M. Anderson Berry (262879)
Gregory Haroutunian (330263)
CLAYEO C. ARNOLD
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Fax: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

Nathan D. Prosser (*pro hac vice* forthcoming)
HELLMUTH & JOHNSON, PLLC
8050 West 78th Street
Edina MN 55439
Telephone: (952) 941-4005
Fax: (952) 941-2337
nprosser@hjlawfirm.com

Terence R. Coates (*pro hac vice* forthcoming)
Dylan J. Gould (*pro hac vice* forthcoming)
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Telephone: (513) 665-0204
Fax: (513) 665-0219
tcoates@msdlegal.com
dgould@msdlegal.com

Attorneys for Plaintiff and Putative Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

ADAM ENGER, on behalf of himself and on behalf of all others similarly situated,

Plaintiff,

v.

SEQUOIA BENEFITS AND INSURANCE SERVICES LLC dba SEQUOIA CONSULTING GROUP,

and

SEQUOIA ONE PEO LLC,

Defendants.

Case No. _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Adam Enger ("Plaintiff") brings this Class Action Complaint against Sequoia Benefits and Insurance Services LLC d/b/a Sequoia Consulting Group ("Sequoia Consulting") and Sequoia One PEO LLC ("Sequoia One") (collectively, "Defendants") in his individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Defendants provide benefit and payroll management services. Plaintiff bring this class action against Defendants for their failure to properly secure and safeguard Personally Identifiable Information ("PII") provided by their clients or the employees of its clients, including, without limitation, names, addresses, dates of birth, gender, marital status, employment status, Social Security numbers, work email addresses, wage data related to benefits, and member IDs as well as any other ID cards, Covid-19 test results, and vaccine cards that individuals uploaded to the employment system (collectively "Private Information").

2. Defendants failed to use reasonable industry standard security measures, which would have prevented this type of attack from being successful. Defendants' failure to use such measures is particularly egregious given the amount of highly sensitive Private Information that they maintain and the prevalence of data security incidents in the finance and banking industries.

3. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiff and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

4. Criminals can access and then offer for sale this unencrypted, unredacted Private Information to criminals. The exposed Private Information of Plaintiff and Class Members can be sold on the dark web. Plaintiff and Class Members now face a present and continuing lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

5. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendants' failure to: (i) adequately protect the Private Information

of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendants' inadequate information security practices; and (iii) effectively secure its network containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendants' conduct amounts to negligence and violates federal and state statutes.

6. Plaintiff and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) lost or diminished value of Private Information; (ii) out-of-pocket expenses associated with the prevention of, detection of, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (iv) the continued and certainly increased 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 Private Information.

7. Defendants disregarded the rights of Plaintiff and Class Members by recklessly or negligently failing to implement and maintain adequate and reasonable measures to ensure that the Private Information of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the Private Information of Plaintiff and Class Members was compromised through disclosure to a known criminal organization. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

8. Plaintiff Adam Enger is domiciled in the State of Illinois. Plaintiff received a notice letter from Sequoia Benefits and Insurance Services, LLC dated December 7, 2022 informing him that his Private Information was compromised in the Data Breach.

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

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

11. 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.

JURISDICTION & VENUE

12. The Court has personal jurisdiction over Defendants because they are headquartered in this District.

13. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. 1332(d)(2). The matter in controversy exceeds $5,000,000 in the aggregate, exclusive of interest and costs. Further, Plaintiff alleges a nationwide class, and Plaintiff himself is domiciled in a different state than Defendant.

14. Venue is appropriate in this District under 28 U.S.C. § 1391(a) because Defendants are headquartered in this District, and because a substantial portion of the events giving rise to this cause of action occurred in this District.

15. 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.

BACKGROUND

16. Defendants offer human resources, employee compensation, and employee benefits management and administrative services to businesses. Sequoia One 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.

17. According to its website, Defendants are licensed in 50 states and have over 1,500 corporate clients.[1] Last year, Defendants realized approximately $184 million in revenue.

