Exhibit A

CLARKSON LAW FIRM, P.C.
Yana Hart (SBN 306499)
yhart@clarksonlawfirm.com
Mark Richards (SBN 321252)
mrichards@clarksonlawfirm.com
Bryan P. Thompson (SBN 354683)
bthompson@clarksonlawfirm.com
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050

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

MILBERG COLEMAN BRYSON PHILLPS GROSSMAN, PLLC
John J. Nelson (SBN 317598)
jnelson@milberg.com
280 S. Beverly Drive
Beverly Hills, CA 92102
Tel: (858) 209-6941

Interim Co-Lead Counsel for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

In re SAG Health Data Breach Litigation This Document Relates to: All Actions	Lead Case No. 2:24-cv-10503-MEMF-JPR CONSOLIDATED ACTION **CONSOLIDATED CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiffs Matthew Rouillard, Kristy Munden, Lee Wilkof, Steven Barr, and Massimiliano Furlan ("Plaintiffs") individually and on behalf of all others similarly situated, ("Plaintiffs") bring this Action against SAG-AFTRA Health Plan ("SAG Health" or "Defendant"), and allege upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. SAG Health provides a comprehensive health care benefits program for eligible participants and their dependents in the entertainment industry. Entertainment workers can earn eligibility through employment with producers who have signed a collective bargaining agreement with the entertainment industry's largest union: the Screen Actors Guild-American Federation of Television and Radio Artists ("**SAG-AFTRA**"). Tens of thousands of SAG-AFTRA members have availed themselves of SAG Health's offerings, which include a wide range of medical services.

2. To obtain any of these services, members are required to entrust SAG Health with their highly sensitive and personally identifiable information ("**PII**") and personal health information ("**PHI**"), which SAG Health uses to engage in its usual business activities. SAG Health understands that it has a responsibility to protect the data it collected from unauthorized access, assuring its customers that it is "committed to protecting [members'] privacy."[1] Despite this assurance to its customers, however, SAG Health failed to protect the very customer information it was entrusted, compromising the personal information of an undisclosed number of its members ("**The Data Breach**"), announced by Defendant on December 2, 2024.[2]

3. SAG Health failed to properly secure and safeguard the highly valuable,

1 SAG-AFTRA Health Plan Privacy Policy, SAG-AFTRA Health Plan (2019), https://www.sagaftraplans.org/health/privacy (last accessed July 31, 2025).

2 SAG-AFTRA Health Plan Email Phishing Notice, SAG-AFTRA Health Plan (2024), https://www.sagaftraplans.org/health/emailphishingnotice (last accessed July 31, 2025).

PII and PHI of its members, including their names, Social Security numbers, and information associated with claims and health insurance information, and other sensitive medical and non-medical data (collectively, "**Private Information**"), failed to comply with industry standards to protect information systems that contain Private Information, and failed to provide timely and adequate notice to Plaintiffs and other members of the Class that their Private Information had been accessed and compromised.

4. Even the most fundamental Private Information, like names, email addresses, home addresses, or phone numbers, when paired with other uniquely personalized data like health insurance information, Social Security numbers, and health plan identification numbers, become especially valuable to cybercriminals to create seemingly legitimate, personalized phishing scams. The combined exfiltrated data effectively provides criminals with a key to their personal lives, making it easy to match additional data, gaining access to their personal and financial accounts and insight on their preferences. Hackers are now able to build a three-dimensional picture, and thereby exploit SAG Health's members.

5. SAG Health disregarded the rights of Plaintiffs and Class Members by, inter alia, failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to properly train its staff and employees on proper security measures.

6. SAG Health should have ensured that it had adequate monitoring software in place to detect intrusions or the transfer of large volumes of data to third party networks, that it implemented multi-factor authentication to verify the credentials of individuals attempting to access Private Information, that it limited

access to Private Information to only necessary employees, that it encrypted or tokenized Private Information in internet accessible locations, and that it deleted or redacted Private Information that it was no longer required to maintain. By failing to implement these reasonable and industry standard data security measures, SAG Health enabled the unauthorized access of Plaintiffs' and Class Members' Private Information.

7. In addition, SAG Health failed to properly monitor its computer network and systems that housed the Private Information. Had it properly monitored these electronic and cloud-based systems, it would have discovered the intrusion sooner or prevented it altogether.

8. The unfortunate reality is that this could have been avoided, had Defendant taken adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions. Instead, it neglected industry standards, failed to take standard and reasonably available steps to prevent the Data Breach, all while promising its members advanced security to maintain an advantage in highly sensitive and competitive industry.

9. Equally troubling, SAG Health failed to provide timely and adequate notice to Plaintiffs and other members of the Class that their Private Information had been accessed and compromised. Underscoring its grossly negligent business practices, Defendant waited 3 months before disclosing the Data Breach to SAG-Health Plan members.

10. As a direct and proximate result of Defendant's inadequate security measures and disclosure of information to an unauthorized criminal third-party, Plaintiffs and the class suffered several injuries, including (i) out-of-pocket expenses associated with preventing, detecting, and remediating identity theft, social engineering, and other unauthorized use of their Private Information; (ii) opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iii) the continued, long term, and

certain increased risk that unauthorized persons will access and abuse Plaintiffs' and Class Members' Private Information; (iv) the continued and certain increased risk that the Private Information that remains in Defendant's possession is subject to further unauthorized disclosure for so long as Defendant fails to undertake proper measures to protect the Private Information; (v) invasion of privacy and disclosure of their personal information, as well as an increased risk of fraud and identity theft; (vi) theft of their Private Information and the resulting loss of privacy rights in that information; (vii) diminution in value and/or lost value of Private Information, a form of property that Defendant obtained from Plaintiffs and Class Members.

11. Plaintiffs bring this lawsuit on behalf of themselves and all those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained. To remedy these violations of law, Plaintiffs and Class Members thus seek actual damages, statutory damages, restitution, and injunctive and declaratory relief (including significant improvements to Defendant's data security protocols and employee training practices), reasonable attorneys' fees, costs, and expenses incurred in bringing this action, and all other remedies this Court deems just and proper.

II. PARTIES

A. Plaintiff Matthew Rouillard

12. Plaintiff Matthew Rouillard is a citizen and resident of New York, New York.

13. Plaintiff Rouillard entrusted his Private Information to Defendant in connection with his enrollment and participation in the SAG-AFTRA Health Plan.

14. Plaintiff Rouillard received a notice of the Data Breach from Defendant on December 2, 2024.

15. Plaintiff Rouillard only allowed Defendant to maintain, store, and use his Private Information because he reasonably expected that Defendant would use basic security measures to protect his Private Information and prevent its access by

unauthorized third parties, such as requiring passwords and multi-factor authentication to access accounts or databases storing his Private Information, exercising appropriate managerial control to require employee training in recognizing and thwarting social engineering attacks, and timely disclosing and patching any data security vulnerabilities. As a result of this expectation, Plaintiff Rouillard entrusted his Private Information to Defendant, and his Private Information was within the possession and control of Defendant at the time of the Data Breach.

16. Plaintiff Rouillard's Private Information was exposed in the Data Breach.

17. As a result of the Data Breach, Plaintiff Rouillard has devoted considerable time and resources to protect himself from the Data Breach, including but not limited to researching the Data Breach and monitoring his accounts for suspicious activity.

18. The substantial risk of imminent harm and loss of privacy has also caused Plaintiff to suffer stress, fear, emotional distress, and anxiety.

19. Plaintiff Rouillard has also been injured by the damages to and loss of value of his Private Information – a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when his Private Information was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

20. Given the highly sensitive nature of the information involved, the Data Breach has also caused Plaintiff Rouillard to suffer imminent harm arising from a substantially increased risk of additional fraud, identity theft, financial crimes, and misuse of his Private Information. This highly sensitive information is now in the hands of criminals as a direct and proximate result of Defendant's misconduct.

