Code § 1798.150(b).

On behalf of our Client and the proposed Classes, we hereby demand that Sequoia immediately: (1) cease, and desist from engaging in, the foregoing violations of the CCPA and CLRA by, *inter alia*, implementing and maintaining reasonable security procedures and practices appropriate to the nature of the information, and protecting the personal information from unauthorized access, use, and disclosure, in the manner required by statute; and (2) make full restitution to all persons for their time, expense, and injury of dealing with the Data Breach.

We further demand that Sequoia preserve all documents and other evidence which refer or relate to any of the above-described practices including, but not limited to, the following:

1. All documents concerning the design, development, testing, implementation, and/or maintenance of Sequoia's digital security systems, including but not limited to contractual agreements between Sequoia and its customers, including but not limited to LegalZoom, concerning the provision of services by Sequoia;
2. All documents concerning Sequoia's knowledge of potential digital security incidents involving Sequoia's properties, including the Data Breach that is the subject of this letter;
3. All documents concerning requests for personal identifying information from consumers;
4. All documents concerning Sequoia's collection, storage, and use of the personal identifying information of employees, former employees, beneficiaries, and dependents;
5. All documents or communications concerning areas of exposure that may have resulted in the Data Breach;
6. All documents and communications with law enforcement concerning Sequoia's response to the Data Breach; and
7. All documents sufficient to show the design and maintenance of the Sequoia services; and
8. All documents or communications concerning the number of persons affected by the Data Breach, and lists of those persons.

If you contend that any statement in this letter is inaccurate in any respect, please provide us with your contentions and supporting documents immediately upon receipt of this letter.

This letter also serves as a thirty (30) day notice and demand requirement under Cal. Civ. Code § 1782 for damages. Accordingly, should Sequoia fail to rectify the situation on a class-wide basis within 30 days of receipt of this letter, our Client will amend his complaint to seek

actual and punitive damages against Sequoia for violations of the CLRA on behalf of himself and the proposed Class(es), seeking monetary damages and equitable relief.

Please contact me right away if you wish to discuss an appropriate way to remedy this matter. If I do not hear from you promptly, I will take that as an indication that you are not interested in doing so.

Sincerely,

A handwritten signature in dark ink, reading "Julia K. Venditti". The signature is written in a cursive, flowing style. The first name "Julia" is written with a large, looped 'J'. The last name "Venditti" is written with a large, looped 'V' and a trailing flourish.

Julia K. Venditti