18. Sequoia One says it serves more than 500 venture-capital backed firms.[2]

19. Upon information and belief, Defendants store the Private Information of millions of individuals.

20. Defendants encourage their clients to "Un-silo your data and fully leverage your entire HR stack," stating that their Sequoia HRX platform "brings together all your data from previously-disconnected transactional systems and centralizes everything in one place for a holistic view of the programs that make up your total people investment."[3]

21. Defendants' services are largely data-driven. Their website states that "Operating people programs with siloed data stuck in disconnected systems makes it hard to see the bigger picture and understand how your people investments impact your business. People and business leaders need to bring everything together – unifying your people data, program designs, utilization metrics, benchmarking, and more – under a complete and holistic strategy that addresses the entire lifecycle of total people investment."[4]

THE DATA BREACH

22. According to Defendants, unauthorized actors gained access to Defendants' cloud computing storage systems between September 22, 2022, and October 6, 2022.

[1] https://www.sequoia.com/about/ (last visited December 18, 2022).
[2] https://www.bankinfosecurity.com/report-outsourced-hr-firm-sequoia-one-undergoes-data-breach-a-20666 (last visited December 18, 2022).
[3] https://www.sequoia.com/platform/sequoia-hrx/ (last visited December 19, 2022).
[4] https://www.sequoia.com/total-people-investment/ (last visited December 19, 2022).

23. According to a disclosure that Defendants made to the Maine Attorney General, Defendants did not discover the unauthorized access until November 17, 2022.[5]

24. A sample notice letter dated December 12, 2022 that Defendants provided to the California Attorney General unequivocally states that an "unauthorized party was able to access your personal information …."[6]

25. Publications have noted that it is "not clear if Sequoia has the technical means, such as logs, to determine what information was accessed or what data was siphoned, if any."[7] However, it is clear that "'this is a massive breach that will have a large impact on all affected customers based on the amount of sensitive data that has been stolen.'"[8]

26. Defendants reported to the Maine Attorney General that the Data Breach exposed the Private Information of 580,818 victims.

27. Recognizing the severity of the Data Breach, Defendants have provided victims with the opportunity to sign up for 36 months of Experian Identity Works credit monitoring services.

The Data Breach was Foreseeable and Preventable

28. In an August 11, 2017, blog post, Defendants warns clients that "[a] thorough review of your exposures, systems in place, contracts with partners, and data collected are critical when analyzing your cyber exposure. With the increased risk of cyber threats in today's global economy, your first defense is being sure you have the right protection in place."[9]

29. In a July 16, 2020 blog post, Defendants acknowledged that "[o]ver the past ten years, there have been massive, high-profile data breaches and abuses of consumer trust

[5] https://apps.web.maine.gov/online/aeviewer/ME/40/b0f0f020-c1d8-408a-97be-7ab76094a7ae.shtml (last visited Dec. 18, 2022).
[6] https://oag.ca.gov/system/files/Sequoia%20-%20Sample%20Notices.pdf (last visited Dec. 19, 2022).
[7] https://techcrunch.com/2022/12/12/sequoia-human-resources-hackers/ (last visited Dec. 18, 2022).
[8] https://siliconangle.com/2022/12/08/personal-information-exposed-breach-employer-services-company-sequoia/ (last visited Dec. 18, 2022).
[9] https://www.sequoia.com/2017/08/guide-cyber-protection/ (last visited Dec. 19, 2022).

(Facebook/Cambridge Analytica, Yahoo, Marriott, Equifax, Target)."[10] The blog post quotes "Ameesh Divatia, co-founder and CEO of data protection company Baffle," who warns that those ""that play 'fast and loose' will see an immediate hit to their brand impact, mounting legal and regulatory costs and their long-term health of their business come into question. In contrast, those that design their systems to share data responsibly will thrive and soar in value."'[11]

30. The rate of cyberattacks on American businesses increased dramatically in the wake of the COVID-19 pandemic. As Defendants noted in a November 16, 2022, blog post, "[w]ith a surge in cybercrime since the pandemic began, it is critical that companies train employees to remain vigilant and protect their employers' data both online and offline."[12]

31. An August 2, 2021, blog post on Defendants' website states that "Cyber attacks continue to rise," citing a report which found that in 2021, the percentage of businesses experiencing a cyber-attack increased from 38% to 43%.[13]

32. A February 14, 2022, blog post on Defendants' website again acknowledged that, "[c]yber-attacks are on the rise! This phrase, or similar ones, have been appearing in the news and in information security articles for many years, and will continue to do so."[14]

33. Defendants state that they use "strong encryption algorithms such as AES-256 for data at rest and TLS 1.2/1.3 for HTTPS connections so that data is encrypted both in transit and at rest (when stored)."[15] However, upon information and belief, the Private Information accessed in the Data Breach was not encrypted, as evidenced by the fact that Defendants reported the Data