21. Had Plaintiff Rouillard been informed of Defendant's insufficient data security measures to protect his Private Information, he would not have willingly provided his Private Information to Defendant.

B. Plaintiff Kristy Munden

22. Plaintiff Kristy Munden is a resident and citizen of Los Angeles, California.

23. Plaintiff Munden entrusted her Private Information to Defendant in connection with her enrollment and participation in the SAG-AFTRA Health Plan.

24. On approximately December 2, 2024, Plaintiff Munden received a notice from Defendant stating her Private Information had been accessed by unauthorized third parties in the Data Breach.

25. Plaintiff Munden only allowed Defendant to maintain, store, and use her Private Information because she reasonably expected that Defendant would use basic security measures to protect her Private Information and prevent its access by unauthorized third parties, such as requiring passwords and multi-factor authentication to access accounts or databases storing her Private Information, exercising appropriate managerial control to require employee training in recognizing and thwarting social engineering attacks, and timely disclosing and patching any data security vulnerabilities. As a result of this expectation, Plaintiff Munden entrusted her Private Information to Defendant, and her Private Information was within the possession and control of Defendant at the time of the Data Breach.

26. Plaintiff Munden's Private Information was exposed in the Data Breach.

27. As a result of the Data Breach, Plaintiff Munden has devoted considerable time and resources to protect herself from the Data Breach, including but not limited to researching the Data Breach and monitoring her accounts for suspicious activity.

28. The substantial risk of imminent harm and loss of privacy has also caused Plaintiff to suffer stress, fear, emotional distress, and anxiety.

29. Plaintiff Munden has also been injured by the damages to and loss of value of her Private Information – a form of intangible property that Plaintiff Munden entrusted to Defendant. This information has inherent value that Plaintiff Munden

was deprived of when her Private Information was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

30. Given the highly sensitive nature of the information involved, the Data Breach has also caused Plaintiff Munden to suffer imminent harm arising from a substantially increased risk of additional fraud, identity theft, financial crimes, and misuse of her Private Information. This highly sensitive information is now in the hands of criminals as a direct and proximate result of Defendant's misconduct.

31. Had Plaintiff Munden been informed of Defendant's insufficient data security measures to protect her Private Information, she would not have willingly provided her Private Information to Defendant.

C. Plaintiff Lee Wilkof

32. Plaintiff Lee Wilkof is a resident and citizen of Gardiner, New York.

33. Plaintiff Wilkof entrusted his Private Information to Defendant in connection with his enrollment and participation in the SAG-AFTRA Health Plan.

34. On approximately December 2, 2024, Plaintiff Wilkof received a notice from Defendant stating his Private Information had been accessed by unauthorized third parties in the Data Breach.

35. Plaintiff Wilkof only allowed Defendant to maintain, store, and use his Private Information because he reasonably expected that Defendant would use basic security measures to protect his Private Information and prevent its access by unauthorized third parties, such as requiring passwords and multi-factor authentication to access accounts or databases storing his Private Information, exercising appropriate managerial control to require employee training in recognizing and thwarting social engineering attacks, and timely disclosing and patching any data security vulnerabilities. As a result of this expectation, Plaintiff Wilkof entrusted his Private Information to Defendant, and his Private Information was within the possession and control of Defendant at the time of the Data Breach.

36. Plaintiff Wilkof's Private Information was exposed in the Data Breach.

37. As a result of the Data Breach, Plaintiff Wilkof has devoted considerable time and resources to protect himself from the Data Breach, including but not limited to researching the Data Breach and monitoring his accounts for suspicious activity.

38. The substantial risk of imminent harm and loss of privacy has also caused Plaintiff Wilkof to suffer stress, fear, emotional distress, and anxiety.

39. Plaintiff Wilkof has also been injured by the damages to and loss of value of his Private Information – a form of intangible property that Plaintiff Wilkof entrusted to Defendant. This information has inherent value that Plaintiff Wilkof was deprived of when his Private Information was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

40. Given the highly sensitive nature of the information involved, the Data Breach has also caused Plaintiff Wilkof to suffer imminent harm arising from a substantially increased risk of additional fraud, identity theft, financial crimes, and misuse of his Private Information. This highly sensitive information is now in the hands of criminals as a direct and proximate result of Defendant's misconduct.

41. Had Plaintiff Wilkof been informed of Defendant's insufficient data security measures to protect his Private Information, he would not have willingly provided his Private Information to Defendant.

D. Plaintiff Steven Barr

42. Plaintiff Steven Barr is a resident and citizen of Los Angeles County, California.

43. Plaintiff Barr entrusted his Private Information to Defendant in connection with his enrollment and participation in the SAG-AFTRA Health Plan.

44. On approximately December 9, 2024, Plaintiff Barr received a notice from Defendant stating his Private Information had been accessed by unauthorized third parties in the Data Breach.

45. Plaintiff Barr only allowed Defendant to maintain, store, and use his Private Information because he reasonably expected that Defendant would use basic

security measures to protect his Private Information and prevent its access by unauthorized third parties, such as requiring passwords and multi-factor authentication to access accounts or databases storing his Private Information, exercising appropriate managerial control to require employee training in recognizing and thwarting social engineering attacks, and timely disclosing and patching any data security vulnerabilities. As a result of this expectation, Plaintiff Barr entrusted his Private Information to Defendant, and his Private Information was within the possession and control of Defendant at the time of the Data Breach.

46. Plaintiff Barr's Private Information was exposed in the Data Breach.

47. As a result of the Data Breach, Plaintiff Barr has devoted considerable time and resources to protect himself from the Data Breach, including but not limited to researching the Data Breach and monitoring his accounts for suspicious activity.

48. The substantial risk of imminent harm and loss of privacy has also caused Plaintiff Barr to suffer stress, fear, emotional distress, and anxiety.

49. Plaintiff Barr has also been injured by the damages to and loss of value of his Private Information – a form of intangible property that Plaintiff Barr entrusted to Defendant. This information has inherent value that Plaintiff Barr was deprived of when his Private Information was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

50. Given the highly sensitive nature of the information involved, the Data Breach has also caused Plaintiff Barr to suffer imminent harm arising from a substantially increased risk of additional fraud, identity theft, financial crimes, and misuse of his Private Information. This highly sensitive information is now in the hands of criminals as a direct and proximate result of Defendant's misconduct.

51. Had Plaintiff Barr been informed of Defendant's insufficient data security measures to protect his Private Information, he would not have willingly provided his Private Information to Defendant.

E. Plaintiff Massimiliano Furlan

52. Plaintiff Massimiliano Furlan is a resident and citizen of Arleta, California.

53. Plaintiff Furlan entrusted his Private Information to Defendant in connection with his enrollment and participation in the SAG-AFTRA Health Plan.

54. On approximately, December 2, 2024, Plaintiff Furlan received a notice from Defendant stating his Private Information had been accessed by unauthorized third parties in the Data Breach.

55. Plaintiff Furlan only allowed Defendant to maintain, store, and use his Private Information because he reasonably expected that Defendant would use basic security measures to protect his Private Information and prevent its access by unauthorized third parties, such as requiring passwords and multi-factor authentication to access accounts or databases storing his Private Information, exercising appropriate managerial control to require employee training in recognizing and thwarting social engineering attacks, and timely disclosing and patching any data security vulnerabilities. As a result of this expectation, Plaintiff Furlan entrusted his Private Information to Defendant, and his Private Information was within the possession and control of Defendant at the time of the Data Breach.

