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

Counsel for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

ARNAB MITRA and ZARINA ABARDO, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

SEQUOIA BENEFITS AND INSURANCE SERVICES, LLC and SEQUOIA ONE PEO, LLC,

Defendants.

Case No.

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiffs Arnab Mitra and Zarina Abardo, individually and on behalf of all others similarly situated, bring this action against Sequoia Benefits and Insurance Services, LLC and Sequoia One PEO, LLC (collectively, "Sequoia" or "Defendants"), and allege as follows:

INTRODUCTION

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

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

3. Despite marketing itself as a safe repository for sensitive information, Sequoia failed to take basic precautions designed to keep that information secure. According to Sequoia, between September 22, 2022, and October 6, 2022, hackers gained access to the cloud system that Sequoia uses to store a wide range of sensitive personal information on its customers' employees and their family members – including names, addresses, dates of birth, employment status, marital status, Social Security numbers, wage data related to benefits, member identification cards, Covid-19 test results, and vaccination cards.

4. In the Data Breach notification letters, Sequoia admits that information in its cloud storage system was accessed by unauthorized individuals. The particularly sensitive nature of the exposed data, which includes Social Security numbers, driver's license numbers, and medical information, means Plaintiffs and Class members have suffered irreparable harm and are subject to an increased risk of identity theft for the foreseeable future. Indeed, the information taken in the Sequoia Data Breach already is reportedly being used to perpetrate identity theft against class members.

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

of its business.

6. As a result of the Data Breach, Plaintiffs' and Class members' PII has been exposed to criminals for misuse. The injuries Plaintiffs and the Class have suffered and will continue to suffer include: theft of personal, medical, and financial information; financial losses caused by misuse of their PII; the loss in value of their PII as a result of the Data Breach; lost time and costs associated with the detection and prevention of identity theft; the loss in the benefits that Defendants were to provide Plaintiffs; and lost time and costs associated with spending time to address and mitigate the actual and future consequences of the breach.

JURISDICTION AND VENUE

7. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. At least one member of the Class defined below is a citizen of a different state than Defendants, and there are more than 100 putative Class members.

8. This Court has personal jurisdiction over Defendants because Defendants maintain their principal place of business in this District, are registered to conduct business in California, and have sufficient minimum contacts with California.

9. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred in this District.

INTRADISTRICT ASSIGNMENT

10. Under Local Rule 3-2(c) and (d), assignment of this action to the San Francisco or Oakland Division is proper because Defendant Sequoia Benefits and Insurance Services, LLC is headquartered in the County of San Mateo and Defendant Sequoia One PEO, LLC is headquartered in the County of San Francisco, and a substantial part of the events or omissions which give rise to the claims alleged herein occurred in those counties.

PARTIES

11. Plaintiff Arnab Mitra is a citizen of Utah and resides in Salt Lake City, Utah. Mr. Mitra works for an organization that uses Sequoia One PEO, LLC 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, Mr. 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, Mr. Mitra is concerned that he will have to freeze their credit reports to ensure that no one can take out credit in their names. Around the end of November 2022, someone tried to open a credit card in his wife's name, and she was advised to file a police report by Bank of America.

12. Plaintiff Zarina Abardo is a citizen of New York and resides in New York City, New York. Ms. Abardo works for an organization that uses Sequoia One PEO, LLC to manage its employee compensation and benefits. In December 2022, Ms. Abardo received a Data Breach notification letter from Sequoia informing her that PII concerning her and her partner was compromised in the Data Breach.

13. Defendant Sequoia Benefits and Insurance Services, LLC ("Sequoia Benefits") is a California corporation headquartered at 1850 Gateway Drive, Suite 700, San Mateo, CA 94404. Sequoia Benefits offers services, including a software platform that allows businesses to manage employee experience, employee statistics, compensation, and benefits.

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

15. Defendants Sequoia Benefits and Insurance Services, LLC and Sequoia One PEO, LLC are related entities, with Sequoia One PEO specializing in servicing small businesses. Both Defendants issued breach notification letters following the Data Breach.