[10] https://www.sequoia.com/2020/07/2020-cyber-risk-landscape-lets-do-a-deep-dive/ (Dec. 19, 2022).
[11] *Id.*
[12] https://www.sequoia.com/2020/11/policies-for-remote-work-cybersecurity/ (last visited Dec. 19, 2022).
[13] https://www.sequoia.com/2021/08/hiscox-cyber-readiness-report/ (last visited Dec. 19, 2022).
[14] https://www.sequoia.com/2022/02/the-value-of-information-and-why-attackers-send-text-messages-to-your-phone/ (last visited Dec. 18, 2022).
[15] https://www.sequoia.com/trust/#security (last visited Dec. 18, 2022).

Breach to the California Attorney General and sent notifications to individual victims. California law requires companies to notify California residents "whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person" due to a "breach of the security of the system[.]" Cal. Civ. Code § 1798.82(a)(1). Defendants notified the California Attorney General of the Data Breach on or about December 12, 2022, evidencing that the exposed data was unencrypted.

34. Defendants state that their "endpoints are secured using advanced solutions to detect and respond quickly to malicious attacks. We also leverage web filtering solutions to prevent malicious internet traffic. Systems are monitored 24/7 by a variety of technologies and our SIEM is monitored 24/7/365 by a leading MSSP."[16] Upon information and belief, these representations are false, as evidenced by the fact that unauthorized third parties had uninterrupted access to Defendants' cloud storage system between September 22, 2022, and October 6, 2022, which Defendants did not detect until November 17, 2022.[17]

35. To prevent and detect unauthorized cyber-attacks, in addition to following its own advice, Defendant could and should have implemented, as recommended by the United States Government, the following measures known to be generally effective at mitigating the risk of a cyberattack:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users, and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

[16] https://www.sequoia.com/trust/#security (last visited Dec. 18, 2022).
[17] https://apps.web.maine.gov/online/aeviewer/ME/40/b0f0f020-c1d8-408a-97be-7ab76094a7ae.shtml (last visited Dec. 19, 2022).

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[18]

36. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks. . . .

[18] *Id.* at 3–4.

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net). . . .
- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it. . . .
- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic. . . .[19]

37. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates;
- Use threat and vulnerability management;
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

[19] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Dec. 19, 2022).

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities;
- Hunt for brute force attempts;
- Monitor for cleanup of Event Logs;
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall;
- Enable tamper protection;
- Enable cloud-delivered protection;
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[20]

38. Even if the cybercriminals had been able to access Defendant's network despite reasonable security measures, Defendant could have prevented the consequences by properly encrypting the files containing PII, or destroying PII it no longer had a legitimate need for.

39. Given that Defendant was storing the PII of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

40. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the unauthorized exposure and exfiltration of the PII of Plaintiff and Class Members.

Defendants Violated Federal Trade Commission Guidelines

[20] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Dec. 19, 2022).

41. Defendants also violated the duties applicable to it under the Federal Trade Commission Act (15 U.S.C. § 45 et seq.) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC, pursuant to that Act, has concluded that a company's failure to maintain reasonable and appropriate data security for sensitive personal information is an "unfair practice" in violation of the FTC Act.

42. As established by these laws, Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the medical information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants also owed a duty to Plaintiff and Class Members to provide reasonable security in compliance with industry standards, and state and federal requirements, and to ensure that its computer systems, networks, and protocols adequately protected this medical information and were not exposed to infiltration. This also included a duty to Plaintiff and Class Members to design, maintain, and test its computer systems to ensure that the Private Information and medical information was adequately secured and protected; to create and implement reasonable data security practices and procedures to protect the Private Information and medical information in its possession, and avoid access to its systems through processes such as phishing, including adequately training employees and others who accessed information within its systems on how to adequately protect this information and to avoid permitting such infiltration such as by use of multi-factor authentication; to implement processes that would detect a breach of its data security systems in a timely manner, and to act upon data security warnings and alerts in a timely fashion; to disclose if its computer systems and data security practices were inadequate to safeguard individuals' Private Information; and to disclose in a timely and accurate manner when data breaches or ransomware attacks occurred.

43. Defendants also needed to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network were compromised, hackers could not gain access to other portions of Defendants' systems. It is apparent from the data accessed that Defendants did not do so.

