UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

FAALON ANDREWS, *individually and on behalf of all others similarly situated*, Plaintiff, v. CALIFORNIA PHYSICIANS' SERVICE d/b/a BLUE SHIELD OF CALIFORNIA, Defendant.	Case No.: _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff, Faalon Andrews ("Plaintiff"), individually and on behalf of the Class defined below of similarly situated persons, alleges the following against Defendant California Physicians' Service d/b/a Blue Shield of California ("Defendant" or "Blue Shield"), based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation by counsel as to all other matters:

SUMMARY OF THE CASE

1. This action arises from Defendant's failure to secure the personally identifiable information ("PII")[1] protected health information ("PHI")[2] (collectively, "Private Information")

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected

of Plaintiff and the members of the proposed Class, where Plaintiffs are current and former customers of Defendant.

2. Blue Shield is a health insurance company that provides its customers access to high quality healthcare.[3]

3. On or around August 26, 2024, Young Consulting, Inc., on behalf of Blue Shield, notified Plaintiff of a cyberattack on its system. Young Consulting determined that between April 10, 2024, and April 13, 2024, an unauthorized actor downloaded filed off its system, which contained the Private Information of Blue Shield customers (the "Data Breach").[4]

4. The Private Information intruders accessed and infiltrated from Defendant's systems included, at the very least name, Social Security numbers, dates of birth, and insurance policy/claim information.[5]

5. As a result of the Data Breach, which Defendant failed to prevent, the Private Information of its customers, including Plaintiff and the proposed Class Members, was stolen.[6]

6. Instead, Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to implement reasonable measures to safeguard its current and former customers' Private Information and by failing to take necessary steps to prevent unauthorized disclosure of that information. Defendant's woefully inadequate data

---

health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last visited September 3, 2024).

[3] https://www.blueshieldca.com/en/home/about-blue-shield (last visited September 4, 2024).

[4] *See* the Notice Letter Plaintiff received from Young Consulting, Inc. attached hereto as ***Exhibit A***. A Sample Notice Letter can be found at https://youngconsulting.com/notice/youngconsulting-notice.html (last visited September 4, 2024).

[5] *See* Ex. A.

[6] *Id*.

security measures made the Data Breach a foreseeable, and even likely, consequence of its negligence.

7. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have suffered actual and present injuries, including but not limited to: (a) present, certainly impending, and continuing threats of identity theft crimes, fraud, scams, and other misuses of their Private Information; (b) diminution of value of their Private Information; (c) loss of benefit of the bargain (price premium damages); (d) loss of value of privacy and confidentiality of the stolen Private Information; (e) illegal sales of the compromised Private Information; (f) mitigation expenses and time spent responding to and remedying the effects of the Data Breach; (g) identity theft insurance costs; (h) "out of pocket" costs incurred due to actual identity theft; (i) credit freezes/unfreezes; (j) expense and time spent on initiating fraud alerts and contacting third parties; (k) decreased credit scores; (l) lost work time; and (m) anxiety, annoyance, and nuisance; (n) continued risk to their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

8. Plaintiff and Class Members would not have provided their valuable Private Information had they known that Defendant would make their Private Information Internet-accessible, not encrypt personal and sensitive data elements and not delete the Private Information it no longer had reason to maintain.

9. Through this lawsuit, Plaintiff seek to hold Defendant responsible for the injuries they inflicted on Plaintiff and Class Members due to their impermissibly inadequate data security measures, and to seek injunctive relief to ensure the implementation of security measures to protect the Private Information that remains in Defendant's possession.

10. The exposure of one's Private Information to cybercriminals is a bell that cannot be un-rung. Before this Data Breach, Plaintiff's and the Class's Private Information was exactly that—private. Not anymore. Now, their Private Information is forever exposed and unsecure.

JURISDICTION AND VENUE

11. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of Class Members is about 180,000 people, many of whom have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

12. The Court has general personal jurisdiction over Defendant because Defendant's headquarters and principal place of business is located in this District.

13. Venue is proper in this Court pursuant to 28 U.S.C. § 1391, because it is the District within which Defendant has the most significant contacts.

PARTIES

14. Plaintiff Faalon Andrews is, and at all relevant times has been, a resident and citizen of Texas, where she intends to remain.

15. Defendant Blue Shield is a California corporation with its headquarters and principal place of business located at 601 12th St. Oakland, CA 94607.