FACTUAL BACKGROUND

A. Background on Sequoia

16. Sequoia Benefits is a human resources, payroll, and benefits management company based in California. It provides software that allows businesses to streamline employee compensation, health benefits, retirement plans, and compliance with human resources requirements. Sequoia Benefits also

provides consulting services on those same topics.

17. Sequoia One provides outsourced human resources, benefits, and payroll. Sequoia One's services are particularly marketed to startups, trying to grow quickly and confidently. Sequoia's website lists Sequoia One under services offered by Sequoia and explains that when a company is ready to move from the outsource model, Sequoia will help the company transition to other Sequoia products and services.

18. Sequoia has been in business for over 20 years. Its annual revenue is $184 million.[1] The company serves over 1,700 corporate clients, including Dropbox, Zoom, Buzzfeed, and Minted. Sequoia is also popular with startups, and says it works with over 500 venture-backed companies.

19. Sequoia promotes itself as being able to help businesses "establish secure processes for uploading health information, storing medical verification documents, and ensuring only the right people have access to this sensitive data."[2]

20. 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]

B. The Data Breach

21. As reported by Sequoia, between September 22, 2022, and October 6, 2022, hackers successfully infiltrated the cloud storage system that Sequoia uses to store sensitive personal information on its customers' employees and their dependents. The system contained a wide range of personal information, including names, addresses, dates of birth, employment status, marital status, Social Security numbers, wage data related to employee benefits, member identification cards, personal ID cards such as driver's licenses, Covid-19 test results, and vaccination cards.

---

[1] https://www.zoominfo.com/c/sequoia-llc/156303577

[2] https://www.sequoia.com/platform/workplace/

[3] https://www.sequoia.com/2017/08/guide-cyber-protection/

[4] https://www.sequoia.com/2020/11/cyber-liability-in-the-time-of-covid-ransomware/

[5] https://www.sequoia.com/2020/11/policies-for-remote-work-cybersecurity/

22. On or around December 2, 2022, it began sending data breach notification letters to the individuals whose data was exposed in the breach.

23. Sequoia has declined to disclose how many individuals' data was compromised in the breach. But based on the company's long list of customers, and the scope of information that Sequoia carelessly stored in the cloud, the breach likely affected millions of individuals.

24. Sequoia's Data Breach notification letters attempt to downplay the harm caused by the Data Breach, stating that Sequoia conducted a forensic review of the breach and "found no evidence that the unauthorized party misused or distributed data" at this time.[6] This statement appears to be designed mislead the data breach victims. Forensic reviews examine the breached company's information systems to determine the scope of the intrusion and what data was taken; they do not typically investigate whether the hackers have misused or distributed the data. In fact, Sequoia's breach notification letters admit that there was unauthorized access to the PII of Plaintiffs and Class members. Cybercriminals seek access to exactly the kind of PII that Sequoia left exposed precisely because they can use it to commit identity theft and other fraud. That means that the individuals affected by the Data Breach remain at risk that their data will be distributed on the dark web and fraudulently used in the future. The extent of the breach and the level of harm it will incur on the affected individuals is not yet known.

C. The Data Breach Was Entirely Avoidable and Foreseeable.

25. Sequoia could have easily prevented the Data Breach. It failed to take adequate and reasonable measures to ensure its computer and cloud storage systems were protected against unauthorized access.

26. Sequoia was well aware of the need to protect the PII that it collects and maintains. The PII compromised in the Data Breach is a valuable commodity to identity thieves, and Sequoia knew or should have known of the likelihood of attempted cyberattacks. In fact, Sequoia's articles on cybersecurity make clear that Sequoia realized the risks of unsecured databases, particularly those hosted in the cloud.

[6] https://www.wired.com/story/sequoia-hr-data-breach/ (last visited December 11, 2022).

27. Sequoia also failed to disclose to Plaintiffs and Class members that its systems and security practices were inadequate to reasonably safeguard their sensitive personal information, and then failed to immediately notify them of the data breach.