44. Defendants owed these duties to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices. Defendants affirmatively chose to design these systems with inadequate user authentication, security protocols and privileges, and set up faulty patching and updating protocols. These affirmative decisions resulted in unauthorized actors being able to execute the ransomware attack and exfiltrate the data in question, to the injury and detriment of Plaintiff and Class Members. By taking affirmative acts inconsistent with these obligations that left Defendants' computer systems vulnerable to a ransomware attack, Defendants disclosed and/or permitted the disclosure of Private Information and medical information to unauthorized third parties. Defendants thus failed to preserve the confidentiality of Private Information it was duty-bound to protect.

Value of Personally Identifiable Information

45. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Defendants' own blog states that, "We all know data is valuable to organizations, and it directly translates to services and money. But data is also valuable to the 'bad guys.'"[21]

46. The Sequoia blog post cites a 2021 Forbes article, which explained the value of a full set of PII is "valued at $1,010."[22]

[21] https://www.sequoia.com/2022/02/the-value-of-information-and-why-attackers-send-text-messages-to-your-phone/ (last visited Dec.19, 2022).
[22] *Id.*

47. Defendants' blog includes the following graphic created by Experian to explain the value of PII:[23]

48. Indeed, numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[24] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[25] Criminals can also purchase access to entire company data breaches from $900 to $4,500.

49. Social Security numbers, for example, 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 for an individual to change. The Social Security Administration stresses that the loss of an

[23] *Id.*

[24] *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 Dec. 19, 2022).

[25] *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 Dec. 18, 2022).

individual's Social Security number, as is the case here, 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.[26]

50. It is incredibly difficult to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

51. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[27]

52. Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft.

53. Indeed, a robust cyber black market exists in which criminals post stolen Medical Information, PII and PHI on multiple underground internet websites, commonly referred to as the dark web, to create fake insurance claims, purchase and resell medical equipment, or access prescriptions for illegal use or resale. According to a 2017 Javelin strategy and research presentation, fraudulent activities based on data stolen in data breaches that are between two and

---

[26] *Identity Theft and Your Social Security Number*, Social Security Administration, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Dec. 19, 2022).

[27] Bryan 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 Dec. 19, 2022).

six years old had increased by nearly 400% over the previous four years.[28] Thus, an offer of credit monitoring service that is only for two years is not an adequate remedy or offer, even if it conducts dark web scanning (which is unclear here).

54. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, only 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, including Social Security numbers and names, is impossible to "close" and difficult, if not impossible, to change.

55. 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."[29]

56. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

57. 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.[30]

---

[28] *See,* Brian Stack, *Here's How Much Your Personal Information is Selling for on the Dark Web* (2017) https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Dec. 19, 2022).

[29] Time 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 Dec. 19, 2022).

[30] *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: https://www.gao.gov/assets/gao-07-737.pdf (last visited Dec. 19, 2022).

58. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

59. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

60. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' storage platform, amounting to potentially millions of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

61. To date, Defendants have offered Plaintiff and Class Members only three years of identity theft detection services. The offered service is wholly inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the Private Information at issue here, and is not an adequate cure of the Data Breach.

62. Defendants has not provided sufficient information in its Data Breach Notice Letter such that Plaintiff and Class Members could understand and appreciate the full nature of the risk to them caused by Defendants' Data Breach, allowing them to make informed decisions about how to protect themselves and their Private Information.

63. Defendants have not provided credit monitoring and identity theft protection to Plaintiff and Class Members for a long enough period of time, limiting the bulk of the protection services to 2 years even though this data may be used for years after that.

64. Defendants' identity theft protection offer of Experian's IdentityWorks 3B does not prevent fraudulent transactions, such as unauthorized credit card charges or exchanges of Plaintiff's Private Information on the dark web from occurring using the Private Information

disclosed by Defendant. Further, IdentityWorks 3B does not provide 3-Bureau Credit Report & FICO Scores monthly, unlike other Experian products.

65. Enrollment in IdentityWorks 3B requires Plaintiff and Class Members to disclose Private Information to Experian, a company that had its own data breach in 2015, exposing the personal information of approximately 15 million individuals.

66. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

Plaintiff's Experience

67. Plaintiff is an employee of one of Defendants' clients.

68. Plaintiff provided his Private Information to his employer and Defendants with the expectation that his Private Information would remain confidential.