FACTUAL ALLEGATIONS

A. The Data Breach

16. As a condition of receiving healthcare, Plaintiff and Class Members were required to provide Blue Shield with their sensitive and confidential Private Information, including their

names, Social Security numbers, and other sensitive information, that would be held by Defendant in its computer systems.

17. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiff and Class Members, such as encrypting the information or deleting it when it is no longer needed, causing the exposure of Private Information.

18. As evidenced by the Data Breach, the Private Information contained in Defendant's network and was not encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

B. The Value of Private Information

19. In April 2020, ZDNet reported in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year", that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for complaints as revenge against those who refuse to pay."[7]

20. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[8]

21. Stolen Private Information is often trafficked on the dark web, as is the case here.

[7] https://www.zdnet.com/article/ransomeware-mentioned-in-1000-sec-filings-over-the-past-year/ (last visited September 4, 2024).

[8] *See* https://www.cisa.gov/sites/default/files/2023-01-CISA_MSISAC_Ransomware%20Guide_8508C.pdf (last visited September 4, 2024).

Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

22. When malicious actors infiltrate companies and copy and exfiltrate the Private Information that those companies store, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[9]

23. Another example is when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [Private Information] belonging to victims from countries all over the world. One of the key challenges of protecting Private Information online is its pervasiveness. As data breaches in the news continue to show, Private Information about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[10]

24. The Private Information of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, Private Information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $2009.[11] Experian reports

[9] *Shining a Light on the Dark Web with Identity Monitoring, IdentityForce*, Dec. 28, 2020, https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited September 4, 2024).
[10] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor, April 3, 2018, https://www.armor.com/resources/blog/stolen-pii- ramifications- identity-theft-fraud-dark-web/ (last visited September 4, 2024).
[11] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, https://www.digitaltrends.com/computing/personal- data-sold-on-the-dark-web- how-much-it-costs/ (last visited September 4, 2024).

that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[12] Criminals can also purchase access to entire company data breaches.[13]

25. Once Private Information is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional Private Information being harvested from the victim, as well as Private Information from family, friends and colleagues of the original victim.

26. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.

27. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

28. Data breaches facilitate identity theft as hackers obtain consumers' Private Information and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' Private Information to others who do the same.

29. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use Private Information to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[14] The GAO Report further notes that this type of identity fraud is the most harmful

[12] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is- selling-for-on-the-dark-web/ (last visited September 3, 2024).
[13] *In the Dark*, VPNOverview, 2019, https://vpnoverview.com/privacy/anonymous- browsing/in-the- dark/ (last visited September 3, 2024).
[14] *See* Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), https://www.gao.gov/assets/gao- 07-737.pdf (last visited September 3, 2024).

because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[15]

30. The market for Private Information has continued unabated to the present, and in 2023 the number of reported data breaches in the United States increased by 78% over 2022, reaching 3205 data breaches.[16]

31. The exposure of Plaintiff's and Class Members' Private Information to cybercriminals will continue to cause substantial risk of future harm (including identity theft) that is continuing and imminent in light of the many different avenues of fraud and identity theft utilized by third-party cybercriminals to profit off of this highly sensitive information.

C. Defendant Failed to Comply with Regulatory Requirements and Standards.

32. Federal and state regulators have established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and employees. There are a number of state and federal laws, requirements, and industry standards governing the protection of Private Information.

33. For example, at least 24 states have enacted laws addressing data security practices that require businesses that own, license, or maintain Private Information about a resident of that

[15] *Id*.

[16] Beth Maundrill, *Data Privacy Week: US Data Breaches Surge, 2023 Sees 78% Increase in Compromises*, INFOSECURITY MAGAZINE (Jan. 23, 2024); https://www.infosecurity-magazine.com/news/us-data-breaches-surge-2023/ (last visited September 4, 2024); *see also* Identity Theft Resource Center, *2023 Data Breach Report*, https://www.idtheftcenter.org/publication/ 2023-data-breach-report/ (last visited September 4, 2024).

state to implement and maintain "reasonable security procedures and practices" and to protect Private Information from unauthorized access.