28. The Federal Trade Commission has established guidelines for fundamental data security principles and practices for businesses.[7] Among other things, the guidelines note businesses should encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack the system, and have a response plan ready in the event of a breach.[8]

29. Sequoia was at all times aware of its obligations under federal and state laws and regulations to protect data entrusted to it. Despite that awareness, Sequoia's treatment of the PII it stored for Plaintiffs and Class members fell short of satisfying its legal obligations. Among other things, Sequoia failed to encrypt the PII in its possession, and failed to implement and maintain reasonable measures to prevent unauthorized access to that data. To the extent Sequoia relied on outside vendors for cloud security, it failed to ensure that they were implementing reasonable security controls.

D. The Data Breach Harmed Plaintiffs and Class Members, and Will Cause Additional Harm.

30. Individuals who have been victims of data breaches are much more likely to become victims of identity theft than those who have not. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201(9).

31. PII is highly valuable to identity thieves because, as the FTC explained, "[o]nce identity

[7] Federal Trade Commission, Protecting Personal Information: A Guide for Business (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited December 11, 2022).

[8] *Id.*

thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[9]

32. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult to change. The Social Security Administration stresses that the loss of an individual's Social Security number can lead to identity theft and extensive financial fraud:

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

33. Therefore, information compromised in this Data Breach is more valuable than the loss of, for example, credit card information in a retailer data breach. There, victims can close credit and debit card accounts, typically for free. Here, the information compromised—Social Security numbers, names, dates of birth, and addresses—cannot be "closed" and is difficult, if not impossible, to change.

34. Sequoia is offering victims three years of free identity protection services, but the identity protection services Sequoia is offering are inadequate protection. In fact, identity thieves often hold onto personal information in order to commit fraud years after such free programs expire.

35. As a direct and proximate result of Sequoia's wrongful actions, inaction and/or omissions, the resulting Data Breach, and the unauthorized disclosure of Plaintiffs' and Class members' PII, Plaintiffs and Class members have suffered, and will continue to suffer, ascertainable losses, economic damages, and other injuries, including:

a. The compromise, publication, theft, and/or unauthorized use of their PII;

---

[9] http://www.leginfo.ca.gov/pub/15-16/bill/asm/ab_1551-1600/ab_1580_cfa_20160613_144620_sen_comm.html (last visited December 11, 2022).

[10] Social Security Administration, Identity Theft and Your Social Security Number, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited December 11, 2022).

b. Lost value of their PII as a result of its theft and unauthorized use;

c. Loss of the benefit of the bargain that Sequoia agreed to provide to Plaintiffs and Class Members;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from 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 identity theft and fraud; and

f. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of Plaintiffs' and Class members' lives.

36. In addition to a remedy for economic harm, Plaintiffs and Class members maintain an undeniable interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft.

37. To date, other than providing three years of identity protection services, Sequoia does not appear to be taking any measures to assist Plaintiffs and Class members.

CLASS DEFINITION AND ALLEGATIONS

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

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

Plaintiff Mitra also seeks certification of a Utah Subclass, defined as follows:

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

Plaintiff Abardo also seeks certification of a New York Subclass, defined as follows:

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

39. The Nationwide Class, Utah Subclass, and New York Subclass are collectively referred to herein as the "Class" unless otherwise stated.

40. 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.

41. Plaintiffs reserve the right to amend or modify the class definitions with greater specificity or division, or create and seek certification of additional classes, after having had an opportunity to conduct discovery.

42. **Numerosity**: Although the exact number of Class members is uncertain and can only be ascertained through appropriate discovery, the number is great enough – with the Data Breach impacting, on information and belief, millions of individuals – such that joinder is impracticable. The disposition of the claims of these Class members in a single action will provide substantial benefits to all parties and to the Court. Class members may be identifiable from objective means, such as information and records in Defendants' possession, custody, or control.