69. Plaintiff is very careful about sharing his sensitive Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff stores any documents containing his Private Information in a safe and secure location or destroys the documents.

70. Plaintiff received a letter from Sequoia Benefits and Insurance Services, LLC dated December 7, 2022, stating that the following personal information may have been accessed in the Data Breach: name, address, date of birth, gender, marital status, employment status, Social Security number, work email address, member IDs, wage data for benefits, any attachments that he provided for advocate services, ID cards, COVID test results, and vaccination card.

71. As a result of the Data Breach, Plaintiff has spent time dealing with the consequences of the Data Breach, which include time spent verifying the legitimacy of the notice he received, exploring credit monitoring and identity theft protection services, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

72. Plaintiff has suffered injury from the invasion of his privacy.

73. Plaintiff suffered injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

74. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

75. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of unauthorized third parties.

76. Upon information and belief, Plaintiff's Private Information remains in Defendants' possession. Plaintiff has a continuing interest in ensuring that his Private Information—which, upon information and belief, remains backed up in Defendants' possession—is protected and safeguarded from future data breaches.

CLASS ACTION ALLEGATIONS

77. Plaintiff brings this nationwide class action on behalf of himself and all others similarly situated under Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

78. The Nationwide Class is defined as follows:

> **All persons Defendants identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.**

79. Excluded from the Class are Defendants' officers and directors; any entity in which Defendants has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

80. Plaintiff reserves the right to amend or modify the Class definitions and/or create additional subclasses as this case progresses.

81. Numerosity. The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time the Classes consists of more than 500,000 current and former employees of Defendants and acquired subsidiaries whose sensitive data was compromised in Data Breach.

82. Commonality. There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendants owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendants breached their duty to Class Members to safeguard their Private Information;

g. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

h. Whether Defendants should have discovered the Data Breach sooner;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

j. Whether Defendants' conduct was negligent;

k. Whether Defendants failed to provide notice of the Data Breach in a timely

manner; and,

l. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

83. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

84. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's counsel are competent and experienced in litigating class actions.

85. Predominance. Defendants has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

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

87. Defendants has 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.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

88. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 87.

89. As a condition of receiving services from Defendant, Defendants' current and former customers were obligated to provide Defendants with their Private Information or the Private Information of their employees.

90. Plaintiff and the Class entrusted their Private Information to Defendants on the premise and with the understanding that it would be safeguarded, used for business purposes only, and not disclosed to unauthorized third parties.

91. Defendants had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

92. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

93. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that the Private Information of Plaintiff and the Class in Defendants' possession was adequately secured and protected.

94. Defendants also had a duty to implement appropriate data retention schedules regarding Private Information, and to delete it when Defendants were no longer required to retain

it pursuant to regulations or legitimate business purposes.

95. Defendants also had a duty to have procedures in place to detect and prevent the improper access and misuse of the Private Information of Plaintiff and the Class.

96. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants on the one hand and Plaintiff and the Class on the other. That special relationship arose because Plaintiff and the Class entrusted Defendants with their confidential Private Information, as a necessary part receiving services from Defendant.

97. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiff or the Class.

98. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

99. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of providing adequate security of that information, and the necessity for encrypting or redacting Private Information stored on Defendants' systems.

100. Defendants' own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendants' misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included their decisions to not comply with industry standards for the safekeeping of the Private Information of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

101. Plaintiff and the Class had no ability to protect their Private Information that was in, and likely remains in, Defendants' possession.

102. Defendants were in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

103. Defendants had and continues to have a duty to adequately disclose that the Private Information of Plaintiff and the Class within Defendants' possession might have been

104. compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

105. Defendants had a duty to employ proper procedures to prevent the unauthorized dissemination of the Private Information of Plaintiff and the Class.

106. Defendants has admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

107. Defendant, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Private Information of Plaintiff and the Class during the time the Private Information was within Defendants' possession or control.

108. Defendants improperly and inadequately safeguarded the Private Information of Plaintiff and the Class by deviating from standard industry rules, regulations, and practices at the time of the Data Breach.

109. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect the Private Information of Plaintiff and the Class in the face of increased risk of theft.

110. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of Private Information.

111. Defendants, through their actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

112. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the Class, the Private Information of Plaintiff and the Class would not have been compromised.