34. Additionally, cybersecurity firms have promulgated a series of best practices that at a minimum should be implemented by sector participants including, but not limited to: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting of physical security systems; protecting against any possible communication system; and training staff regarding critical points.[17]

35. The FTC has issued several guides for businesses, highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be considered for all business decision-making.[18]

36. Under the FTC's 2016 *Protecting Personal Information: Guide for Business* publication, the FTC notes that businesses should safeguard the personal customer information they retain; properly dispose of unnecessary personal information; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to rectify security issues.[19]

37. The guidelines also suggest that businesses use an intrusion detection system to expose a breach as soon as it happens, monitor all incoming traffic for activity indicating someone

[17] *See Addressing BPO Information Security: A Three-Front Approach*, DATAMARK, INC. (Nov. 2016), https://insights.datamark.net/addressing-bpo-information-security (last visited September 4, 2024).
[18] *Start With Security*, Fed. Trade Comm'n ("FTC"), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited September 4, 2024).
[19] *Protecting Personal Information: A Guide for Business*, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited September 4, 2024).

is trying to hack the system, watch for large amounts of data being siphoned from the system, and have a response plan in the event of a breach.

38. The FTC advises companies to not keep information for periods of time longer than needed to authorize a transaction, restrict access to private information, mandate complex passwords to be used on networks, utilize industry-standard methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[20]

39. The FTC has brought enforcement actions against companies for failing to adequately and reasonably protect consumer data, treating the failure to do so as an unfair act or practice barred by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders originating from these actions further elucidate the measures businesses must take to satisfy their data security obligations.

40. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

41. Defendant's failure to verify that it had implemented reasonable security measures constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

42. Furthermore, Defendant is required to comply with the HIPAA Privacy 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. The Privacy Rule and the Security Rule set nationwide standards for protecting health information, including

[20] *Id.*

health information stored electronically.

43. The Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.[21]

44. Pursuant to HIPAA's mandate that Blue Shield follows "applicable standards, implementation specifications, and requirements . . . with respect to electronic protected health information," 45 C.F.R. § 164.302, Blue Shield was required to, at minimum, "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information," 45 C.F.R. § 164.306(e), and "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

45. Blue Shield is also required to follow the regulations for safeguarding electronic medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

46. Both HIPAA and HITECH obligate Blue Shield to follow reasonable security

[21] *Summary of the HIPAA Security Rule*, HHS, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited Mar. 12, 2024).

standards, respond to, contain, and mitigate security violations, and to protect against disclosure of sensitive patient Private Information. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); 45 C.F.R. § 164.530(f); 42 U.S.C. § 17902.

47. As alleged in this Complaint, Blue Shield has failed to comply with HIPAA and HITECH. It has failed to maintain adequate security practices, systems, and protocols to prevent data loss, failed to mitigate the risks of a data breach and loss of data, and failed to ensure the confidentiality and protection of PHI.

D. Defendant Failed to Comply with Industry Practices.

48. Various cybersecurity industry best practices have been published and should be consulted as a go-to resource when developing an organization's cybersecurity standards. The Center for Internet Security ("CIS") promulgated its Critical Security Controls, which identify the most commonplace and essential cyber-attacks that affect businesses every day and proposes solutions to defend against those cyber-attacks.[22] All organizations collecting and handling Private Information, such as Defendant, are strongly encouraged to follow these controls.

49. Further, the CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the adoption of a secure build standard for any governance and security initiative, including PCI DSS, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley and ITIL.[23]

50. Several best practices have been identified that a minimum should be implemented by data management companies like Defendant, including but not limited to securely configuring business software, managing access controls and vulnerabilities to networks, systems, and

[22] Center for Internet Security, *Critical Security Controls*, at 1 (May 2021), https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf (last visited September 4, 2024).
[23] *See CIS Benchmarks FAQ*, Center for Internet Security, https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/ (last visited September 4, 2024).

software, maintaining network infrastructure, defending networks, adopting data encryption while data is both in transit and at rest, and securing application software.[24]

51. Defendant failed to follow these and other industry standards to adequately protect the Private Information of Plaintiff and Class Members.

E. The Data Breach Caused Injury to Class Members and Will Result in Additional Harm Such as Fraud.

52. Without detailed disclosure to the victims of the Data Breach, individuals whose Private Information was compromised by the Data Breach, including Plaintiff and Class Members, were unknowingly and unwittingly exposed to continued misuse and ongoing risk of misuse of their Private Information for months without being able to take available precautions to prevent imminent harm.

53. The ramifications of Defendant's failure to secure Plaintiff's and Class Members' data are severe.

54. Victims of data breaches are much more likely to become victims of identity theft and other types of fraudulent schemes. This conclusion is based on an analysis of four years of data that correlated each year's data breach victims with those who also reported being victims of identity fraud.

55. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[25] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[26]

---

[24] *See* Center for Internet Security, *Critical Security Controls* (May 2021), https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf (last visited September 4, 2024).
[25] 17 C.F.R. § 248.201 (2013).
[26] *Id*.

56. Identity thieves can use Private Information, such as that of Plaintiff and Class Members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

57. As demonstrated herein, these and other instances of fraudulent misuse of the compromised Private Information has already occurred and are likely to continue.

58. As a result of Defendant's delay between the Data Breach in April and the notice of the Data Breach sent to affected persons in August, the risk of fraud for Plaintiff and Class Members increased exponentially.

59. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[27]

60. The 2017 Identity Theft Resource Center survey[28] evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed;
- 67% reported anxiety;

[27] *Victims of Identity Theft*, Bureau of Justice Statistics (Sept. 2015) http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited September 4, 2024).
[28] *Id*.

- 66% reported feelings of fear related to personal financial safety;
- 37% reported fearing for the financial safety of family members;
- 24% reported fear for their physical safety;
- 15.2% reported a relationship ended or was severely and negatively impacted by identity theft; and
- 7% reported feeling suicidal.

61. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate / lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[29]

62. There may be a time lag between when harm occurs versus when it is discovered, and also between when private information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[30]

---

[29] *Id*.

[30] GAO, *Report to Congressional Requesters*, at 29 (June 2007), http://www.gao.gov/new.items/d07737.pdf (last visited September 4, 2024).

Thus, Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

F. Plaintiff and Class Members Suffered Damages.

63. As a direct and proximate result of Defendant's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class Members have already been harmed by the fraudulent misuse of their Private Information, and have been placed at an imminent, immediate, and continuing increased risk of additional harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate both the actual and potential impact of the Data Breach on their lives. Such mitigatory actions include, *inter alia*, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, sorting through dozens of phishing and spam email, text, and phone communications, and filing police reports. This time has been lost forever and cannot be recaptured.

64. Defendant's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' Private Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft and misuse of their personal and financial information;

b. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals and misused via the sale of Plaintiff's and Class Members' information on the Internet's black market;

c. the untimely and inadequate notification of the Data Breach;

d. the improper disclosure of their Private Information;

e. loss of privacy;

f. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. ascertainable losses in the form of deprivation of the value of their Private Information, for which there is a well-established national and international market;

h. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the Data Breach; and

i. nominal damages.

65. While Plaintiff's and Class Members' Private Information has been stolen, Defendant continues to hold Plaintiff's and Class Members' Private Information. Particularly because Defendant has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and Class Members have an undeniable interest in ensuring that their Private Information is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

G. Plaintiff's Experience.

66. Plaintiff Faalon Andrews was an employee of Box from 2019 until 2022 and gave

Blue Shield her Private Information, including her Social Security number, as a condition of receiving healthcare benefits with Blue Shield.

67. Plaintiff provided Private Information, directly or indirectly, to Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect her Private Information.

68. Since the Data Breach, Plaintiff has experienced anxiety and increased concerns for the loss of her privacy, as well as anxiety over the impact of cybercriminals accessing and using her Private Information.

69. Plaintiff would not have entrusted her Private Information to Defendant had she known they would not take reasonable steps to safeguard her information.

70. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

71. Plaintiff is very careful about sharing sensitive Private Information. She stores documents containing Private Information in safe and secure locations and has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source. Plaintiff would not have entrusted her Private Information to Defendant had she known of Defendant's lax data security policies.

72. As a direct and proximate result of the Data Breach, Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring her financial accounts.

73. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

She has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

CLASS ALLEGATIONS

74. Plaintiff brings this class action individually on behalf of herself and all members of the following Class of similarly situated persons pursuant to Federal Rule of Civil Procedure 23. Plaintiff seeks certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3) of the following Class:

> All persons residing in the United States whose Private Information was compromised in the Data Breach, including all who were sent a notice of the Data Breach.

75. Excluded from the Class are Defendant and its affiliates, parents, subsidiaries, officers, agents, and directors, any entities in which Defendant has a controlling interest, as well as the judge(s) presiding over this matter and the clerks, judicial staff, and immediate family members of said judge(s).

76. Plaintiff reserves the right to modify or amend the foregoing Class definitions before the Court determines whether certification is appropriate.