56. Plaintiff Furlan's Private Information was exposed in the Data Breach.

57. As a result of the Data Breach, Plaintiff Furlan has devoted considerable time and resources to protect himself from the Data Breach, including but not limited to researching the Data Breach and monitoring his accounts for suspicious activity.

58. The substantial risk of imminent harm and loss of privacy has also caused Plaintiff Furlan to suffer stress, fear, emotional distress, and anxiety.

59. Plaintiff Furlan has also been injured by the damages to and loss of value of his Private Information – a form of intangible property that Plaintiff Furlan entrusted to Defendant. This information has inherent value that Plaintiff Furlan was

deprived of when his Private Information was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

60. Given the highly sensitive nature of the information involved, the Data Breach has also caused Plaintiff Furlan to suffer imminent harm arising from a substantially increased risk of additional fraud, identity theft, financial crimes, and misuse of his Private Information. This highly sensitive information is now in the hands of criminals as a direct and proximate result of Defendant's misconduct.

61. Had Plaintiff Furlan been informed of Defendant's insufficient data security measures to protect his Private Information, he would not have willingly provided his Private Information to Defendant.

62. As a result of the Data Breach, Plaintiffs been further injured by the damages to and loss in value of their Private Information -a form of intangible property that Plaintiffs entrusted to Defendant. This information has inherent value that Plaintiffs were deprived of when their Private Information was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

63. Given the nature of the information involved and the malicious and intentional means through which the information was stolen, the Data Breach has also caused Plaintiffs to suffer imminent harm arising from a substantially increased risk of additional fraud, identity theft, financial crimes, and misuse of their Private Information. This highly sensitive information, which includes their name, Social Security number, and information associated with claims and health insurance information, is now in the hands of criminals as a direct and proximate result of Defendant's misconduct.

64. As a result of the actual harm Plaintiffs have suffered due to the Data Breach and the imminent and substantial risk of future harm, the Data Breach has forced Plaintiffs to spend significant time and energy dealing with issues related to the Data Breach, including self- monitoring their accounts to ensure no fraudulent activity has occurred, investigating fraudulent activity, alerting their banking services

about the breach, and changing identifying information and passwords for their accounts. Much of the time and energy that Plaintiffs expended, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

65. The substantial risk of imminent harm and loss of privacy has also caused Plaintiffs to suffer stress, fear, emotional distress, and anxiety.

F. Defendant SAG-AFTRA Health Plan

66. Defendant SAG-AFTRA Health Plan is a labor-management trust established under California law, with its principal place of business located in Burbank, California. Defendant conducts business, providing health benefits to eligible participants, across the nation.

III. JURISDICTION AND VENUE

67. This Court has subject matter jurisdiction of this action pursuant to 28 U.S.C. Section 1332(d) because this is a class action where the aggregate amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant. This Court has supplemental jurisdiction over any state law claims pursuant to 28 U.S.C. Section 1367. Furthermore, the affected victims of the data breach – the Class Members – reside nationwide.

68. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District: Defendant's principal place of business is located in this District from where its board of directors and/or officers direct Defendant's activities including to their actions and inactions leading to the data breach at issue; Defendant gains revenue and profits from doing business in this District; Class Members were affected by the breach from SAG Health's actions and inactions directed from this District.

IV. FACTUAL ALLEGATIONS

69. SAG Health is a provider of health and medical benefits servicing tens of thousands of SAG-AFTRA members and their families primarily in California and New York. Defendant collects and processes the personal data of its members. To avail themselves of benefits coverage, members are forced to entrust Defendant with their Private Information.

70. The information collected and stored by Defendant includes, but is not limited to, ***names, Social Security numbers, and information associated with claims and health insurance information***. Plaintiffs and other similarly situated members trusted Defendant with their sensitive and valuable Private Information.

A. The Data Breach

71. At all material times, SAG Health failed to maintain proper security measures despite its promises of safety and security to consumers.

72. On September 18, 2024, Defendant became aware that an employee's email account had been compromised; specifically, on September 16 and 17, there was unauthorized access to Defendant's internal systems. Defendant did not notify its customers then, nor made any announcements to alert of this major security issue. By October 3, 2024, Defendant concluded that members' information was likely acquired.[3] Yet again, Defendant chose not to notify the affected customers for the next several months.

73. On around December 2, 2024, Defendant finally began notifying some members of the Data Breach, including Plaintiffs, when nearly three months had passed since learning of the unauthorized access and two months had passed since Defendant concluded that personal information had likely been acquired.

74. In its December 2 statement, Defendant did not disclose how many members' Private Information was breached, leaving consumers to speculate whether

[3] *SAG-AFTRA Health Plan Email Phishing Notice*, *supra* fn 2.

it is likely that their PII/PHI has been compromised and without any clear instruction on what they can do to protect themselves now that their Private Information has been exposed. Instead, Defendant downplayed the extent of the Data Breach, and the likely harm affected victims may experience.

75. Separately and without informing Plaintiffs and the Class, Defendant notified the U.S. Department Office Health and Human Services Office of Civil Rights that 35,592 individuals had been affected by the Data Breach.[4]

76. Defendant acknowledged the risk posed to Class Members and their Private Information as a result of the Data Breach, explicitly stating that "We take this matter very seriously," encouraging members to "be on alert for any suspicious activity related to their financial accounts and credit reports" and to "regularly monitor their credit report, statements, and records to ensure that there are no transactions or other activities that were not initiated or authorized by them."

B. Data Breaches and the Market for PII/PHI

77. When a victim's data is compromised in a breach, the victim is exposed to serious ramifications regardless of the sensitivity of the data—including but not limited to identity theft, fraud, decline in credit, inability to access healthcare, as well as legal consequences.[5] These harms are amplified where, as here, the compromised data is particularly sensitive.

78. The U.S. Department of Justice's Bureau of Justice Statistics has found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that resolution of those problems

[4] The State Journal Register, https://data.sj-r.com/health-care-data-breaches/sag-aftra-health-plan-ca-35592-20241202-hacking-email/ (last accessed July 31, 2025).

[5] Identity Theft Resource Center, 2017 Annual Data Breach Year-End Review, https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_ V2_combinedWEB.pdf (last accessed July 31, 2025).

could take more than a year.[6]

79. The U.S. Government Accountability Office (GAO) has concluded that it is common for data thieves to hold onto stolen data for extended periods of time before utilizing it for identity theft.[7] In the same report, the GAO noted that while credit monitoring services can assist with detecting fraud, those services do not stop it.[8]

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

81. PII is a valuable commodity for which a black market exists on the dark web, among other places. Personal data can be worth from $1,000-$1,200 on the dark web and the legitimate data brokerage industry is valued at more than $250 billion.[9, 10]

82. In fact, "[a] stolen Social Security number is one of the leading causes of

[6] U.S. Department of Justice, Bureau of Justice Statistics, Victims of Identity Theft, 2014 (Sept. 2015), http://www.bjs.gov/content/pub/pdf/vit14.pdf (last accessed July 31, 2025).

[7] U.S. Government Accountability Office Report to Congressional Requesters, Data Breaches – Range of Consumer Risks Highlights Limitations of Identity Theft Services, https://www.gao.gov/assets/700/697985.pdf (last accessed July 31, 2025).

[8] *Id.*

[9] Ryan Smith, *Revealed-how much is personal data worth on the dark web?*, INSURANCE BUSINESS MAGAZINE, https://www.insurancebusinessmag.com/ca/news/cyber/revealed--how-much-is-personal-data-worth-on-the-dark-web-444455.aspx (last accessed July 31, 2025).