113. There is a close causal connection between Defendants' failure to implement security measures to protect the Private Information of Plaintiff and the Class and the present harm, or risk of imminent harm, suffered by Plaintiff and the Class. The Private Information of Plaintiff and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

114. Defendants' violations of California and federal statutes also constitute negligence *per se*. Defendants violated California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendants to undertake reasonable measures to safeguard the Private Information of Plaintiff and the Class, as well as the FTC Act.

115. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present 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 Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information of Plaintiff and the Class; and (viii) costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

116. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiff and the Class 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.

117. Additionally, as a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, 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 Private Information in their continued possession.

118. Plaintiff and Class Members are therefore entitled to damages, including restitution and unjust enrichment, declaratory and injunctive relief, and attorneys' fees, costs, and expenses.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Nationwide Class)

119. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 87.

120. The Private Information of Plaintiff and the Class was provided and entrusted to Defendants. Plaintiff and the Class provided their Private Information to Defendants, either directly or indirectly through Defendants' clients, as part of Defendants' regular business practices.

121. As a condition of employment from Defendants' clients, Plaintiff and the Class provided and entrusted their Private Information to Defendants. In so doing, Plaintiff and the Class entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen, in return for the business services provided by Defendants.

122. A meeting of the minds occurred when Plaintiff and the Class agreed to, and did, provide their Private Information to Defendants and/or Defendants' clients with the reasonable understanding that their Private Information would be adequately protected from foreseeable threats. This inherent understanding exists independent of any other law or contractual obligation any time that highly sensitive PII is exchanged as a condition of receiving services. It is common sense that but for this implicit and/or explicit agreement, Plaintiff and Class Members would not have provided their Private Information.

123. Defendants separately had contractual obligations arising from and/or supported by the consumer-facing statements in their Privacy Policies.

124. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendants.

125. Defendants breached the implied contracts they made with Plaintiff and the Class by failing to safeguard and protect their Private Information, and by failing to provide timely and accurate notice that Private Information was compromised as a result of the Data Breach.

126. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

127. As a result of Defendants' breach of implied contract, Plaintiff and the Class are entitled to and demand actual, consequential, and nominal damages.

COUNT III
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiff and the Nationwide Class)

128. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 87.

129. Plaintiff brings this claim for breach of third-party beneficiary contract against Defendants in the alternative to Plaintiff's claim for breach of implied contract.

130. Defendants entered into various contract with their clients to provide services.

131. These contracts are virtually identical to each other and were made expressly for the benefit of Plaintiff and the Class, as it was their Private Information that Defendants agreed to collect and protect through their services, and their employee benefits that Defendants' were contracting to administer. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties.

132. Defendants knew that if it were to breach these contracts with its clients, the clients' employees, including Plaintiff and the Class, would be harmed by, among other things, fraudulent misuse of their Private Information.

133. Defendants breached their contracts with their clients when they failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiff's and Class Members' Private Information.

134. As reasonably foreseeable, Plaintiff and the Class were harmed by Defendants' failure to use reasonable data security measures to store their Private Information, including but not limited to, the actual harm through the loss of their Private Information to cybercriminals.

135. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, 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, as defined herein, and appointing Plaintiff and their Counsel to represent each such 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 Private Information of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff 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 its 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 Plaintiff 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 Plaintiff and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

v. prohibiting Defendants from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;

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

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

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

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

x. requiring Defendants to conduct regular database scanning and securing checks;

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

xii. 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;

xiii. requiring Defendants to implement a system of tests to assess their 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;

xiv. 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;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential Private Information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. 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, statutory, nominal, and consequential 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

Plaintiff hereby demands that this matter be tried before a jury.

Respectfully Submitted,

DATED: December 19, 2022

By, */s/ M. Anderson Berry*

M. Anderson Berry (262879)
Gregory Haroutunian (330263)
CLAYEO C. ARNOLD
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Fax: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

Nathan D. Prosser (*pro hac vice* forthcoming)
HELLMUTH & JOHNSON, PLLC
8050 West 78th Street
Edina MN 55439
Telephone: (952) 941-4005
Fax: (952) 941-2337
nprosser@hjlawfirm.com

Terence R. Coates (*pro hac vice* forthcoming)
Dylan J. Gould (*pro hac vice* forthcoming)
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Telephone: (513) 665-0204
Fax: (513) 665-0219
tcoates@msdlegal.com
dgould@msdlegal.com