43. **Commonality and Predominance**: Common questions of law and fact exist as to the proposed Class members and predominate over questions affecting only individual Class members. These common questions include:

a. Whether Defendants knew or should have known that their systems were vulnerable to unauthorized access;

b. Whether Defendants failed to take adequate and reasonable measures to ensure their data systems were protected;

c. Whether Defendants failed to take available steps to prevent and stop the breach from happening;

d. Whether Defendants owed a legal duty to Plaintiffs and Class members to protect their PII;

e. Whether Defendants breached any duty to Plaintiffs and Class members by failing to exercise due care in protecting their PII;

f. Whether Plaintiffs and Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

g. Whether Plaintiffs and Class members are entitled to equitable relief, including, but not limited to, injunctive relief or restitution.

44. **Typicality:** Plaintiffs' claims are typical of the claims of other Class members. All Class members were subject to the data breach and had their PII accessed by and/or disclosed to unauthorized third parties.

45. **Adequacy of Representation:** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other Class members they seek to represent; they have retained counsel competent and experienced in class action litigation and data breach litigation, and Plaintiffs will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

46. **Declaratory and Injunctive Relief:** The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for Defendants. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class members and impair their interests. Defendants have acted and/or refused to act on grounds generally applicable to the Class, making injunctive relief or corresponding declaratory relief appropriate.

47. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and Class members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendants, making it impracticable for Class members to individually seek redress for Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individual litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents

far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

FIRST CAUSE OF ACTION

Negligence

(On behalf of the nationwide class)

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

49. As a condition of receiving Sequoia's services, Plaintiffs and Class members were required to provide Sequoia with their PII.

50. Plaintiffs and Class members entrusted their PII to Sequoia with the understanding that Sequoia would take reasonable measures to safeguard their PII.

51. Sequoia owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII entrusted to it from being compromised, lost, stolen, accessed, or misused by unauthorized persons. This duty included: (a) designing, maintaining, and testing Sequoia's security systems to ensure that Plaintiffs' and Class Members' PII in Sequoia's possession was adequately secured and protected; (b) designing, maintaining, and testing the configuration of any cloud storage or other external services used by Sequoia to ensure the PII stored in or accessible from them was adequately secured and protected including protection against any known or unknown threats; (c) implementing processes that would detect a breach of its security systems in a timely manner; (d) timely acting upon warnings and alerts, including those generated by these security systems; and (e) maintaining data security measures consistent with industry standards.

52. Sequoia's duty to use reasonable care arose from several sources, including those listed below.

a. Sequoia had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class members were the foreseeable and probable victims of any inadequate security practices. Not only was it foreseeable that Plaintiffs and Class members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for identity theft, Sequoia knew

that it was more likely than not that Plaintiffs and other Class members would be harmed in the event of a Data Breach.

b. Sequoia's duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII by companies such as Sequoia. Various FTC publications and data security breach orders also form the basis of Sequoia's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created Sequoia's duty.

c. Sequoia's duty also arose from Sequoia's unique position as an organization that specializes in handling PII. Sequoia holds itself out as a trusted steward of the PII that it receives, and thereby assumes a duty to reasonably protect that data. Otherwise, Plaintiffs and Class members would be powerless to fully protect their interests with regard to their PII in Sequoia's hands.

d. Sequoia's duty also arose under state statutes that required Sequoia to reasonably safeguard sensitive PII, as detailed herein.

53. Sequoia breached the duties it owed to Plaintiffs and Class members described above and was thus negligent by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols, and practices, sufficient to protect the PII of Plaintiffs and Class members; (b) maintain security systems consistent with industry standards; (c) failing to encrypt the PII in its possession; (d) and failing to provide adequate and timely notice of the Data Breach to consumers.

54. Plaintiffs and Class members were the foreseeable victims of Sequoia's inadequate data security. Sequoia knew that a breach of its systems could cause harm to Plaintiffs and Class members.

55. Sequoia's conduct created a foreseeable risk of harm to Plaintiffs and Class members. Sequoia's conduct included its failure to adequately secure its cloud storage infrastructure to protect the PII of Plaintiffs and Class members.