[10] Maria LaMagna, *The sad truth about how much your Google data is worth on the dark web*, MARKETWATCH (last accessed July 31, 2025). 17 Emily Wilson, The Worrying Trend of Children's Data Being Sold on the Dark Web, TNW (February 23, 2019), https://thenextweb.com/contributors/2019/02/23/children-data-sold-the-dark- web/ (last accessed July 31, 2025).

identity theft and can threaten your financial health."[11] "Someone who has your SSN can use it to impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits."[12]

83. Medical data is even more valuable because unlike other personal information, such as credit card numbers which can be quickly changed, medical data is static. This is why companies possessing medical information, like Defendant, are targeted by cyber-criminals.[13]

84. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information (*e.g.,* patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PHI/PII is a valuable commodity for which a "cyber black market" exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites. Unsurprisingly, the healthcare industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

85. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions

---

[11] *How to Protect Yourself from Social Security Number Identity* Theft, EQUIFAX https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/ (last accessed July 31, 2025).

[12] *What Is an SSN? What to Know About Social Security Numbers*, INVESTOPEDIA https://www.investopedia.com/terms/s/ssn.asp (last accessed July 31, 2025).

[13] Caroline Humer & Jim Finkle, *Your medical record is worth more to hackers than your credit card*, REUTERS (September 24, 2014), https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924 (last accessed July 31, 2025).

and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[14]

86. A 2021 report by Invisibly, a team of application developers focused on reclaiming users' data, found that personal medical information is one of the most valuable pieces of information within the market for data. The report noted that "[i]t's worth acknowledging that because health care records often feature a more complete collection of the PII User's identity, background, and personal identifying information (PII), health care records have proven to be of particular value for data thieves." While a single SSN might go for $0.53, a complete health care record sells for $250 on average.[15]

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

[14] Michael Ollove, The Rise of Medical Identity Theft in Healthcare, Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/

[15] *How Much is Your Data Worth? The Complete Breakdown for 2024*, INVISIBLY (July 13, 2021) https://www.invisibly.com/learn-blog/how-much-is-data-worth/ (last accessed July 31, 2025).

87. Medical records are even worth more than an SSN, credit card, and driver's license combined, according to federal officials. They estimate that medical records can go for anywhere between $250 to $1,000.[16]

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

89. PII has a distinct, high value—which is why legitimate companies and criminals seek to obtain and sell it.

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

91. A study done by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that most victims of medical identity theft were forced to pay out of pocket costs for healthcare they did not receive to restore coverage.[17] Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.

92. It should be no surprise that in today's digital economy the "world's most

[16] Wilkinson, Kate. *RI hospitals fight cyberattacks on 'almost a daily basis',* WPRI (Oct. 10, 2023), https://www.wpri.com/target-12/ri-hospitals-fight-cyberattacks-on-almost-a-daily-basis/ (last accessed July 31, 2025).

[17] *See* Elinor Mills, Study: *Medical Identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last accessed July 31, 2025).

valuable resource is no longer oil, but data."[18] As such, personal information is a valuable property right.[19] Its value is axiomatic, considering the value of "big data" in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that personal information has considerable market value.

93. In a consumer-driven world, the ability to capture and use consumer data to shape products, solutions, and the buying experience is critically important to a business's success. Research shows that organizations who "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[20]

94. Indeed, an entire economy exists related to the value of personal data. In 2022, the big data technology market was valued at roughly $309 billion, and that value is expected to grow to $842 billion by 2023.[21]

95. In 2013, the Organization for Economic Cooperation and Development ("OECD") even published a paper entitled "Exploring the Economics of Personal

---

[18] *The world's most valuable resource is no longer oil, but data*, The Economist (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longeroil-but-data.

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

[20] Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing value from your customer data*, McKinsey (Mar. 15, 2017), https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data.

[21] Big Data Technology Market Research Report, Fortune Business Insights (Sept. 2023), https://www.fortunebusinessinsights.com/industry-reports/big-data-technology-market-100144

Data: A Survey of Methodologies for Measuring Monetary Value."[22] In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."[23] OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e. $2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military [record] is estimated to cost USD 55."[24]

96. Defendant knew or should have known that Plaintiffs' and Class Members' Private Information is valuable, both to legitimate entities, like Defendant, and to cybercriminals.

97. Defendant knew or should have known that Plaintiffs and Class Members would reasonably rely upon and trust Defendant's promises regarding security and safety of their data and systems, and that their valuable Private Information would be protected.

98. By collecting, using, selling, monitoring, and trafficking Plaintiffs' and other members' Private Information, and failing to protect it by maintaining inadequate security systems, failing to properly archive the Private Information, allowing access of third parties, and failing to implement security measures, Defendant caused harm to Plaintiffs and other SAG Health plan members.

C. The Sensitivity of Members' Private Information Demands Heightened Protection

99. Entities in the healthcare industry are popular targets for cyberattacks and require top-tier security measures to protect PII/PHI, especially given that these

[22] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013), https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf.
[23] *Id.* at 25.
[24] *Id.*

databases store sensitive patient records.

100. Ponemon Institute, an expert in the annual state of cybersecurity, indicated in 2020 that organizations storing PHI were top targets for cyber-attacks. In fact, Defendant has been on notice for years that PHI is a prime target for scammers due to the amount and value of confidential patient information maintained. In 2019 alone, numerous entities in the healthcare sector suffered high-profile data breaches, including Quest Diagnostics and LabCorp.

101. In a survey released by Ponemon Institute in January 2023, nearly half of respondents (47%) said their organizations experienced a ransomware attack in the past two years, up from 43% in 2021. And 45% of respondents reported complications from medical procedures due to ransomware attacks, up from 36% in 2021.[25]

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

103. Data breaches of this caliber can result in the exposure of extremely sensitive information about adults and children's medical histories, medical conditions, psychological assessments, psychiatric evaluations, location of employers, schools, residences, and much more, which poses great dangers on its own – and more importantly poses a great danger not only to SAG members but their minor dependents. The FBI has warned that "widespread collection of student data could

[25] Southwick, Ron. *California medical group discloses ransomware attack, more than 3 million affected*, CHIEF HEALTHCARE EXECUTIVE (10 May 2023), https://www.chiefhealthcareexecutive.com/view/california-medical-group-discloses-ransomware-attack-more-than-3-million-affected (last accessed July 31, 2025).

have privacy and safety implications if compromised or exploited."[26] Defendant manages health benefit coverage for its members and their dependents; its failure to safeguard Private Information puts its members' children at risk.

104. Due to these risks, it is imperative for entities like Defendant to routinely: (a) monitor for system breaches, cyberattacks and other exploitations; (b) update their software, security procedures, and firewalls; and (c) make sure its employees are adequately trained to recognize and thwart social engineering attacks, such as phishing.

D. Defendant's Duty to Safeguard Private Information

105. Defendant is responsible for safeguarding the Private Information of tens of thousands of its members, including PII/PHI of those members' families.

106. Defendant collects, receives, and accesses members' extensive individually identifiable information. This Private Information includes names and Social Security numbers, as well as PHI in the form of health insurance information.

107. Defendant was prohibited by the Federal Trade Commission Act (the "**FTC Act**") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "**FTC**") has concluded that an entity's failure to maintain reasonable and appropriate data security for individuals' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

108. The FTC has brought enforcement actions against entities engaged in commerce for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section

[26] Education Technologies: *Data Collection and Unsecured Systems Could Pose Risks to Children*, FBI Alert No. I-091318-PSA (Sept. 13, 2018), https://www.ic3.gov/media/2018/180913.aspx (last accessed July 31, 2025).

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

109. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all decision-making.[27]

110. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[28] The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

111. The FTC further recommends that entities not maintain PII/PHI longer than needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[29]

112. Furthermore, FTC requires that entities like Defendant conduct risk assessments, implement and periodically review access control, encrypt customer

---

[27] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed July 31, 2025).