77. Numerosity: The members in the Class are so numerous that joinder of all Class Members in a single proceeding would be impracticable.

78. Commonality and Predominance: Common questions of law and fact exist as to all Class Members and predominate over any potential questions affecting only individual Class Members. These common questions of law or fact include, *inter alia*:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class Members' Private Information from unauthorized access and disclosure;

c. Whether Defendant's computer systems and data security practices used to protect Plaintiff's and Class Members' Private Information violated the FTC Act and/or state laws, and/or Defendant's other duties discussed herein;

d. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and Class Members;

e. Whether Defendant unlawfully shared, lost, or disclosed Plaintiff's and Class Members' Private Information;

f. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

h. Whether Plaintiff and Class Members suffered injury as a proximate result of Defendant's negligent actions or failures to act;

i. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiff's and Class Members' Private Information;

j. Whether Defendant breached duties to protect Plaintiff's and Class Members' Private Information;

k. Whether Defendant's actions and inactions alleged herein were negligent;

l. Whether Defendant were unjustly enriched by their conduct as alleged herein;

m. Whether an implied contract existed between Class Members and Defendant with respect to protecting Private Information and privacy, and whether that contract was breached;

n. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages or other relief, and the measure of such damages and relief;

o. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

p. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

79. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff on behalf of herself and all other Class Members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

80. Typicality: Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had her Private Information compromised in the Data Breach. Plaintiff and Class Members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class Members.

81. Adequacy: Plaintiff will fairly and adequately protect the interests of the Class Members. Plaintiff is an adequate representative of the Class and has no interests adverse to, or conflict with, the Class she seeks to represent. Plaintiff has retained counsel with substantial

experience and success in the prosecution of complex consumer protection class actions of this nature.

82. Superiority: A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and all other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class Members to individually seek redress from Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

83. Injunctive and Declaratory Relief: Defendant has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

84. Likewise, particular issues are appropriate for certification under Rule 24(c)(4) because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such issues include, but are not limited to: (a) whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, and safeguarding their Private Information; (b) whether Defendant failed to adequately monitor and audit their data security systems; and (c) whether

Defendant failed to take reasonable steps to safeguard the Private Information of Plaintiff and Class Members.

85. All members of the proposed Class are readily ascertainable. Defendant has access to the names in combination with addresses and/or e-mail addresses of Class Members affected by the Data Breach. Indeed, impacted Class Members already have been preliminarily identified and sent a breach notice letter.

CAUSES OF ACTION

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

86. Plaintiff restates and realleges paragraphs 1 through 85 above as if fully set forth herein.

87. Defendant requires its customers to submit non-public Private Information as a condition of receiving insurance.

88. Defendant gathered and stored the Private Information of Plaintiff and Class Members as part of its business, which affects commerce.

89. Plaintiff and Class Members entrusted Defendant with their Private Information with the understanding that the information would be safeguarded.

90. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if their Private Information were wrongfully disclosed.

91. By assuming the responsibility to collect and store this data, Defendant had duties of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

92. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

93. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiff and Class Members, on the other hand. That special relationship arose because Defendant was entrusted with their confidential Private Information as a condition of receiving insurance with Defendant.

94. Defendant also had a duty to exercise appropriate clearinghouse practices to remove its former customers' Private Information they were no longer required to retain pursuant to regulations.

95. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach, but failed to do so.

96. Defendant had and continues to have duties to adequately disclose that Plaintiff's and Class Members' Private Information within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

97. Defendant breached its duties and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Allowing unauthorized access to Class Members' Private Information;

d. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

e. Failing to remove former customers' Private Information they were no longer required to retain pursuant to regulations; and

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

98. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

99. Defendant knew or should have known that its failure to implement reasonable data security measures to protect and safeguard Plaintiff's and Class Members' Private Information would cause damage to Plaintiff and the Class.

100. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

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

102. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of corporate cyberattacks and data breaches.

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

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

105. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

106. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

107. Defendant's duties extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which have been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

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

109. But for Defendant's wrongful and negligent breaches of duties owed to Plaintiff and the Class, Plaintiff's and Class Members' Private Information would not have been compromised.

110. There is a close causal connection between Defendant's failure to implement security measures to protect Plaintiff's and Class Members' Private Information, and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. Private Information was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care by adopting, implementing, and maintaining appropriate security measures.

111. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised Private Information; (ii) invasion of privacy; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Private Information for the rest of their lives; (ix) the present value of ongoing credit monitoring and identity defense services necessitated by the Data Breach; (x) the value of the unauthorized

access to their Private Information permitted by Defendant; and (xi) any nominal damages that may be awarded.

112. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses including nominal damages.

113. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

114. Defendant's negligent conduct is ongoing, in that it still possesses Plaintiff's and Class Members' Private Information in an unsafe and insecure manner.

115. Plaintiff and Class Members are entitled to injunctive relief requiring Defendant to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Class Against Defendant)

116. Plaintiff restates and realleges paragraphs 1 through 85 above as if fully set forth herein.

117. Defendant had duties arising under the FTC Act and HIPAA to protect Plaintiff's and Class Members' Private Information.

118. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information. The specific negligent acts and omissions

committed by Defendant include, but are not limited to, the following: (i) failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information; (ii) failing to adequately monitor the security of their networks and systems; (iii) allowing unauthorized access to Class Members' Private Information; (iv) failing to detect in a timely manner that Class Members' Private Information had been compromised; (v) failing to remove its former customers' Private Information they were no longer required to retain pursuant to regulations; and (vi) failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

119. Defendant's violations of Section 5 of the FTC Act and HIPAA (and similar state statutes) constitute negligence *per se*.

120. Plaintiff and Class Members are consumers within the class of persons that Section 5 of the FTC Act and HIPAA were intended to protect.

121. The harm that has occurred is the type of harm the FTC Act and HIPAA were intended to guard against.

122. The FTC has pursued enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

123. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

124. In addition, under state data security and consumer protection statutes such as those outlined herein, Defendant had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class Members' Private Information.

125. Plaintiff and Class Members were foreseeable victims of Defendant's violations of the FTC Act and HIPAA, and state data security and consumer protection statutes. Defendant knew or should have known that its failure to implement reasonable data security measures to protect and safeguard Plaintiff's and Class Members' Private Information would cause damage to Plaintiff and the Class.

126. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised Private Information; (ii) invasion of privacy; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

127. As a direct and proximate result of Defendant's negligence *per se* Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

128. Finally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class Against Defendant)

129. Plaintiff restates and realleges paragraphs 1 through 85 above as if fully set forth herein.

130. When Plaintiff and Class Members provided their Private Information to Defendant, Plaintiff and Class Members entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members that their data had been breached and compromised.

131. Defendant required Plaintiff and Class Members to provide and entrust their PHI and PII as a condition of receiving insurance.

132. Plaintiff and Class Members would not have provided and entrusted their PHI and PII to Defendant in the absence of the implied contract between them and Defendant.

133. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

134. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect the Private Information of Plaintiff and Class Members and by failing to provide timely and accurate notice to them that their personal information was compromised in and as a result of the Data Breach.

135. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class Against Defendant)

136. Plaintiff restates and realleges paragraphs 1 through 85 above as if fully set forth herein.

137. This count is brought in the alternative to Plaintiff's breach of implied contract count.

138. Plaintiff and Class Members conferred a benefit on Defendant by way of customers' paying Defendant to maintain Plaintiff and Class Members' personal information.

139. The monies paid to Defendant were supposed to be used by Defendant, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and Class Members.

140. Defendant failed to provide reasonable security, safeguards, and protections to the personal information of Plaintiff and Class Members, and as a result Defendant was overpaid.

141. Under principles of equity and good conscience, Defendant should not be permitted to retain the money because Defendant failed to provide adequate safeguards and security measures to protect Plaintiff and Class Members' Private Information that they paid for but did not receive.

142. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

143. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

144. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and the Class are entitled to restitution and disgorgement of profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the class, respectfully requests that the Court enter judgment in Plaintiff's favor and against Defendant as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class representatives, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, nominal damages and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of herself and the class, seek appropriate injunctive relief designed to prevent Defendant from experiencing another data breach by adopting and implementing best data security practices to safeguard Private Information and to provide or extend credit monitoring services and similar services to protect against all types of identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMAND

Plaintiff demands a trial by jury of all claims herein so triable.

Dated: September 4, 2024.

Respectfully submitted,

/s /Jeff Ostrow
Jeff Ostrow
KOPELOWITZ OSTROW FERGUSON WEISELBERG GILBERT
One West Law Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Tel: (954) 332-4200
ostrow@kolawyers.com

Counsel for Plaintiff and the Proposed Class

ClassAction.org