56. Sequoia knew or should have known of the inherent risks in collecting and storing massive

amounts of PII, the importance of providing adequate data security over that PII, and the frequent cyberattacks on businesses that store sensitive PII like that in Sequoia's possession.

57. Plaintiffs and Class members had no ability to protect their PII once it was in Sequoia's possession and control. Sequoia was in an exclusive position to protect against the harm suffered by Plaintiffs and Class members as a result of the Data Breach.

58. But for Sequoia's breach of its duties, the PII of Plaintiffs and Class members would not have been compromised in the Data Breach.

59. There is a temporal and close causal connection between Sequoia's failure to implement adequate data security measures, the Data Breach, and the harms suffered by Plaintiffs and Class members.

60. As a direct and proximate result of Sequoia's negligence, Plaintiffs and Class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include the following: ongoing, imminent, impeding threat of identity theft and fraud, resulting in monetary loss, economic harm, and loss of time; actual identity theft and fraud, resulting in monetary loss, economic harm, and loss of time; loss of value in their PII; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other activities; expenses and time spent initiating fraud alerts; loss of the benefit of the bargain that Sequoia agreed to provide to Plaintiffs and Class Members; and lost work time.

SECOND CAUSE OF ACTION

Negligence per se

(On behalf of the nationwide class)

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

62. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Sequoia of failing to use reasonable measures to protect PII.

63. The FTC publications and orders also form the basis of Sequoia's duty.

64. Sequoia violated Section 5 of the FTC Act (and similar state statutes) by failing to use

reasonable measures to protect PII and not complying with industry standards. Sequoia's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach of that data.

65. Sequoia's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

66. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

67. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and the Class.

68. As a direct and proximate result of Sequoia's negligence, Plaintiffs and Class members have been injured as described herein and in Paragraph 60 above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD 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)

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

70. 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."

71. Sequoia 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 it did not employ reasonable measures to secure the PII of Plaintiff Abardo and the New York Subclass. Sequoia could and should have made a proper disclosure of its failure to employ reasonable safeguards

prior to contracting to provide services to the companies that employ Plaintiff Abardo and the New York Subclass. Sequoia also could and should have made a proper disclosure of its failure to employ reasonable safeguards directly to consumers at the time that it requested or received their PII, or by any other means reasonably calculated to inform the New York Subclass of the inadequate data security.

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

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

d. Omitting and concealing the material fact that it did not comply with common law and statutory duties pertaining to data security, including but not limited to duties imposed by the FTC Act, 15 U.S.C. § 45.

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

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

> [A]ny person who has been injured by reason of any violation of this section may bring an action in his own name to enjoin such unlawful act or practice, an action to recover his actual damages or fifty dollars, whichever is greater, or both such 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.

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

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

76. Sequoia's 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.

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

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

79. 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.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually, and on behalf of all others similarly situated, respectfully request the following relief:

a. An order certifying the proposed Class as requested herein, appointing Plaintiffs as class representatives and their undersigned counsel as class counsel;

b. An order finding that Defendants engaged in the unlawful conduct as alleged herein;

c. An order enjoining Defendants from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of Plaintiffs' and Class members' PII;

d. A mandatory injunction directing Defendants to hereinafter adequately safeguard Plaintiffs' and Class members' PII by implementing improved security procedures and measures;

e. An award of compensatory, statutory, and punitive damages, as appropriate, in an amount to be determined;

f. An award of pre-judgment and post-judgment interest on all amounts awarded;

g. An award of Plaintiffs' and Class members' reasonable attorney's fees and litigation expenses; and

h. Such other relief as the Court deems just and proper.

JURY DEMAND

Plaintiffs, individually, and on behalf of all others similarly situated, hereby demand a trial by jury as to all matters so triable.

Dated: December 12, 2022

Respectfully submitted,

/s/ David M. Berger

GIBBS LAW GROUP LLP
David M. Berger (SBN 277526)
Linda P. Lam (SBN 301461)
Jeffrey B. Kosbie (SBN 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

Counsel for Plaintiffs