[28] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136-protecting-personal-information.pdf (last accessed July 31, 2025).

[29] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed July 31, 2025).

information, implement multi-factor authentication for **anyone accessing customer information within their systems**, dispose of customer information securely, maintain a log of authorized users' activity and keep an eye out of unauthorized access, **train employees regarding security awareness**, conduct audits, penetration testing, and system wide scans regularly to test for publicly known security vulnerabilities – all of which if had been properly implemented would have allowed Defendant to prevent this Data Breach.

113. Defendant failed to properly implement basic data security practices, allowing for this social engineering attack to occur, victimizing thousands of people – by failing to adhere to many of the FTC protocols and allowing access to a hacker impersonating an employee. Defendant should have a multifaceted security protocol in place, including a program that adequately trains employees on recognizing and thwarting phishing and social engineering attacks, monitoring out-of-network emails, segmenting the network, flagging suspicious domain addresses or content, utilized multifactor authentication before allowing access to highly sensitive information, mandating strict compliance with these protocols; mandating regular archiving of email data/removal of sensitive data from emails to servers; avoiding exchanging any sensitive data for patients/members over the emails, simulating social engineering attempts to ensure compliance, increasing spam filtering via email gateways, implementing strict policies regarding exchange of PII/PHI over emails, implementing and enforcing appropriate credential/key procedures including finger print recognition/physical key authentication; monitoring systems 24/7 for any suspicious activity, encrypting data over the email exchanges. Had Defendant maintained these and other proper protocols and regularly conducted audits to ensure its vulnerabilities and training, it would have prevented this Data Breach.

114. Moreover, as a HIPAA covered business associate, Defendant is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health

Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

115. These rules establish national standards for the protection of patient information, including protected health information ("PHI"), defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

116. Plaintiffs and Class Members provided their Private Information to SAG Health with the reasonable expectation and mutual understanding that SAG Health would comply with its obligations to keep such information confidential and secure from unauthorized access.

117. SAG Health's failure to provide adequate security measures to safeguard members' Private Information is especially egregious because it operates in a field which has recently been a frequent target of scammers attempting to gain access to confidential PII/PHI, and it had been targeted by an unauthorized individual before.[30] SAG Health should have been on notice that it was an attractive target for cybercriminals in 2019, when it detected unauthorized access on its systems that led to a threat actor using members' financial information to make unauthorized purchases.[31]

E. Impact of the Data Breach on Consumers

118. Plaintiffs and the Class have suffered actual harm as a result of Defendant's conduct. Defendant failed to institute adequate security measures that led to a data breach. This breach allowed hackers to access the Private Information,

[30] *FAQs for Data Privacy Event* (2019), AFTRA Retirement Fund, available at https://aftraretirement.org/Home/FAQs/faqs-for-data-privacy-event (last accessed July 31, 2025)

[31] *Id.*

including ***names, Social Security numbers, and health insurance information,*** of Plaintiffs and the Class. Now that the Private Information has been accessed and absconded with, it is available for criminal elements to sell or trade and will continue to be at risk for the indefinite future. In fact, the U.S. Government Accountability Office found that, "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[32]

119. Plaintiffs and Class Members are now vulnerable to a full gamut of cybercrimes, loss in value of their property, and have been forced to take remedial action, as listed below:

Digital Phishing Scams

120. Phishing scammers use emails and text messages to trick people into giving them their personal information, including but not limited to passwords, account numbers, and social security numbers. Phishing scams are frequently successful, and the FBI reported that people lost approximately $57 million to such scams in 2019 alone.[33]

121. Defendant knew or should have known of the dangers of digital phishing scams. When Personal Information is employed in a social engineering scheme, criminals can gain unfettered access to individuals, or corporate databases, as the Data Breach itself evinces.

122. Defendant's members are now more likely to become victims of digital phishing attacks because of the compromised information.

SIM-Swap

123. The data leak can also lead to SIM-swap attacks against the Class. A SIM-swap attack occurs when the scammers trick a telephone carrier to porting the victim's

[32] *See* U.S. GOV'T ACCOUNTABILITY OFF. REPORT TO CONGRESSIONAL REQUESTERS 29 2007. https://www.gao.gov/new.items/d07737.pdf. (last accessed July 31, 2025).

[33] *See How to Recognize and Avoid Phishing Scams*, FTC Consumer Advice, https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams (Last accessed July 31, 2025).

phone number to the scammer's SIM card. By doing so, the attacker is able to bypass two-factor authentication accounts, as are used to access cryptocurrency wallets and other important accounts. The type of personal information that has been leaked poses a profound tangible risk of SIM-swap attacks for the Class.

124. Defendant's members are now more likely to become victims of SIM Swap attacks because of the released personal information.

Loss of Time

125. As a result of this breach, Plaintiffs and impacted consumers will suffer unauthorized email solicitations, and experience a significant increase in suspicious phishing scam activity via email, phone calls, text messages, all following the breach. In addition, Plaintiffs, as a result of the breach, have spent significant time and effort researching the breach, monitoring their accounts for fraudulent activity, reviewing unsolicited emails, texts, and answering telephone calls.

Threat of Identity Theft

126. As a direct and proximate result of Defendant's breach of confidence, and failure to protect Private Information, Plaintiffs and the Class have also been injured by facing ongoing, imminent, impending threats of identity theft crimes, fraud, scams, and other misuse of this Private Information, resulting in ongoing monetary loss and economic harm, loss of value of privacy and confidentiality of the stolen Private Information, illegal sales of the compromised Private Information on the black market, mitigation expenses and time spent on credit monitoring, identity theft insurance, credit freezes/unfreezes, expenses and time spent in initiating fraud alerts, contacting third parties; decreased credit scores, lost work time, and other injuries. Defendant, through its misconduct, has enabled numerous bad actors to sell and profit off of Private Information that belongs to Plaintiffs.

Out of Pocket Costs

127. Plaintiffs are now forced to research and subsequently acquire credit monitoring and reasonable identity theft defensive services and maintain these

services to avoid further impact. Plaintiffs anticipate spending out of pocket expenses to pay for these services.

128. Upon information and belief, Defendant also used Plaintiffs' Private Information for profit and continued to use Plaintiffs' Private Information to target Plaintiffs and share their information with various third parties for Defendant's own benefit.

Diminution in Value of a Valuable Property Right

129. Because personal data is valuable personal property, market exchanges now exist where internet users like Plaintiffs and Class Members can sell or monetize their own personal data.

130. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to legitimate marketers or app developers.[34] For example, consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[35]

131. Accordingly, as a result of the Data Breach, Plaintiffs lost the sale value of their Private Information and the opportunity to control how it is used. That a threat actor specifically targeted Defendant demonstrates just how valuable Plaintiffs' Private Information can be to hackers and the significant value of Plaintiffs' Private Information to cybercriminals.

Summary of Actual Economic and Noneconomic Damages

132. In sum, Plaintiffs and similarly situated consumers were injured as follows:

a) Theft of their Private Information and the resulting loss of privacy

[34] *See, e.g.*, *The Personal Data Revolution*, DATACOUP, https://datacoup.com/

[35] Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last accessed July 31, 2025).

rights in that information;

b) Improper disclosure of their Private Information;

c) Loss of value of their Private Information;

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

e) Defendant's retention of profits attributable to Plaintiffs' and other customers' Private Information that Defendant failed to adequately protect;

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

g) Ascertainable out-of-pocket expenses and the value of Plaintiffs' time allocated to fixing or mitigating the effects of this data breach;

h) Overpayments for Defendant's products and/or services which Plaintiffs paid to enroll in;

i) Emotional distress, and fear associated with the imminent threat of harm from the continued phishing scams and attacks as a result of this data breach.

F. Defendant Should Have Invested in Appropriate & Necessary Data Security

133. In the years immediately preceding the Data Breach, Defendant knew or should have known that its computer systems were a target for cybersecurity attacks.

134. The Data Breach was reasonably foreseeable to SAG Health give its close administrative relationship with the AFTRA Retirement Fund ("AFTRA Fund"), which experienced its own data breach in October 2019. Indeed, SAG-Health and the AFTRA-Fund share multiple board trustees, including J. Keith Gorham, Marc

Sandman, and David White.[36]

135. Like the September 2024 Data Breah SAG-Health experienced, the AFTRA Fund breach compromised names, Social Security numbers, addresses, and dates of birth through unauthorized network access that went undetected for several days.[37] And much like SAG Health, despite discovering the breach in October 2019, the AFTRA Fund did not notify retirement fund participants until December 2020—over a year later.[38]

136. With shared governance and direct knowledge of the AFTRA Fund's security failures through common trustees, SAG Health was uniquely positioned to implement appropriate measures to prevent the Data Breach. Moreover, given that SAG Health stores identical types of sensitive data as the AFTRA Fund, it had every reason to prioritize cybersecurity improvements after witnessing the AFTRA Fund's breach and its consequences.

137. But even without such knowledge, SAG Health had reason to foresee the threats posed by email phishing attacks. The FBI and CISA have issued numerous warnings about email phishing attacks targeting healthcare and benefits organizations, with industry standards recognizing email security as a critical vulnerability requiring employee training, multi-factor authentication, and access controls. Yet SAG Health still suffered a breach through a compromised employee email credential—the most basic and preventable attack vector—demonstrating a shocking failure to implement fundamental safeguards that any reasonable healthcare entity would have adopted, especially after seeing a sister organization fall victim to

---

[36] SAG-AFTRA, *Notice of Data Breach Affecting Pension/Retirement Participants*, https://www.sagaftra.org/notice-data-breach-affecting-pensionretirement-participants (last accessed July 31, 2025).

[37] *Compare* SOLIDARITY.US, https://solidarity.us/sag-aftra-health-plan-trustees (last accessed July 31, 2025), *with* SOLIDARITY.US, https://solidarity.us/aftra-retirement-fund-trustees (last accessed July 31, 2025).

[38] *See supra* note 8.

cybercriminals.

138. The FBI, FTC, GAO, U.S. Secret Service, United States Cybersecurity and Infrastructure Security Agency, State Attorney General Offices and many other government and law enforcement agencies, and hundreds of private cybersecurity and threat intelligence firms, have issued warnings that put Defendant on notice, long before the Data Breach, that (1) cybercriminals were targeting companies who store personal health information, such as Defendant; (2) cybercriminals were ferociously aggressive in their pursuit of large collections of Private Information like that in possession of Defendant; (3) cybercriminals were selling large volumes of Private Information and corporate information on Dark Web portals; and (4) the threats were increasing.

139. Had Defendant been diligent and responsible, it would have known about and acted upon warnings published in 2017 that 93% of data security breaches were avoidable and the key avoidable causes for data security incidents are:

- Lack of a complete risk assessment, including internal, third-party, and cloud-based systems and services;
- Not promptly patching known/public vulnerabilities, and not having a way to process vulnerability reports;
- Misconfigured devices/servers;
- Unencrypted data and/or poor encryption key management and safeguarding;
- Use of end-of-life (and thereby unsupported) devices, operating systems, and applications;
- Employee errors and accidental disclosures — lost data, files, drives, devices, computers, improper disposal;
- Failure to block malicious email; and
- **Users succumbing to business email compromise (BEC) and social exploits.**[39]

140. In light of the information and warnings readily available to Defendant before the Data Breach, Defendant had reason to be on guard and to increase data

[39] Gretel Egan, *OTA Report Indicates 93% of Security Breaches Are Preventable*, PROOFPOINT (Feb. 7, 2018), available at https://www.proofpoint.com/us/security-awareness/post/ota-report-indicates-93-security-breaches-are-preventable (last accessed July 31, 2025).

security to avoid an attack.

141. Further, Defendant suffered a data breach in 2019, yet did not employ sufficient remedial measures to prevent additional breaches in the future.

142. Prior to the Data Breach, Defendant thus knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' Private Information could be accessed, exfiltrated and utilized by nefarious individuals as the result of a cyberattack.

143. Prior to the Data Breach, Defendant knew or should have known that it should ensure its employees with access to the Private Information are adequately trained in recognizing and thwarting social engineering attacks, such as the phishing attack which led to the Data Breach.

144. Data security experts advise that "the vast majority of data breaches are preventable" if companies follow widely-available advice on data security practices, including "continually audit[ing] and reevaluat[ing]" their data security practices; being aware of and working proactively to counter cybercriminals' evolving techniques and approaches; and training and re-training their employees.[40]

145. Defendant did not follow this advice; nor did it otherwise remedy the inadequacies that it knew led to the first breach of its systems. On its own website, Defendant provides the link to Online Security Tips posted by the U.S. Department of Labor, including the requirement to use strong and unique password, avoid using repat passwords, changing passwords frequently, using Multi-factor authentication, keeping personal contact information current, deleting/closing unused accounts, avoiding Wi-Fi networks, being vigilant of phishing attacks, avoiding clicking links/providing information to unverified entities even if they appear to look like

[40] Nate Nead, *How To Prevent A Data Breach In Your Company*, FORBES BUSINESS COUNSEL, FORBES (Jul. 30, 2021) available at https://www.forbes.com/sites/forbesbusinesscouncil/2021/07/30/how-to-prevent-a-data-breach-in-your-company/?sh=3828f7b918da (last accessed July 31, 2025).

trusted organizations, and other similar tips. Had Defendant enforced strict compliance with these tips, this Data Breach would have been preventable.

V. CLASS ALLEGATIONS

146. Plaintiffs bring this case individually and, pursuant to Rule 23(b)(2), (b)(3), and (c)(4) of the Federal Rules of Civil Procedure, on behalf of the following Nationwide Class and State Classes (collectively the "Class"):

> **Nationwide Class**
>
> "All persons whose Private Information was accessed, compromised, or stolen in the Data Breach announced by Defendant on December 2, 2024" (the "Class").
>
> **California Subclass**
>
> "All persons who currently reside in California and whose Private Information was accessed, compromised, or stolen in the data breach announced by Defendant on December 2, 2024" (the "California Subclass").

147. Excluded from the Class is Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

148. Plaintiffs reserve the right to modify or amend the definition of the proposed Class, if necessary, before this Court determines whether certification is appropriate.

149. **Numerosity:** The Class is comprised of tens of thousands of SAG-AFTRA Health Plan members throughout the United States and the state of California (the "Class Members"). The Class is so numerous that joinder of all members is impracticable and the disposition of their claims in a class action will benefit the parties and the Court.

150. **Predominance of Common Questions:** Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

a. Whether Defendant's conduct is in violation of Business and Professions Code section 17200, *et seq*.;

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

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

d. Whether Defendant's conduct is in violation of California Civil Code §§ 1798.100, *et. seq.*;

e. Whether Defendant's failure to implement effective security measures to protect Plaintiffs' and the Class's Private Information was negligent;

f. Whether Defendant owed a duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

g. Whether Defendant breached a duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

h. Whether Class Members' Private Information was accessed, compromised, or stolen in the Data Breach;

i. Whether Defendant's conduct caused or resulted in damages to Plaintiffs and the Class;

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

k. Whether Defendant knew or should have known that its systems, including but not limited to training protocols and policies, left it vulnerable to a data breach;

l. Whether Defendant adequately addressed the vulnerabilities that allowed for the Data Breach; and

m. Whether, as a result of Defendant's conduct, Plaintiffs and the Class are entitled to damages and relief.

151. **Typicality:** Plaintiffs' claims are typical of the claims of the proposed Class, as Plaintiffs and Class Members were harmed by Defendant's uniform unlawful conduct.

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

153. The Class is identifiable and readily ascertainable. Notice can be provided to such purchasers using techniques and a form of notice similar to those customarily used in class actions, and by internet publication, radio, newspapers, and magazines.

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

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

156. Defendant has acted on grounds generally applicable to the entire Class, thereby making final injunctive relief and/or corresponding declaratory relief

appropriate with respect to the Class as a whole. The prosecution of separate actions by individual Class Members would create the risk of inconsistent or varying adjudications with respect to individual member of the Class that would establish incompatible standards of conduct for Defendant.

157. Absent a class action, Defendant will likely retain the benefits of its wrongdoing. Because of the small size of the individual Class Members' claims, few, if any, Class Members could afford to seek legal redress for the wrongs complained of herein. Absent a representative action, Class Members will continue to suffer losses and Defendant (and similarly situated companies) will be allowed to continue these violations of law and to retain the proceeds of its ill-gotten gains.

COUNT ONE

VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW

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

(By All Plaintiffs on Behalf Nationwide Class)

158. Plaintiffs, individually and on behalf of the Class, herein repeat, reallege and fully incorporate all allegations in all preceding paragraphs.

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

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

161. Defendant has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), the FTC Act, 15 U.S.C. § 45, California's Confidentiality of Medical Information Act, Cal. Civ. Code § 56, California's Consumer Privacy Act, Cal. Civ. Code § 1798.100, and California common law.

162. Plaintiffs' harm and injuries alleged herein was the direct and proximate result of Defendant's unlawful and wrongful conduct, all of which occurred within the State of California.

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

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

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

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

167. Plaintiffs and the Class have suffered injury-in-fact and have lost money or property as a result of Defendant's unfair conduct. Plaintiffs and the Class would not have given Defendant their Private Information, had they known that their Private Information was vulnerable to a data breach. Additionally, SAG Health members paid money, directly or indirectly to SAH Health in return for membership benefits. Defendant should have applied a portion of that money to data security but instead directed it to its own profit. Likewise, Plaintiffs and Class Members seek an order mandating that Defendant implement adequate security practices to protect members' Private Information. Additionally, Plaintiffs and the members of the Class seek and request an order awarding Plaintiffs and the Class restitution of the money wrongfully acquired by Defendant by means of Defendant's unfair and unlawful practices.

168. **Injunction.** Pursuant to Business and Professions Code Sections 17203, Plaintiffs and the Class seek an order of this Court compelling Defendant to implement adequate safeguards to protect consumer Private Information retained by Defendant. This includes, but is not limited to: improving security systems, deleting

data that no longer needs to be retained by Defendant, archiving that data on secure servers, adopting adequate and robust training policies and protocols for all employees entrusted with access to Personal Information and notifying all affected consumers in a timely manner.

169. No adequate remedy at law. Plaintiffs and the Class are entitled to equitable relief as no adequate remedy at law exist because:

a) Defendant has not yet implemented adequate protections to prevent a future data breach, nor has it given an adequate notice to all affected class members, and therefore, the equitable relief requested here would prevent ongoing and future harm;

b) The equitable relief under the UCL (and also under unjust enrichment discussed below) creates a straightforward cause of action for violations of law (such as statutory or regulatory requirements related to representations and omissions made with respect to Defendant's services). Furthermore, damages for non-UCL claims require additional elements or pre-suit notice letters, which would potentially eliminate possibility of providing damages to the entire class, while restitution would provide certainty and remedy for all affected victims.

c) In addition, discovery—which has not yet been provided and/or completed—may reveal that the claims providing legal remedies are inadequate. At this time, forcing an election of remedies at the initial pleadings stage, in the absence of completed discovery regarding class certification and merits, is premature and likely to lead to subsequent, potentially belated, and hotly contested motions to amend the pleadings to add equitable remedies based on a lengthy historical recount of discovery and analysis of voluminous exhibits, transcripts, discovery responses, document productions, etc., as well as related motions to seal confidential information contained therein.

COUNT TWO

NEGLIGENCE

(By All Plaintiffs on Behalf of the Nationwide Class)

170. Plaintiffs, individually and on behalf of the Class, herein repeat, reallege and fully incorporate all allegations in all preceding paragraphs.

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

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

173. Defendant had a special relationship with Plaintiffs and Class Members, which is recognized by laws and regulations, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to class members from a data breach. Plaintiffs and Class Members were compelled to entrust Defendant with their PII/PHI. At relevant times, Plaintiffs and Class members understood that Defendant would take adequate security precautions to safeguard that information. Only Defendant had the ability to protect Plaintiffs' and Class Members' PII/PHI stored on its servers.

174. Defendant knew or should have known that Plaintiffs' and the Class Members' Private Information is information that is frequently sought after by criminals.

175. Defendant knew or should have known that Plaintiffs and the Class members would suffer harm if their Private Information was leaked.

176. Defendant knew or should have known that its security systems were not adequate to protect Plaintiffs' and the Class Members' Private Information from a data breach.

177. Defendant knew or should have known that adequate and prompt notice of the data breach was required such that Plaintiffs and the Class could have taken more swift and effective action to change or otherwise protect their Private Information. Defendant failed to provide timely notice upon discovery of the data breach. Some Class Members were informed of the data breach on December 2, 2024. Defendant had learned of the data breach more than two months prior, in September 2024, and learned that consumers' PII was compromised over a month prior, in October 2024.

178. Defendant's conduct as described above constituted an unlawful breach of its duty to exercise due care in collecting, storing, and safeguarding Plaintiffs' and the Class Members' Private Information by failing to design, implement, and maintain adequate security measures to protect this information. Moreover, Defendant did not implement, design, or maintain adequate measures to detect a data breach when it occurred.

179. Defendant's conduct as described above constituted an unlawful breach of its duty to provide adequate and prompt notice of the data breach.

180. Plaintiffs' and the Class Members' Private Information would have remained private and secure had it not been for Defendant's wrongful and negligent breach of its duties. The leak of Plaintiffs' and the Class Members' Private Information, and all subsequent damages, was a direct and proximate result of Defendant's negligence.

181. Defendant's negligence was, at least, a substantial factor in causing Plaintiffs' and the Class's Private Information to be improperly accessed, disclosed,

and otherwise compromised, and in causing Class Members' other injuries arising out of the Data Breach.

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

183. Defendant's negligence directly caused significant harm to Plaintiffs and the Class.

COUNT THREE

INVASION OF PRIVACY

(By All Plaintiffs on Behalf of the Nationwide Class)

184. Plaintiffs, individually and on behalf of the Class, herein repeat, reallege and fully incorporate all allegations in all preceding paragraphs.

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

186. Defendant owed a duty to Plaintiffs and Class Members to keep their Private Information confidential.

187. Defendant failed to protect, and released to unknown and unauthorized third parties, the Private Information of Plaintiffs and Class Members.

188. By failing to keep Plaintiffs' and Class Members' Private Information safe, knowingly utilizing unsecure systems and practices, Defendant unlawfully invaded Plaintiffs' and Class Members' privacy by, among others, (i) intruding into Plaintiffs' and Class Members' private affairs in a manner that would be highly offensive to a reasonable person; (ii) failing to adequately secure their Private Information from disclosure to unauthorized persons and/or third parties; and (iii)

enabling the disclosure of Plaintiffs' and Class Members' Private Information without consent.

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

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

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

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

COUNT FOUR

VIOLATION OF CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CALIFORNIA CIVIL CODE SECTION 56, *et seq.*

(By Plaintiffs Munden, Barr, and Furlan, on Behalf of the California Subclass)

193. Plaintiffs Munden, Barr, and Furlan (together, "California Plaintiffs"), individually and on behalf of the California Subclass, herein repeat, reallege and fully incorporate all allegations in all preceding paragraphs.

194. Defendant is subject to the requirements and mandates of the CMIA because it is a "health care service plan" pursuant to Cal. Civ. Code § 56.10.

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

196. As a direct result of its negligent failure to adequately protect the data it collected from the California Plaintiffs and California Subclass Members, Defendant allowed for a Data Breach which released the PII/PHI of Plaintiffs and the Class Members to criminals and/or third parties.

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

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

199. Defendant is in possession of affected individuals' medical insurance and claim information, including, but not necessarily limited to, diagnosis and treatment of patients/customers, laboratory test results, prescription data, radiology reports, and health plan member numbers, with which more data can be ascertained. Further, the compromised data was individually identifiable because it was accompanied by elements sufficient to allow identification of California Plaintiffs by the third parties to whom the data was disclosed. California Subclass Members' names were included in the compromised data.

200. Defendant came into possession of California Plaintiffs' and California Subclass Members' medical information and had a duty pursuant to Section 56.06

and 56.101 of the CMIA to maintain, store and dispose of the California Plaintiffs' and California Subclass Members' medical records in a manner that preserved their confidentiality. Sections 56.06 and 56.101 of the CMIA prohibit the negligent creation, maintenance, preservation, store, abandonment, destruction, or disposal of confidential medical information.

201. Defendant further violated the CMIA by failing to use reasonable care, and in fact, negligently maintained California Plaintiffs' and California Subclass Members' medical information, allowing and enabling a threat actor to view and access unencrypted PHI for California Plaintiffs and the California Subclass. California Plaintiffs' PHI has been misused as a result of Defendant's failure to maintain reasonable security measures and care.

202. Since Defendant maintained California Plaintiffs' and California Subclass Members' medical information in California, on California-based servers, where it was ultimately disclosed to third parties, CMIA equally applies to the entire affected Class. *See, e.g.*, *Doe v. Meta Platforms, Inc.*, No. 22-cv-03580-WHO, 2023 U.S. Dist. LEXIS 158683, at *16 (N.D. Cal. Sep. 7, 2023) (holding that another statute, CIPA, could apply to non-residents of California, because the conduct at issue occurred in California).

203. As a direct and proximate result of Defendant's violations of the CMIA, California Plaintiffs and California Subclass Members have been injured and are entitled to compensatory damages, punitive damages, and nominal damages of one-thousand dollars ($1,000) for each of Defendant's violations of the CMIA, as well as attorneys' fees and costs pursuant to Cal. Civ. Code § 56.36.

COUNT FIVE

VIOLATIONS OF CALIFORNIA'S CONSUMER PRIVACY ACT, CALIFORNIRA CIVIL CODE §§ 1798.100, *et. seq.*

(By Plaintiffs Munden, Barr, and Furlan, on Behalf of the California Subclass)

204. California Plaintiffs, individually and on behalf of the California

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

205. Defendant violated California Civil Code § 1798.150 of California's Consumer Privacy Act ("CCPA") by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted PII of Plaintiffs and the Class. As a direct and proximate result, California Plaintiffs' and California Subclass Members' unencrypted and unredacted PII was subject to unauthorized access and theft.

206. Defendant is a "business" under the meaning of California Civil Code § 1798.140 because Defendant is a "corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners" that "collects consumers' personal information" and is active "in the State of California" and "had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year." Civil Code § 1798.140(d).

207. California Plaintiffs seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards Private Information by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold PII belonging to California Plaintiffs and California Subclass. California Plaintiffs and the California Subclass have an ongoing interest in ensuring that their PII is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

208. On December 13, 2024, Plaintiff Furlan mailed a CCPA notice letter to Defendant's principal place of business pursuant to California Civil Code § 1798.150(b), detailing the specific provisions of the CCPA that Defendant has violated and continues to violate. Defendant has not provided Plaintiff Furlan with an express written statement that the violations have been cured and that no further violations shall occur. Accordingly, seeks all damages and appropriate equitable relief available under the CCPA on behalf of himself and the California Subclass members.

209. On December 10, 2024, Plaintiff Barr mailed a CCPA notice letter to Defendant's principal place of business pursuant to California Civil Code § 1798.150(b), detailing the specific provisions of the CCPA that Defendant has violated and continues to violate. Defendant has not provided Plaintiff Barr with an express written statement that the violations have been cured and that no further violations shall occur. Accordingly, Plaintiff Barr seeks all damages and appropriate equitable relief available under the CCPA on behalf of himself and the California Subclass members.

210. On July 31, 2025, Plaintiff Munden mailed a CCPA notice letter to Defendant's registered service agents Pursuant to California Civil Code § 1798.150(b), detailing the specific provisions of the CCPA that Defendant has violated and continues to violate. If Defendant does not provide express written statement within 30 days that its CCPA violations have been cured and that no further violations shall occur, Plaintiff Munden will amend her CCPA claim to seek statutory damages under the CCPA. At this time, California Plaintiff Munden only seeks actual pecuniary damages for Defendant's violations of the CCPA.

PRAYER FOR RELIEF

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

1. That the Court determines that this Action may be maintained as a Class Action, that Plaintiffs be named as Class Representatives of the Class, that the undersigned be named as Class Counsel of the Class, and that notice of this Action be given to Class Members;
2. That the Court enter an order declaring that Defendant's actions, as set forth in this Complaint, violate the laws set forth above;
3. An order:
    a) Prohibiting Defendant from engaging in the wrongful acts stated herein (including Defendant's utter failure to provide

notice to all affected consumers);

b) Requiring Defendant to implement adequate security protocols and practices to protect consumers' Private Information consistent with the industry standards, applicable regulations, and federal, state, and/or local laws;

c) Mandating the proper notice be sent to all affected consumers, and posted publicly;

d) Requiring Defendant to protect all data collected through any account creation requirements;

e) Requiring Defendant to delete, destroy, and purge the Private Information of Plaintiffs and Class Members unless Defendant can provide reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

f) Requiring Defendant to implement and maintain a comprehensive security program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' Private Information;

g) Requiring Defendant to engage independent third-party security auditors and conduct internal security audit and testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

h) Requiring Defendant to engage independent third-party security auditors and/or internal personnel to run automated security monitoring;

i) Requiring Defendant to create the appropriate firewalls, and implement the necessary measures to prevent further disclosure and leak of any additional information;

j) Requiring Defendant to conduct systematic scanning for data breach related issues;

k) Requiring Defendant to train and test its employees regarding data breach protocols, archiving protocols, and conduct any necessary employee background checks to ensure that only individuals with the appropriate training and access may be allowed to access the Private Information data; and

l) Requiring all further and just corrective action, consistent with permissible law and pursuant to only those causes of action so permitted.

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

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

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

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

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

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

VI. JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs respectfully demand a trial by jury for all claims.

DATED: July 31, 2025,

CLARKSON LAW FIRM, P.C.

/s/ Yana Hart

Yana Hart
Mark Richards
Bryan Thompson
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050
yhart@clarksonlawfirm.com
mrichards@clarksonlawfirm.com
bthompson@clarksonlawfirm.com

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

MILBERG COLEMAN BRYSON
PHILLPS GROSSMAN, PLLC
John J. Nelson
280 S. Beverly Drive
Beverly Hills, CA 92102
Tel: (858) 209-6941
jnelson@milberg.com

Interim Co-Lead Counsel for Plaintiffs and the Proposed Class